



White paper for EXFO

Assurance-driven network automation is key to 5G success

April 2019

Anil Rao

Contents

1.	Executive summary	1
2.	5G is a game changer for CSPs, industries and societies	2
2.1	The ‘race to launch’ 5G has begun	2
2.2	Non-standalone (NSA) 5G network deployments will deliver traditional broadband services	3
2.3	Standalone (SA) deployments will support mMTC and URLLC use cases	3
3.	Network automation will be essential to operationalise complex 5G networks	4
3.1	5G service-based architecture (SBA) brings IT automation concepts to networks	5
3.2	Edge clouds and network slicing are key enablers for critical 5G use cases	6
3.3	NFV, CNC and SDN are pivotal for automating 5G	7
4.	Dynamic and automated assurance is necessary to enable 5G network automation	8
4.1	Unified cross-domain assurance including application performance monitoring	9
4.2	Dynamic monitoring of the 5G network and network slices to guarantee QoS, SLAs and customer experience	10
4.3	ML/AI based predictive assurance and root-cause analysis	10
4.4	Assurance assisted closed-loop automation with MANO	11
5.	Automated assurance must be integrated into CSPs’ chosen network automation platforms	13
6.	Illustrative 5G use cases – the role of automated assurance	13
6.1	Long-distance 5G drones	13
6.2	5G smart grids	14
6.3	The role of automated assurance	16
7.	About EXFO’s assurance-driven automation	18
8.	Conclusion and recommendations	19
	About the author	20
	Analysys Mason’s consulting and research are uniquely positioned	21
	Research from Analysys Mason	22
	Consulting from Analysys Mason	23

List of figures

Figure 1: 5G launch timeline	3
Figure 2: 5G industry use cases	4
Figure 3: The key architectural enablers for 5G	5
Figure 4: Service-based architecture enabling 5G network as a service	6
Figure 5: Edge cloud and network slicing enabling service innovation	7
Figure 6: Key pillars of automated assurance for 5G	8
Figure 7: Unified monitoring of the 5G network	9
Figure 8: ML/AI based root-cause analysis	11
Figure 9: Closed-loop assurance through MANO	12
Figure 10: Service requirements for smart grid applications	14

Figure 11: Service requirements for smart grid applications	16
Figure 12: Assurance enabled network slice lifecycle management.....	16
Figure 13: Automation throughout the service lifecycle.....	18

1. Executive summary

5G is being heralded as a revolution with the potential to transform communications service providers (CSPs), enable the digital transformation of whole industries and enterprises, and change our societies forever. Early 5G use cases based on non-standalone (NSA) deployment will deliver multi-gigabit enhanced mobile broadband (eMBB) services to consumers, but, it is the new business and economic opportunities offered by standalone (SA) 5G in the form of ultra-reliable low latency communications (URLLC) and massive machine-type communications (mMTC) use cases for other industry verticals that are exciting the stakeholders and partners across the spectrum including industries such as manufacturing, automotive, utilities, and healthcare and emergency public services.

To support such diverse industries with a broad array of use cases and varying demands such as service dynamicity, quality of service and latency requirements, the industry is building the 5G network based on innovations such as service-based architecture (SBA), 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.

However, these technological innovations introduce significant network and operational complexities that must be managed to deliver on the promise of 5G. Traditional service management and operational approaches that were built to support physical networks delivering mass market communication services are not fit for purpose. High levels of network automation underpinned by dynamic and automated assurance will be necessary to operationalise 5G networks and services at scale.

Assurance for 5G must be built on four key pillars.

- Provide unified monitoring spanning the 5G cloud core, xHaul (backhaul/front-haul), edge clouds and the 5G New Radio, and incorporate Layer 0–7 monitoring including the application layer.
- Provide dynamic assurance with the ability to adapt and scale with the network functions, service chains and network slices as they are instantiated and modified.
- Provide machine learning and artificial intelligence (ML/AI)-based predictive assurance and root cause analysis using real-time network and service topology.
- Assist closed loop automation by empowering management and network (MANO) systems with policy-driven precise actions to execute the configuration changes into the network.

To achieve the overall automation goals of 5G, CSPs are deploying network automation platforms such as Open Network Automation Platform (ONAP) and other vendor-specific commercial solutions that automate the network and service lifecycle management. These platforms consist of disaggregated and loosely coupled software components that combine the full range of capabilities to automate service design, manage the lifecycle of network functions, service and resource orchestration and automated closed-loop assurance. Other industry bodies such as TMForum and MEF are proposing best practices and operational frameworks that provide the base specifications for network automation. To fully realise the benefits of network automation, assurance systems must become an integral part of the CSPs' preferred automation platforms and frameworks.

2. 5G is a game changer for CSPs, industries and societies

4G is for humans and 5G is for machines, is the general consensus in the industry, which has profound implications for CSPs and a broad range of stakeholders across industries, regulatory bodies, public services, government agencies, and our societies in general. Indeed, 5G delivers multi-gigabit enhanced mobile broadband (eMBB), which has the potential to transform customer experiences for high-bandwidth services such as mobile gaming and VR/AR. However, 4G is still far from reaching its limit and can be further enhanced to support the needs of most consumers for the foreseeable future. Nevertheless, some CSPs are already taking 5G eMBB to consumers through special use cases, such as fixed–wireless access (FWA) for home broadband, which uses 5G New Radio (NR) for the last hop instead of fibre or copper.

5G FWA is an evolution in the use of mobile technology for humans, but 5G will be revolutionary in that it will inspire and enable a new generation of IoT use cases for machines. Capabilities such as mMTC and URLLC promise to transform industries such as manufacturing (Industrial IoT), automotive (autonomous vehicles), utilities (smart grids), healthcare (telemedicine) and emergency public services (disaster response). It is in this context that it is widely accepted that **5G is going to be a revolution not an evolution**, as highlighted by Deutsche Telekom.¹

It is in such capacities that it becomes clear why the technologies from 2G to 4G differ so radically from the fifth generation, and that what is awaiting us is partly a new beginning and partly a turning point, but certainly nothing less than a revolution.

- Deutsche Telekom

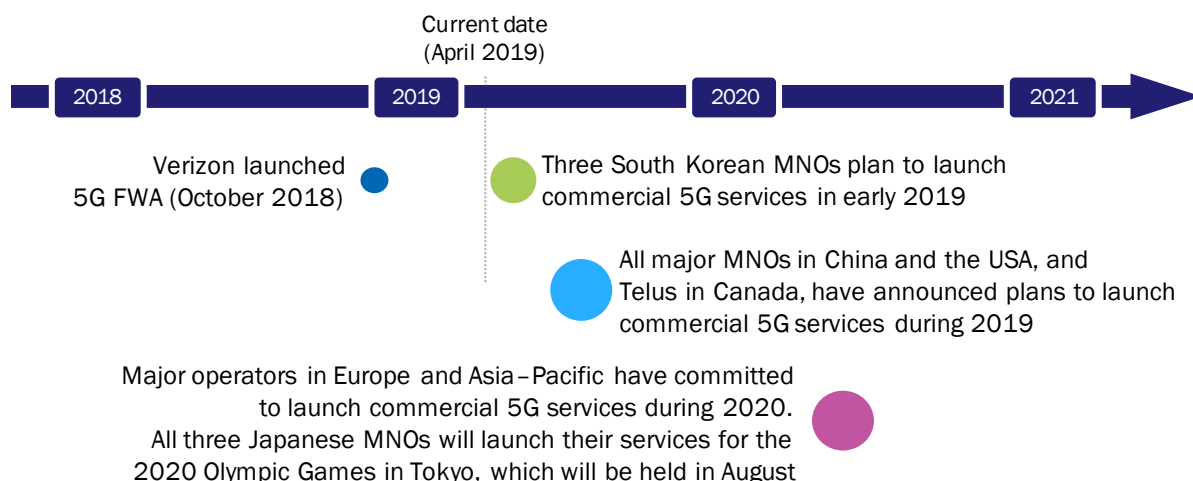
2.1 The ‘race to launch’ 5G has begun

Leading CSPs in North America, Asia and Europe have accelerated their 5G plans in a bid to capture additional market share and to be first-to-market, or to demonstrate their technological lead. (Figure 1)

- American CSP Verizon achieved the highest profile 5G launch to-date, beginning with 5G FWA in four US markets in October 2018.
- CSPs in South Korea are commercialising 5G after SKT and LG Uplus demonstrated trial 5G services at the 2018 Winter Olympics.
- It is expected that 5G services will be demonstrated or launched to coincide with two other major sporting events, the European UEFA championships in 2020 and the 2020 Tokyo Olympics.

¹ For more information, see <https://www.telekom.com/en/company/details/5g-revolution-not-evolution-481778>.

Figure 1: 5G launch timeline



Source: Analysys Mason

2.2 Non-standalone (NSA) 5G network deployments will deliver traditional broadband services

Leveraging the 5G new radio (NR) with CSPs' existing 4G core, the NSA 5G deployments enables CSPs to offer high-capacity eMBB services. Some CSPs will choose the NSA configuration for early launches, such as in the USA and China.² NSA deployments will cater for the 5G FWA service for the fixed broadband market, while the launch of mobile eMBB will depend on the availability of the new 5G mobile chipsets.

However, it is clear that CSPs are not betting on significantly increasing revenue with NSA deployments because the eMBB consumer services will be marketed at about the same price (at best) as the 4G data services. This is emphasised in the following statement by a global Tier 1 CSP based in Europe.

eMBB and FWA will not be the 'cash cow' for 5G but will help to offset some of the deployment costs of 5G services, including spectrum and infrastructure. Incremental revenue will come from new 5G services under the mMTC and URLLC category.







- Global Tier 1 CSP

2.3 Standalone (SA) deployments will support mMTC and URLLC use cases

With the publication of the 3GPP Release 15 and the expected availability of Release 16 specifications by end of 2019, the industry is pressing ahead with testing and commercialising 5G SA, which introduces the new 5G next generation core (NGC). When implemented in full, the SA deployment provides the foundational technical capabilities such as mMTC and URLLC, enabling a much broader 5G market opportunity than traditional telecoms services as discussed in Figure 2 below:

² For more information, see https://api.ctia.org/wp-content/uploads/2018/04/Analysys-Mason-Global-Race-To-5G_2018.pdf.

Figure 2: 5G industry use cases

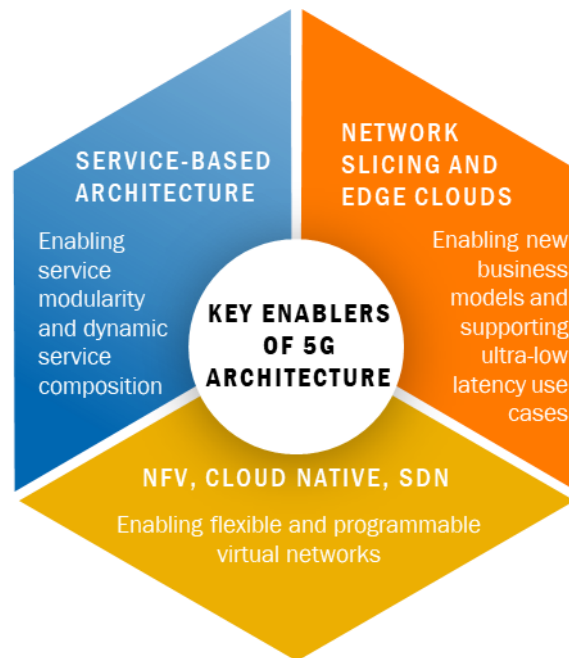
	Market sector	Key use case	Description
	Cross-industry	Long-distance drones	Remote control of drones beyond line of sight for video surveillance
	Transportation	5G V2X services	Vehicle-to-everything (V2X) communications for passenger cars, commercial vehicles and self-driving cars
	Smart cities	Emergency communications	Dedicated mobile connectivity services for emergency services
	Manufacturing	Industry robots	Cloud-based remote control of factory robots
	Utilities	Smart grid	Advanced smart grid applications to wirelessly monitor and control electricity generation and distribution equipment
	Healthcare	Personal emergency response systems	Connected devices used by senior citizens and vulnerable adults for emergency response and location services

Source: Analysys Mason

Successful commercialisation of these use cases will depend on multiple factors such as coordinated cross-industry collaboration to define the use case requirements and a fit-for-purpose network architecture that enables rapid service innovation and new business models. In line with the network changes and the dynamic service demands, CSPs will need a radically different operations and assurance approach to support what is expected to be a highly complex and dynamic 5G network. Sections 3 and 4 will explore these aspects in more detail and will provide primary supporting evidence from the CSPs that were interviewed as part of this research.

3. Network automation will be essential to operationalise complex 5G networks

The diverse nature of the use cases, the service dynamicity and latency requirements, and the need to support new business models has forced the industry to consider new architectural approaches for the 5G network, as illustrated in Figure 3. The introduction of virtualised networks and software components to support 5G-enabled services driven by network slicing and edge clouds will make 5G networks significantly more complex than those of previous generations.

Figure 3: The key architectural enablers for 5G

Source: Analysys Mason

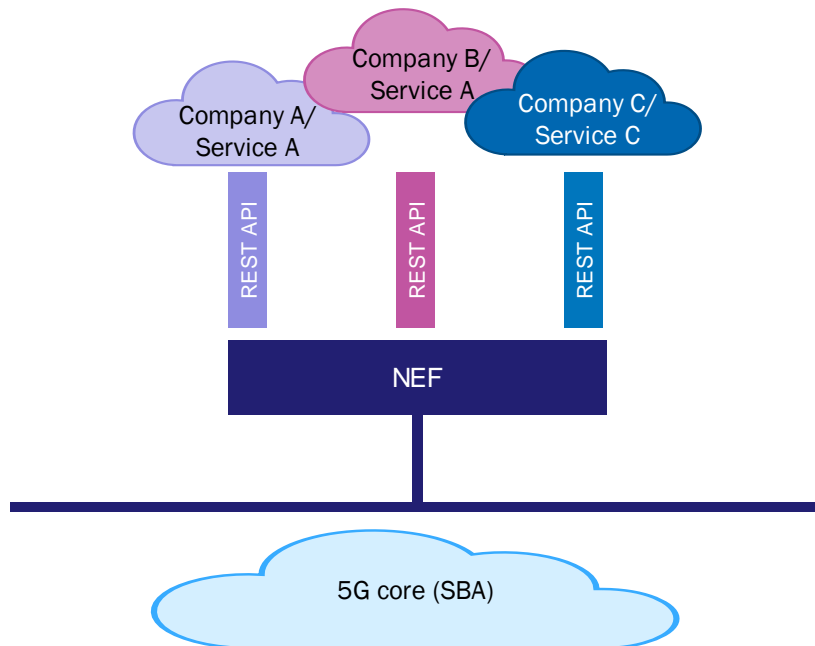
3.1 5G service-based architecture (SBA) brings IT automation concepts to networks

The SBA is like the popular IT and cloud-compliant software design principle service-oriented architecture (SOA) where a set of services are software encoded into composite software applications and exposed to customers, partners or other departments within the business, which are then accessed via open APIs. This allows massive reusability of software components, process automation and significant flexibility of interconnections between the modules.

Applying these concepts to networks, for instance, the control plane functions³ in the 5G NGC will use service-based interfaces for interactions using RESTful APIs instead of Diameter⁴. Among the many 5G network functions, the Network Exposure Function (NEF) is particularly interesting in that it exposes the capabilities of the 5G NGC via northbound RESTful APIs to the external world. Third-party developers and enterprises can create their own network services on-demand. Further tools or analytics services enable enterprises to monitor and maintain their services over the network. (Figure 4)

³ Based on control and user plane separation (CUPS) that was part of the 3GPP Release 14.

⁴ For more information, see <https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201707/Documents/Joe-Wilke-%205G%20Network%20Architecture%20and%20FMC.pdf>.

Figure 4: Service-based architecture enabling 5G network as a service

Source: Analysys Mason

The SBA-enabled 5G network cloud would be accessed much like how cloud computing platforms such as Amazon Web Services are accessed for computing and storage resources through the infrastructure-as-a-service (IaaS) model. This network-as-a-service model will transform CSPs into innovation enablers for vertical industries and third parties bolstering the B2B2C business model. This is highlighted by a Tier 1 CSP.

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.

- Global Tier 1 CSP

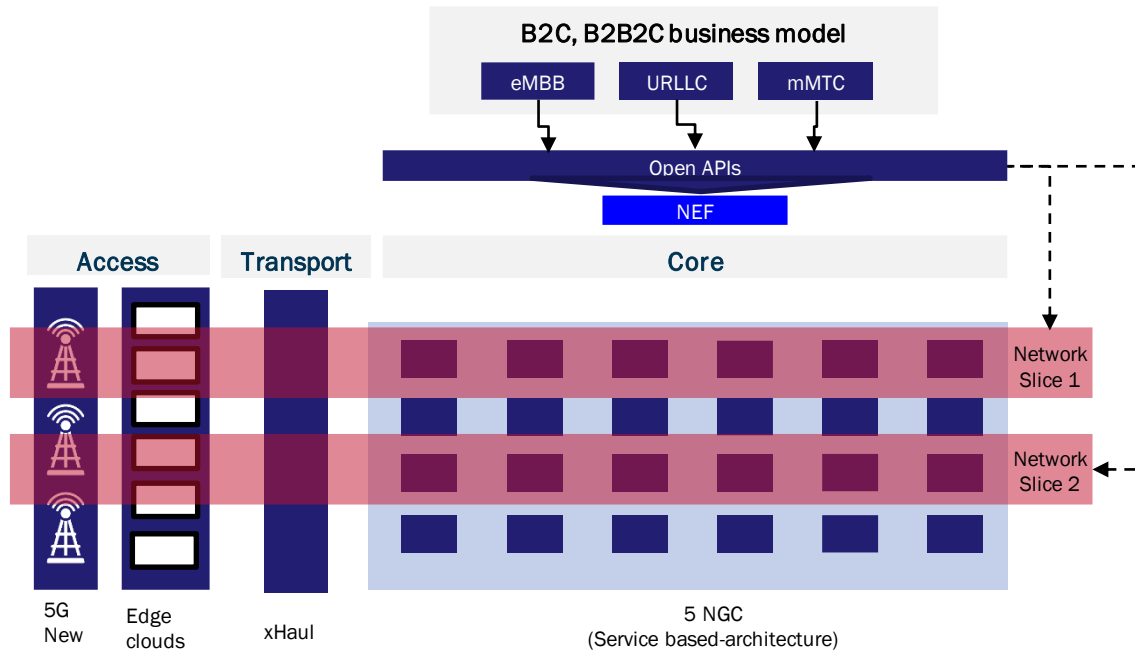
3.2 Edge clouds and network slicing are key enablers for critical 5G use cases

Based on multi-access edge computing (MEC) networking technology, edge clouds enable the use of cloud computing at the edge of the mobile network. Bringing the power of compute and storage closer to the end user or application, edge clouds reduce network congestion and reduce the latency of packet data, because the user plane data need not be hauled all the way back across the network into a central cloud core. Edge clouds promise to deliver microseconds latency allowing the CSP to support the critical URLLC use cases.

Network slicing enables the creation of end-to-end, isolated virtual logical networks cutting across radio, transport, edge and the core, with each slice capable of offering differentiated QoS and SLA to match specific service requirements such as the network capacity, latency and reliability. Network slicing paves the way for CSPs to offer differentiated slice-based services for whole industries or highly granular differentiated slices per use case, subscriber type, application or an enterprise with slice level control, management and QoS. To meet the scale and dynamicity of the service requirements, it is possible that many hundreds or thousands of network slices may be created with some slices existing only for a few seconds or minutes.

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 rapid service innovation within the CSP and enable external innovation through the B2B2C business model. (Figure 5)

Figure 5: Edge cloud and network slicing enabling service innovation



Source: Analysys Mason

3.3 NFV, CNC and SDN are pivotal for automating 5G

NFV and CNC are the foundational capabilities based on which technologies such as network slicing and edge clouds can be realised. These base capabilities provide the fundamental building blocks to transition the traditional rigid physical network into a flexible, dynamic, programmable and highly automated cloud-native network. Using the ability to create and modify network resources to reflect the changing service requirements, NFV enables CSPs to allocate network resources just in time and achieve higher network efficiency through optimum resource utilisation. SDN enables centralised traffic management capabilities to optimise service delivery, reducing network costs while maintaining and improving customer experience.

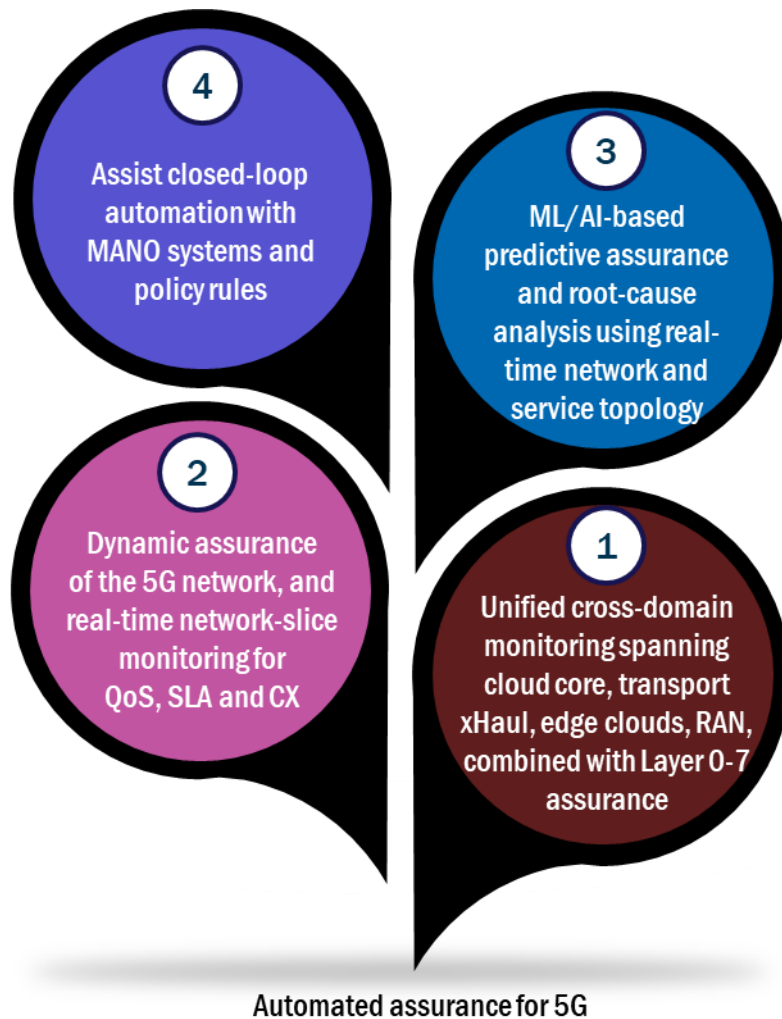
Extending this concept further, designing the network functions using cloud-native technologies such as containers and microservices prepares the network to be deployed in the cloud allowing CSPs to use DevOps and CI/CD methodologies to independently manage the lifecycle of the microservices without having an impact on the service. It also allows automatic scale-up of only those network function service modules that require more capacity and enables rapid service innovation through automated network and service orchestration by interlinking select network function services into end-to-end services, significantly reducing service creation timescales to minutes. 5G services that require network functions to be instantiated in microseconds will depend on cloud-native virtualisation and extreme automation technologies. Their ultra-low latency requirements will mandate the deployment of hundreds, if not thousands of VNF instances in the edge clouds.

4. Dynamic and automated assurance is necessary to enable 5G network automation

The long-term business success of 5G will depend on how CSPs can best exploit the technological capabilities offered by the network to develop new business models and generate new revenue streams. However, 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.

Service assurance systems and processes, which encapsulate some of the most important operational processes responsible to 'keep the lights on' for CSPs, will play an expanded role in enabling network automation. For decades, assurance systems that were designed for static physical networks 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.

Figure 6: Key pillars of automated assurance for 5G



Source: Analysys Mason

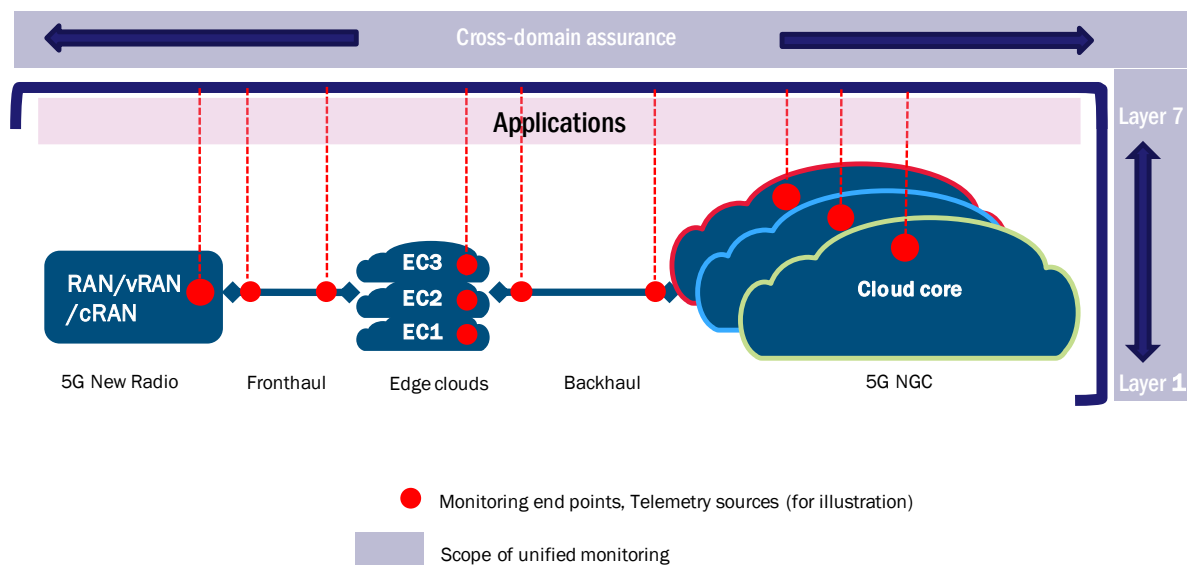
In its new incarnation for 5G, assurance systems will take on the role of the operational ‘nervous system’ responsible for driving the network automation and lifecycle management of the eMBB, URLLC and mMTC services that will be hosted on the 5G network, both for the CSP-owned services and external B2B2C services. Figure 6 illustrates the four key pillars of automated assurance for 5G, which will be discussed further in the following sub-sections.

4.1 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. Service assurance has typically been developed as an amalgamation of disparate and closed IT systems implemented on a case-by-case basis or inherited through M&A, resulting in a highly disjointed assurance estate deployed for specific operational domains. The fractured assurance estate cause poor automation and rely on manual, repetitive and error-prone processes, which in-turn rely on hierarchical and bureaucratic departments for escalations and resolutions. Ultimately, the service suffers from poor service quality and customer experience because it is extremely difficult and time consuming to accurately measure the end-to-end performance of the service and therefore, the actions are delayed. These characteristics significantly hinder CSPs’ ability to operationalise 5G and guarantee a high quality of service, limiting their ambitions to enable new revenue streams and enter new markets.

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 subscriber or edge device, including the backhaul, edge clouds, the front haul and the 5G New Radio. Furthermore, CSPs must also incorporate Layer 0–7 monitoring including the application layer, which is going to be essential to guarantee the service performance for enterprises (Figure 7). 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 the maximum coverage and impact.

Figure 7: Unified monitoring of the 5G network



Source: Analysys Mason

The need for such a unified monitoring solution for 5G is highlighted by the Tier 1 CSP in the following quote:

5G networks are being designed for new 5G applications, not just mobile services. Monitoring the network alone, at the connectivity layer, will not be enough. Monitoring must go all the way up to the application layer.

- Global Tier 1 CSP

4.2 Dynamic monitoring of the 5G network and network slices to guarantee QoS, SLAs and customer experience

Assurance in today's static networks tends to 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.

Without the capability to adapt to the dynamically changing network conditions, CSPs cannot monitor and assure the contracted QoS and SLAs. This would be particularly vital in the case of 5G SA deployments where CSPs will offer network slice-based differentiated services requiring highly dynamic monitoring and assurance for slice-level service quality parameters. Failure to assure network slices may result in inferior customer experience, non-compliance with the contracted terms and financial penalties. The result is not only potential loss of revenue, but also a higher risk of customer churn.

We have automated almost 80% of operations and made effort to transform into a premium digital service provider over the past decade. As we move to the 5G era, customer experience is going to be a key part of our ongoing transformation, so we have already taken significant steps to move from corrective assurance to preventative and predictive assurance.

- Tier 1 CSP in Asia-Pacific

4.3 ML/AI based predictive assurance and root-cause analysis

CSPs must bolster the end-to-end monitoring and dynamic assurance capabilities with ML and AI. 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. In addition, ML is a key component in creating artificial intelligence, which enables applications to learn from their environments.

A data lake and streams architecture provide the ability to record, process and aggregate all the network data points that originate from the 5G network and the hosted applications. Applying data models and analytics algorithms to the aggregated data sets can generate actionable insights, which act as the core engine to drive network automation. Large sets of historical network data can be used as training input for ML algorithms, which can then be taught to spot patterns of degrading network performance and QoS. Remediation routines, such as capacity augmentation or auto-healing routines, can be triggered upon a threshold breach.

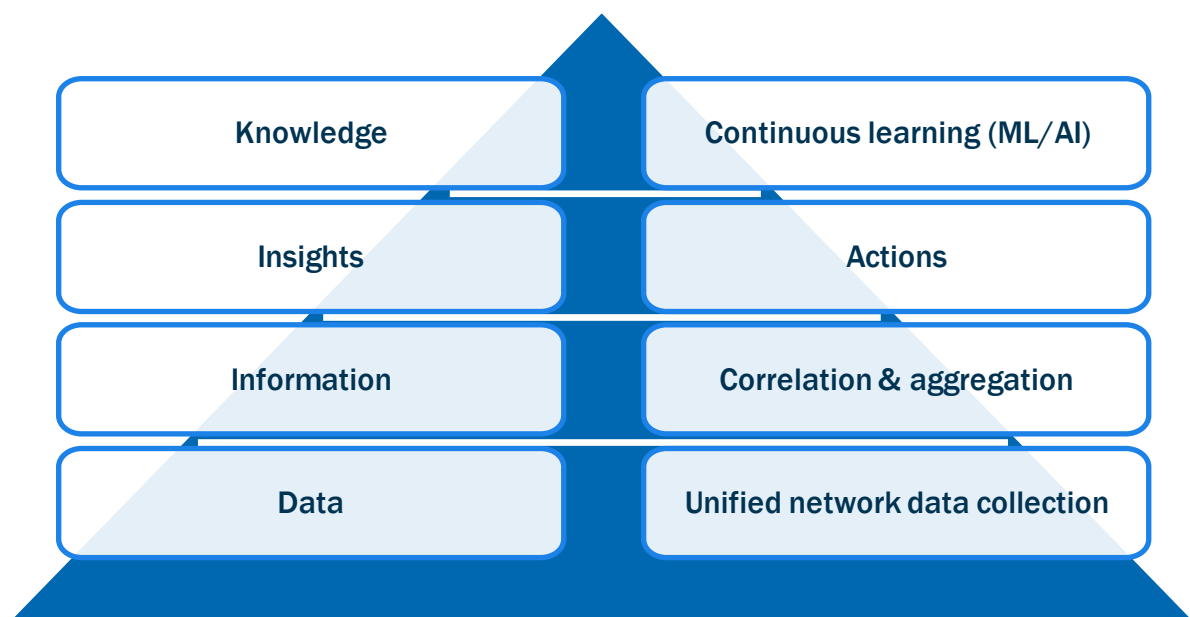
Continuous training and calibration of the ML algorithms can progressively increase the precision of pattern matching and remediation decisions, to a point where there is enough confidence to establish predictive

assurance. The ML models can predict network or service issues, hours, days or even weeks in advance, allowing sufficient time to plan and execute corrective action. Furthermore, the ML routines can be constantly notified of the quality of its decisions in a closed loop manner to increase the accuracy of its next actions (Figure 8). With increasing trust in automations, AI can be introduced to classify or label patterns, by employing grouping or clustering techniques to organise the real time network data to understand potential structures and patterns before predicting outcomes.

Operational automation is important for our global transformation program on zero touch. We are going to apply different AI techniques to solve problems in current 4G and FTTH networks and in future 5G networks (we are currently working in several use cases).

- Global Tier 1 CSP [2]

Figure 8: ML/AI based root-cause analysis



Source: Analysys Mason

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. 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.

Furthermore, real-time topology for assuring network slice-based services is extremely important because of the critical nature of the services that it supports. Poorly performing network slices can result in SLA breaches but, more importantly, can have a significant impact on enterprises and their customers. Therefore, assurance for network slice-based services must use a multi-dimensional real-time topology that captures the correlation between the physical layer, NFV and SDN layer and the network slice overlay.

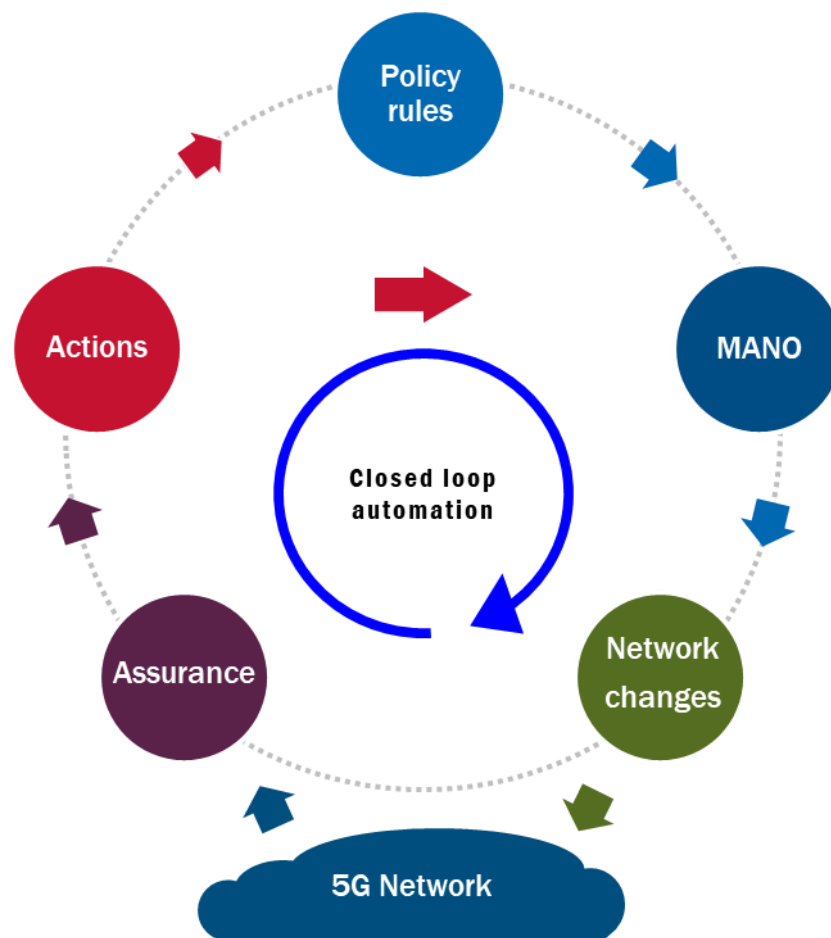
4.4 Assurance assisted closed-loop automation with MANO

The focus of 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, the operations personnel would analyse the outputs and manually execute a workflow of steps to identify the root causes of the performance and service degradation; most of this knowledge is either written in the form of standard operating procedures and runbooks, or, in many cases, is only known by the personnel in question. With the maturity of analytics and ML techniques, CSPs can now significantly increase the efficiency and efficacy of troubleshooting processes through automated root cause analysis. However, following through with the actions to rectify the network issues through configuration changes is altogether independent set of processes, usually executed as part of the change management process.

Closed-loop automation seamlessly integrates the two sets of processes (Figure 9). This level of network automation can be achieved by gaining the highest level of trust in automated root-cause analysis (discussed in section 4.3) and by establishing clear policy rules as network and service (and potentially customer experience) preconditions to trigger the configuration changes back into the network. The changes themselves will be executed through the MANO systems such as NFV orchestration, SDN control and multi-domain WAN configuration systems that are being deployed for the virtualised and cloud-native 5G networks.

Figure 9: Closed-loop assurance through MANO



Source: Analysys Mason

5. Automated assurance must be integrated into CSPs' chosen network automation platforms

The demands of the 5G era are triggering significant changes to the operational approaches to increase service agility and reduce the cost of operating and supporting the complex networks. At the heart of the new operational model for 5G is the network automation platform that will perform the function of automated network and service lifecycle management.

Leading CSPs are defining and building, and in some cases procuring, commercial network automation platforms. Open-source platforms such as Open Network Automation Platform (ONAP) are made up of disaggregated software components that combine design time operations (for example, service design automation) and run-time operations (for example, service orchestration, resource orchestration and automated closed-loop assurance), to deliver end-to-end automated operations.

In addition to The Linux Foundation's ONAP, many other industry organisations are promoting operational frameworks and best practices for network automation. ETSI's Open Source MANO (OSM) provides a framework for the management and network orchestration focusing mainly on the run-time operations. The TMForum's Zero-touch Orchestration, Operations and Management (ZOOM) initiative is developing best practices and open APIs for network automation, while the MEF's LSO initiative focuses on developing the specifications required to automate the entire lifecycle for services orchestrated across multiple provider networks and multiple technology domains within a provider network.

As established in section 4, automated assurance plays a vital role in operationalising 5G, but to achieve the overall benefits of service and business agility, and specifically, to bolster network automation, assurance systems must become an integral part of CSPs' preferred network automation platform and frameworks. By providing the actionable insights and actions to perform the operational tasks, assurance will drive the automation of the network and service lifecycle management. Some of these lifecycle management tasks include auto-healing of the network functions and service chains, and scaling of virtualised, cloud-native network functions and network slices.

6. Illustrative 5G use cases – the role of automated assurance

6.1 Long-distance 5G drones

Interest in drones for commercial services is growing significantly; Vodafone reported in 2018 that the market opportunity for drone-powered solutions would grow to USD84 billion by 2025.⁵ Such solutions will address a wide variety of use cases from mapping to inspection and photography, across many industry verticals. These use cases are beginning to emerge using 4G connectivity, but 5G is expected to further drive the adoption of these services.

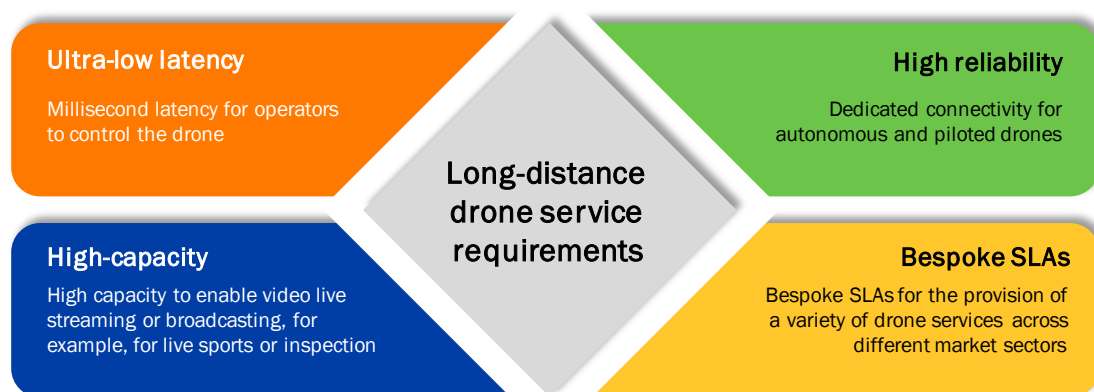
⁵ For more information, see www.vodafone.com/business/media/document/648_white_paper_drones.pdf.

5G capabilities will enable the long-distance and remote control of drones and provide connectivity to autonomous drones. Further, the guaranteed QoS and SLA provision from 5G will significantly improve the value proposition for these cellular connected drone services. Figure 10 illustrates the service requirements of the long-distance 5G drone services. Given the mobile nature of drones, network resources will need to be reallocated on demand to follow the drone. The network slice for that drone service, along with all assurance capabilities, must also dynamically adjust with the service to maintain the SLA and QoS as the network and topology change.

Operators have begun to trial and demonstrate the application of 5G for drone services, and Verizon has committed to becoming the first operator to have 1 million drones connected to its 5G network:

- AT&T has designed drones that can fly in all weather conditions to assist in disaster recovery efforts.⁶ One such drone carries a small cell and a series of antennas to provide emergency communications in areas of poor coverage or where network infrastructure has been damaged.
- BT, Ericsson and Verizon demonstrated how 5G-connected drones could be used in disaster and emergency situations to deliver emergency supplies and provide intelligence to response workers.⁷
- Vodafone has been exploring the opportunity for drone-as-a-service use cases as part of its IoT platform, covering the requirements from the connectivity provider and ecosystem partnerships.⁸

Figure 10: Service requirements for smart grid applications



Source: Analysys Mason

6.2 5G smart grids

Analysys Mason forecasts the number of wireless smart grid connections in 2018 to be 36 million and this will grow to over 250 million connections by 2026. Smart grid applications include a broad range of use cases deployed broadly across the national grid within power generation, transmission, distribution and consumption. Today, smart grid use cases are typically limited to equipment monitoring and fault reporting combined with smart metering to transmit consumption data. Dedicated physical networks are required for more advanced use cases where 4G mobile connectivity cannot guarantee the necessary performance and security. However, given

⁶ For more information, see https://about.att.com/innovationblog/extreme_connections

⁷ For more information, see www.ericsson.com/en/news/2018/2/case-study-bt-verizon-and-ericsson

⁸ For more information, see www.vodafone.com/business/news-and-insights/white-paper/the-rise-of-drones

the scale of national power grids, with thousands of sites containing equipment, physical networks can become unsustainable.

5G is expected to revolutionise smart grid applications by offering an alternative mobile technology that provides the necessary networking requirements and effectively scales with the national grid. 5G will also enable new solutions for emerging challenges, such as the future demand from electric vehicles, the disaggregation of micro-grids and the management of renewable sources. Research from Telefónica O2 identified the loss incurred from faults in the national grid and the growing demand from electric vehicles:

In 2015, the UK experienced 533 hours of blackouts, costing GBP23.4 billion in lost productivity. The UK's energy grid capacity will need to increase by 30% for the widescale adoption of electric vehicles to become a reality by 2040.

- Telefónica O2⁹

Telefónica O2's research highlights the application of 5G's mMTC capabilities and IoT for real-time monitoring and control of the grid, which can rapidly detect and respond to spikes in energy demand, such as charging electric vehicles on a national scale. Telefónica O2 suggests the economic benefits include the creation of micro-grids, small-scale power grids that operate independently or are synchronised to the national grid. This enhanced connectivity across national and micro-grids will improve competition and efficiency in the market, especially for unreliable renewable source such as wind farms, and more dynamic and transparent energy pricing for households. Other operators and vendors are similarly exploring the potential for 5G in smart grid applications:

- China Telecom, China's State Grid, and Huawei collaborated on the first project to explore 5G slicing for smart grid solutions. The project identified the 5G service features and technical requirements in various smart grid solutions.¹⁰
- Deutsche Telekom, the City of Dresden and the Dresden University of Technology to build a testbed for smarter energy grid management using 5G connectivity.¹¹
- Nokia and industry stakeholders ABB and Kalmar successfully demonstrated that 5G's URLLC capabilities fulfil the requirements for fault monitoring and resolution in power distribution networks.¹²

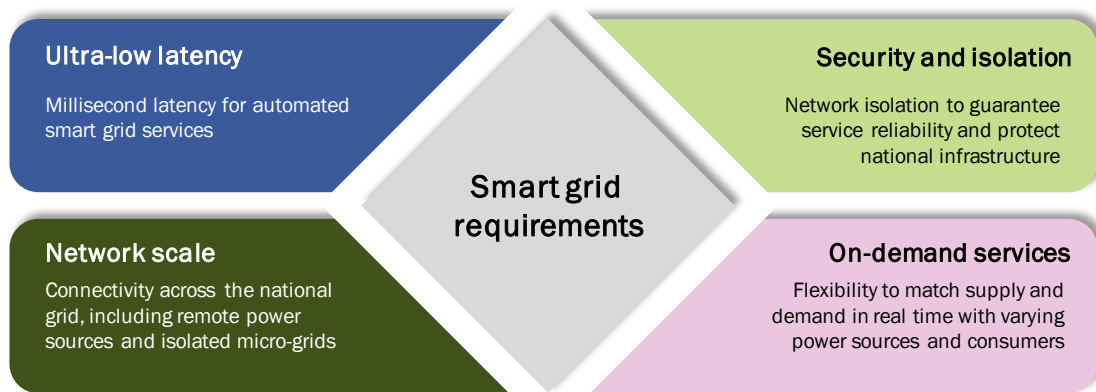
Further research also suggests advanced applications using grid data collected via 5G to provide accurate forecasting of electricity supply and demand, take a predictive approach to energy management, and employ automatic fault correction or self-healing grid solutions. Figure 11 illustrates the service requirements of the smart grid applications.

⁹ For more information, see www.mobileuk.org/cms-assets/O2%20Smart%20Cities.pdf.

¹⁰ For more information, see www.huawei.com/en/press-events/news/2018/1/the-worlds-first-5g-smart-grid-slicing-industry-report.

¹¹ For more information, see www.telekom.com/en/media/media-information/archive/greater-network-performance-advancing-5g-516112.

¹² For more information, see www.nokia.com/about-us/news/releases/2018/11/14/nokia-abb-and-kalmar-conduct-industrys-first-trial-with-ultra-reliable-low-latency-5g-technology-for-electricity-grid-and-harbor-automation/.

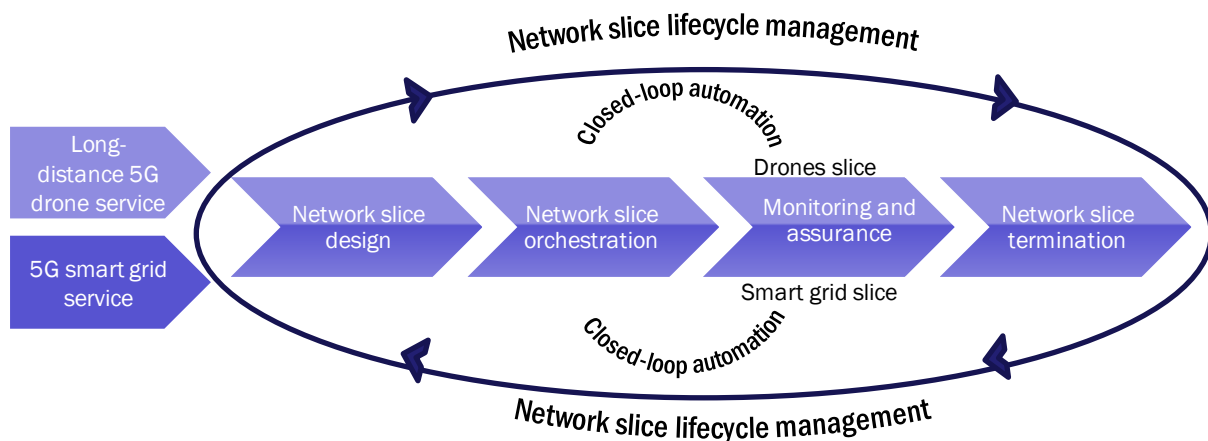
Figure 11: Service requirements for smart grid applications

Source: Analysys Mason

6.3 The role of automated assurance

5G connected drones will present very different connectivity requirements and SLAs compared to traditional mobile connections, or other basic IoT connections. Various long-distance drone services such as rapid delivery of emergency supplies and monitoring of critical infrastructure will require bespoke SLAs and QoS considerations. Consequently, assuring and monitoring the low-latency connectivity and the associated SLAs and QoS performance will be essential for long-distance or remote drone operators to guarantee service.

Similarly, the 5G-enabled smart grid services will require millisecond latency to effectively implement automated processes when responding to changes in energy demand or equipment faults. Additionally, high volume of data is expected from the power supply end points and distribution units, which is likely to require the mMTC capability. 5G-enabled smart grids will be a key component of the critical national infrastructure, which will require carrier-grade assurance and monitoring.

Figure 12: Assurance enabled network slice lifecycle management

Source: Analysys Mason

5G network slicing capability will be used to deliver the URLLC and mMTC requirements of these use cases. Network slice design, instantiation and orchestration, monitoring and assurance and slice termination are the key operational functions of the network slice lifecycle management (Figure 12). As explained in sections 4.2 and

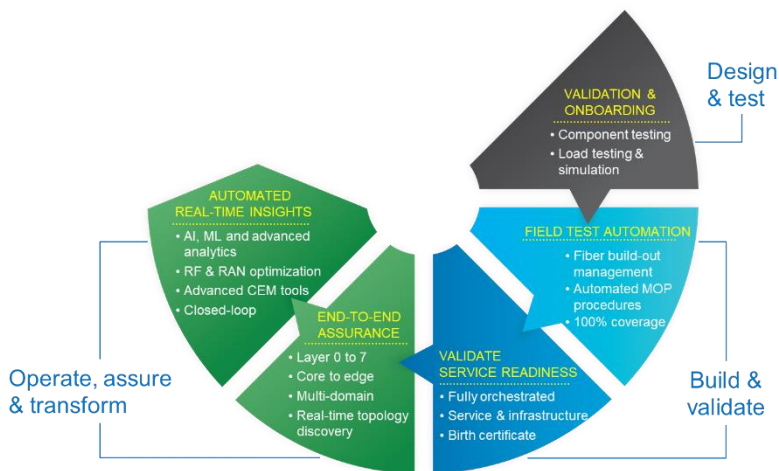
4.3, automated assurance must work in conjunction with orchestration systems to guarantee the SLAs and QoS of the services. This will be critical to perform the closed-loop automation based on the insights generated from monitoring the drone and smart grid services.

7. About EXFO's assurance-driven automation

As service providers continue the transformation of their networks to support 5G and the new services it enables, they are also driven to transform their operations tools and processes to address the increased agility, complexity and scale of these new networks. Automate everything, is the new mantra.

At the heart of any automation system is data, and in the case of 5G networks, this data comes from real-time network, service and subscriber assurance. But data alone does not really solve the challenge of complexity and scale; for this you require tools to make sense of the data. Machine learning and artificial intelligence to find issues, real-time topology discovery to keep track of the ever-changing network and services, combined advanced analytics to derive actionable insights. It is through this new assurance environment that operators gain real visibility into the virtual network. EXFO continues to evolve its assurance solutions to address this emerging reality – assembling a powerful suite of solutions to address network and service assurance, throughout the entire lifecycle.

Figure 13: Automation throughout the service lifecycle



Source: EXFO

EXFO's approach to assurance-driven automation is the 'vendor independence' of the assurance solution. Open network architectures will naturally have multiple-vendor VNFs operating within the same network, and possibly even on the same service. EXFO's service assurance solution:

- does not require customisation and is vendor independent by nature
- generates data consistently, regardless of VNF flavour
- automatically accounts for the dynamic SDN network
- supports service VNF swapping and upgrades
- adheres to open APIs for integration into standard operations environments.

Additionally, leveraging a 'big data' solution for network, service and subscriber data, enables advanced analytics for high-value solutions like customer experience management, customer usage patterns for targeted service bundles, network resource trending for capacity planning, and predictive and prescriptive assurance, which are fundamental goals of network automation.

To learn more about these network, service and subscriber assurance solutions, please visit:

www.exfo.com/en/solutions/communication-service-providers/service-assurance

8. Conclusion and recommendations

The network and operational complexity of 5G networks combined with the strategic need to achieve service agility and support new business models requires CSPs to implement high levels of network automation. Critical use cases that support multiple industry verticals will require real-time monitoring and automated healing techniques. NFV, CNC, SDN, edge clouds and network slicing technologies will enable the 5G network to be deployed as a network cloud platform enabling CSPs to rapidly compose and deliver new services. The 5G network cloud platform will transform CSPs into innovation enablers for vertical industries bolstering the B2B2C business model by allowing them to access the network cloud in a network-as-a-service model much like the infrastructure-as-a-service (IaaS) model that revolutionised the computing world.

To operationalise the complex 5G network at scale and support the diverse use cases and business models, CSPs must make automated assurance an integral part of their network automation strategy. Analysys Mason recommends that CSPs should:

- consider an automated assurance solution that supports unified monitoring of the 5G network from the cloud core to the subscriber or edge device, as well as support Layer 0-7 monitoring to guarantee service performance for enterprises and third parties that use the 5G network cloud as the platform for service innovation
- demand an assurance solution that rapidly adapts to the changing network and service conditions, providing real-time network slice-level assurance encompassing the validation of network slices upon activation and modification, and the ongoing monitoring of slices so CSPs can deliver on the contracted QoS and SLAs
- choose an assurance solution that incorporates ML/AI techniques to provide predictive assurance and automated root-cause analysis using real-time network and service topology, and network-slice topology
- use the insights and actions generated from the automated assurance systems to drive policy-driven closed-loop assurance in conjunction with their MANO systems
- choose an 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.

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 whitepaper was commissioned by EXFO. Analysys Mason does not endorse any of the vendor's products or services.

Analysys Mason's consulting and research are uniquely positioned

Analysys Mason is a trusted adviser on telecoms, 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 rigour
- develop innovative propositions to gain competitive advantage.

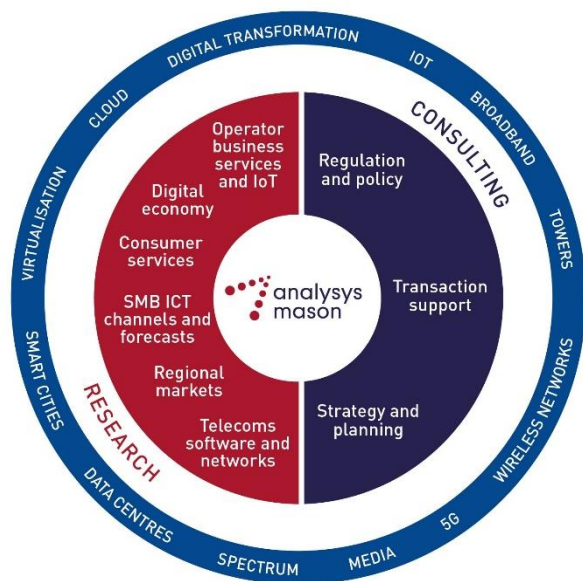
We have around 220 staff in 14 offices and are respected worldwide for the exceptional quality of our work, as well as our independence and flexibility in responding to client needs. For over 30 years, we have been helping clients in more than 110 countries to maximise their opportunities.

Consulting

- We deliver tangible benefits to clients across the telecoms 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.

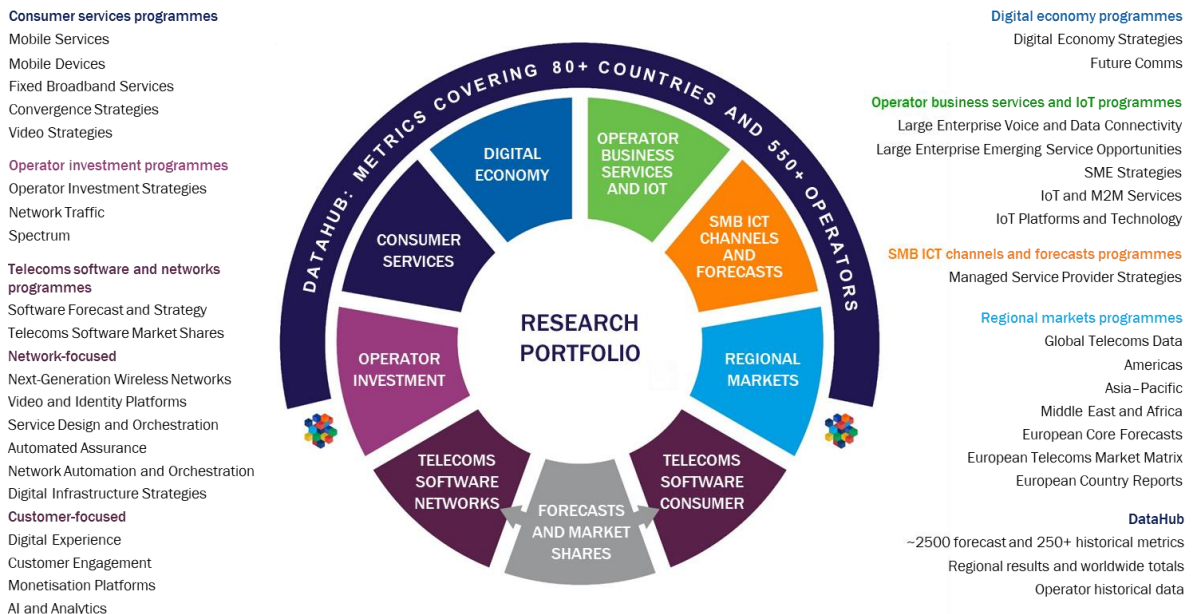


Research from Analysys Mason

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

The division consists of a specialised 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 programmes cover the following key areas.



Each subscription programme 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 standardised suite of research programmes, Analysys Mason's Custom Research team undertakes specialised, bespoke research projects for clients. The dedicated team offers tailored investigations and answers complex questions on markets, competitors and services with customised 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 telecoms, 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.