IDC

TECHNOLOGY SPOTLIGHT

Brought to You by VMware, Powered by IDC

5G services are changing how business does business. Automated operations, especially automated service assurance, are essential to successful 5G service delivery. Service assurance driven by artificial intelligence (AI) holds the keys to 5G services success.

AI-Driven Automated Service Assurance Is a Vital Link to 5G/MEC Business Success

May 2022

Written by: Karl Whitelock, Research Vice President, Communications Service Provider Operations and Monetization

Introduction

Transparency, always-on availability, procurement on demand, edge access, and high-level network performance are the service characteristics business customers want. In answer, multi-access edge computing (MEC) coupled with 5G standalone (SA) (often in the form of 5G SA network slicing) can address critical business needs in ways not previously possible. This capability is especially relevant for customers that want personalized preferences powered by the characteristic 5G service attributes of low latency, high throughput volume, and near gigabit speeds.

5G/MEC and 5G SA network slicing are truly game changing for customers, especially enterprise customers, in how they conduct business and in how they can provide value. 5G/MEC and 5G SA slicing are also bringing opportunity to communications service providers (SPs) through new delivery channels and solution offerings. However, the promises of 5G/MEC and 5G SA slicing will be realized only if the key communications SP business and operations processes are redirected from a network-only focus to a real-time "assured customer experience." Getting to this point means adopting the right systems that can satisfy the dynamic characteristics of business solutions with the flexibility to incorporate real-time machine learning (ML), analytics, and predictive responses to most work tasks. It also means that through 5G-enabled and customer-defined connectivity pathways (5G SA network slices), what was once the impossible becomes an everyday reality.

Estimates vary concerning the impact 5G can have on business, though a multitrillion-dollar global opportunity is forming for industries that embrace what "digital everything" can enable. Communications SPs stand to gain from this market swell but only if network management, service-level operations, customer experience processes, and monetization functions are tuned to regularly making unforgettable customer experiences.

AT A GLANCE

KEY TAKEAWAYS

- 5G/MEC and 5G SA network slicing complexity places service monitoring with SLA-based quality of service commitments into the realm of automated operations the likes of which have never been done before.
- Service assurance, especially network-driven customer experience management, integrated with service delivery as one end-to-end process is critical to 5G/MEC and 5G SA slicing success.
- Service assurance/service delivery and multifaceted partner interactions are essential for "frictionless" 5G-based B2B2x solution offerings.

5G/MEC Brings New Business Management and Operations Requirements

Outside the traditional approach of designing, delivering, and monitoring service performance, the 5G/MEC world and 5G SA slicing place an additional spin on each of these functions. This new focus means accommodating the real-time operational aspects of a personalizable network, maintaining flexible functionality to keep pace with rapidly changing customer/market conditions, and satisfying real-time configuration adjustments for meeting ongoing market demand. The following functional requirements — and their related questions — need attention before 5G/MEC and 5G SA network slicing can satisfy customer expectations at scale:

- **The assurance side of service ordering and fulfillment.** How will 5G/MEC and 5G SA network slice offerings be provisioned at scale? How will configuration changes be looped into the ordering, provisioning, catalog, and activation functions when service performance conditions based on a service-level agreement (SLA) deteriorate at the edge? At the core? Within the compositional layers of one or more network slices? How will partner resources (physical or logical or a combination) be defined and accounted for as part of the provisioning process? When real-time monitoring detects service performance slipping outside of quality-of-service (QoS) commitment levels, how will increased network capacity be configured and delivered without disturbing existing service offerings? How will this process be automated at scale when the number of 5G service implementations or slice instances grows from a handful to many? What parts of the fulfillment process need human involvement, and how can automation keep the fulfillment function continuously aligned with changing service performance conditions?

- **Customer experience management and service-level assurance.** How will service-level expectations of 5G/MEC and 5G SA slicing customers be monitored for QoS? How will latency expectations of 5G/MEC and 5G SA slicing services be maintained, especially if they are tied to an SLA-based contract? How will 5G/MEC sites be monitored? How will virtual network resources be managed at scale, especially as end-to-end service instances will likely contain a mix of both physical and virtual network assets? How will the viability of partner resources be maintained? If instances of assurance applications are implemented at each MEC site to maintain latency expectations, how will these apps synch back with a core assurance system to manage data integrity? Network slicing involves the radio access network (RAN) as well as the core and transport networks to form an end-to-end personalized virtual connectivity path that shares common infrastructure components with other slices and service offerings. How will each part of a network slice be monitored for end-to-end service integrity? How will intercarrier handoff of in-session data flows be maintained for slice parameter accuracy and SLA conformance? How will slice parameter accuracy and SLA conformance monitoring be achieved for intertechnology handoff when available, without data session interruption (e.g., 5G cellular to Wi-Fi or 5G cellular to LEO satellite handoff)?

Network slicing involves the radio access network (RAN) as well as the core and transport networks to form an end-to-end personalized virtual connectivity path that shares common infrastructure components with other slices and service offerings. How will each part of a network slice be monitored for end-to-end service integrity?

- **Service monetization and revenue accountability.** For most assurance and fulfillment issues, real-time charging combined with distributed policy becomes the control mechanism behind both the service delivery function and the customer experience function. As in prepaid billing processes, the network and billing functions work collectively to allow or disallow resource usage by a device or customer app. With 5G/MEC and 5G SA network slicing, the added challenge of partner resource utilization now plays a role, both in any B2B back-end service definitions and in front-end B2C customer engagements. This step, when combined with dynamically changing customer needs and roaming within a hybrid 4G/5G architecture, means that the monetization functions — rating, charging, billing, and notifications — need to simultaneously address multiple business models. Monetization and revenue accountability are important to note as a condition to be addressed when service composition changes based on service performance compared with SLA commitments to satisfy end-to-end QoS parameters.
- **Security.** Multipartner services with built-to-fit devices also play an important role with 5G networks. Due to the sheer volume of these devices, there is a growing probability that they will have minimal security protection or even no protection other than the default passwords defined during the manufacturing processes. In such cases, the accompanying business solution becomes highly vulnerable to exploitation. Massively connected, high-bandwidth devices expand the number of connected devices satisfying various business needs, opening the compromised device probability window beyond previous generations of mobile technology. This is especially concerning when coupled with the amount of open access points (e.g., MEC sites within the network itself).

The preceding list of operational challenges is not exhaustive. However, while the service assurance and customer experience functions are the focus of this document, addressing the provisioning and monetization needs of end-to-end service operations is no less important. In fact, all four functions — fulfillment, assurance, billing, and security — must work collectively and on a real-time basis and, in some cases, in a dynamic manner for the benefits of 5G/MEC and 5G SA network slicing to deliver on all the promises.

AI-Driven Assurance Is the Key to 5G Success

Service assurance is a core network process and will continue to be for a long time. The traditional functions of network fault management and performance monitoring are ingrained in the operations management strategy of every communications SP globally. These needs are one of the reasons why network operations and service operations centers exist. These centers of command and control are why automation of select assurance functions first began over three decades ago and why increasing levels of automation are necessary to maintain both network and service integrity as complexity increases from all sides — network technology, partner assets, and customer needs.

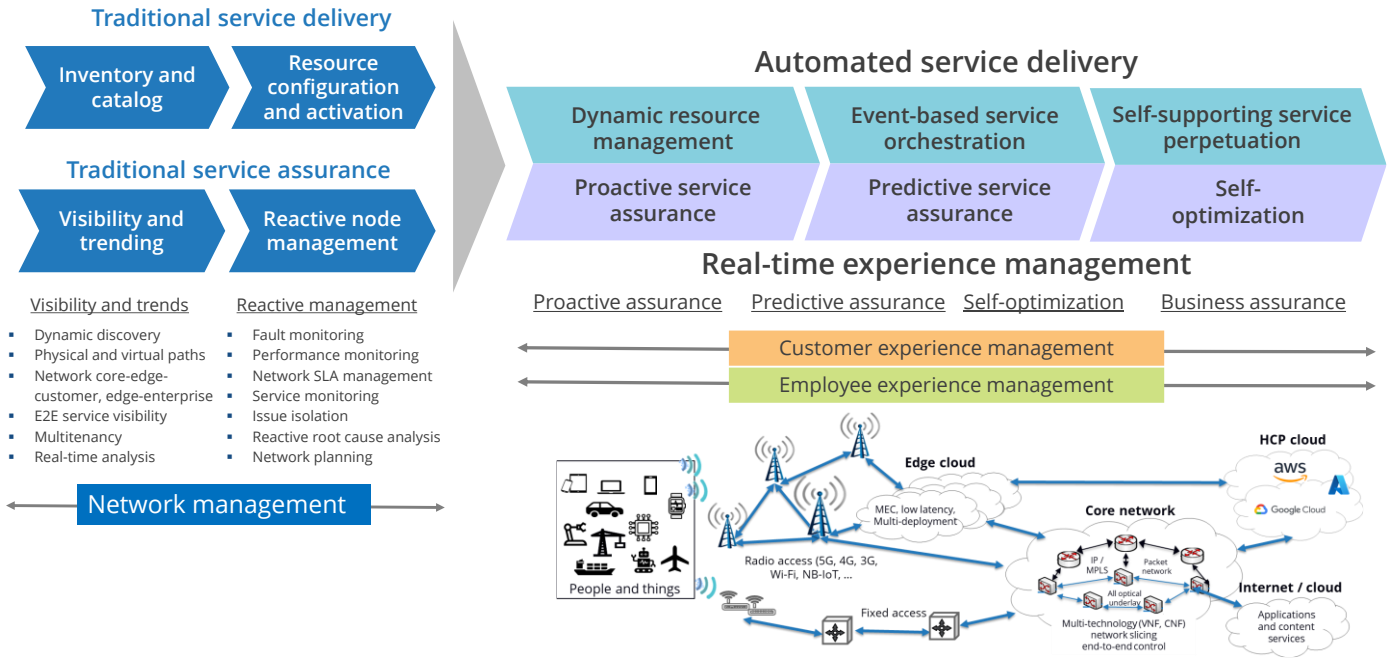
The demand for more insight at both the customer level and the network level is tantamount to measuring and managing the customer experience. In many ways, as Figure 1 shows, the assurance function must now be inextricably linked with the service fulfillment process to satisfy the real-time complexities that hybrid 4G/5G networks, 5G/MEC, and 5G SA network slicing bring to bear. For example, network latency thresholds from an assembly-line process or autonomous vehicle operations have very different technical needs and tolerance limits pertaining to how a low-latency, high-bandwidth, and ultra-fast 5G SA network slice needs to address

The assurance function must now be inextricably linked with the service fulfillment process to satisfy the real-time complexities that hybrid 4G/5G networks, 5G/MEC, and 5G SA network slicing bring to bear.

service design requirements. Regardless of how these tunable network performance parameters are managed, addressing the operational parameters of 5G/MEC services with associated network slice definitions as listed previously is essential for continuous end-to-end customer service availability and operability.

For a communications SP working with a MEC partner (e.g., hyperscaler cloud provider [HCP]), the density of connected Internet of Things (IoT) devices is expected to approach 1 million per square kilometer over the next few years. To meet latency requirements, the edge network connecting these devices will need hundreds if not thousands of MEC sites per operator. Whatever the number, MEC will grow as 5G deployment continues, business solutions proliferate, and device connectivity expands. In like manner, 5G SA network slices will greatly multiply over time and will also need considerable network and service monitoring attention.

FIGURE 1: ***5G SA Service Management Means Integrated Delivery and Assurance Processes***



Source: IDC, 2022

Business processes and network operations systems designed decades ago to support voice and messaging services were not created to satisfy the dynamic network and services environment that 5G SA slicing and 5G/MEC require. Concatenation of the service delivery and assurance processes along with new complexities from network slicing makes automated service assurance an addressable necessity in the 5G era, especially for managing E2E solution performance at or above service-level expectations.

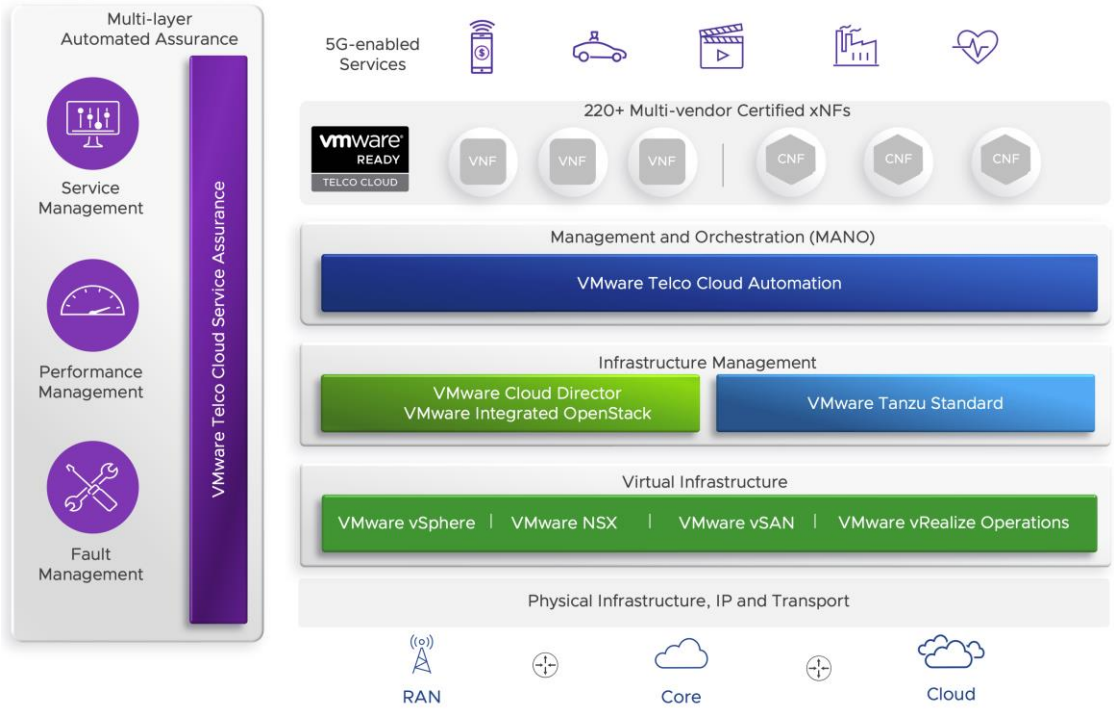
As customer needs expand, intelligent service-aware capabilities become a business necessity and are no longer a planning objective that will need to be satisfied after all 5G technical attributes are addressed. 5G advancement will continue as customer expectations and service design opportunities emerge with standards evolution and technology materialization. Significant effort must continue to be placed in the software systems needed to satisfy all new operations, orchestration, assurance, and monetization requirements that the services envisioned for these advanced network capabilities will need. Business success depends on it.

VMware Telco Cloud Service Assurance

VMware Telco Cloud Service Assurance is an automated service assurance solution with fault management, performance management, service management, root cause analysis, and service impact analysis capabilities packaged within a single platform. VMware Telco Cloud Service Assurance provides communications SPs and large enterprises with the operational intelligence needed to holistically manage complex multivendor virtual and physical environments, from the core to the edge to the RAN, all through a "single pane of glass."

As Figure 2 illustrates, the platform's customizable graphical interface enables network operations center (NOC) and service operations center (SOC) personnel to look at a graphical topology view for resolving and optimizing fault and network performance conditions relating to the network core and RAN. This insight can be used to identify the root cause of troubles, provide notifications and alerts, establish performance analytics, and report on service health. Such an approach to network fault and service-level performance enables communications SPs to track quality of service and quality of experience measures that in turn could be shared with customers.

FIGURE 2: ***VMware Telco Cloud Service Assurance: Cross-Domain Multilayer Assurance from Core to RAN***



Source: VMware, 2022

With 5G/MEC, high levels of network performance and availability make the need for real-time analysis a significant concern. VMware Telco Cloud Service Assurance addresses the complex assurance needs of business solutions through several design considerations and features, including:

- **Multitenancy.** Multitenancy gives communications SPs a flexible framework to group and report services, which enables them to define tenant users to access specific domains, metrics, events, and topology. This solution feature uses open source identity management capabilities.
- **Autodiscovery and network topology.** Autodiscovery queries devices and acquires needed data to map a communications SP's network from a variety of domains ranging from the infrastructure to service layers. It presents this data in a graphical network topology view. The system accomplishes this task through API integration and various networking protocols such as SNMP and HTTP.
- **Cross-domain visibility.** Communications SPs are provided with cross-domain visibility of complex, hybrid networks in a multivendor and multicloud environment. The range of view extends horizontally from core to edge to enterprise to RAN domains.
- **Multilayer fault and performance.** A multilayer fault and performance management view includes physical and virtual infrastructure, transport layers, virtualized and containerized network functions (VNFs/CNFs), applications, and services.
- **Performance analytics.** With topographical insight, VMware Telco Cloud Service Assurance uses AI and ML to define dynamic baselining and performance thresholding, anomaly detection, and correlation of performance management KPIs to preempt issues potentially affecting services and tenants. This is done while building a historical base and delivering notifications.
- **Unified data model.** The model includes a real-time collector framework to capture, filter, enrich, and transform data from multiple technology domains. Numerous collectors are available.
- **Root cause analysis.** Root cause analysis uses a model-based engine to connect problems with symptoms by traversing multilayered relationships that look for problem signatures or root cause. Given visibility into tenants, it can also rank alerts according to business impact, set priorities, and suppress extraneous alarms before providing notifications.
- **Service health and impact analysis.** Service health correlates cross-domain services with underlying infrastructure to present proactive service health and impact analysis using an automatic dashboard for service management reporting.
- **Configuration management.** Configuration management automatically discovers and backs up network device configurations. It maintains configuration alignment between physical infrastructure, virtual infrastructure, and containers as a service (CaaS). It provides compliance and policy management of network infrastructure.
- **Integration with VIM/CaaS Kubernetes and NFVO.** Integration of the VMware vRealize Operations and VMware Telco Cloud Automation enables both Kubernetes/NFVI cluster discovery and health, provides core VNF and RAN CNF connectivity, offers closed-loop automation, and can suggest remediations.

- **Closed-loop automation for network slicing.** VMware Telco Cloud Service Assurance together with VMware Telco Cloud Automation becomes a closed-loop automation and remediation solution for enabling communications SPs to improve operational efficiency and to reduce opex automation through faster response times. The solution also optimizes resource and workload requirements for meeting a surge of demand from edge and service requirements pertaining to a network slice.

An advantage of VMware Telco Cloud Service Assurance is the company's 20+ years of experience in integrated fault and performance management, plus the company's extended expertise and a full-stack product portfolio in virtual network, multicloud, 5G, and RAN environments.

Challenges

Automation Is Strategic in the 5G Era

Insight from data analysis provides guidance for how communications SPs can design and build 5G-based solutions that will change how industries do business. 5G/MEC is a game-changing combination that brings the enterprise edge and telecom cloud together. At the center of this effort are a communications SP's core systems tied to the service fulfillment, assurance, and monetization functions. The pathway to full automation of network operations is long, and the challenges in getting there are significant. However, 5G/MEC will be successful only if automation is incorporated effectively into day-to-day operations, especially within the service assurance domain, as network complexity continues to expand in multiple dimensions.

System and Process Transformation

Companies in various industries are adopting a digital services mindset in the way they conduct business. Getting to this level with 5G-powered network connectivity requires change at all levels, especially in how communications SPs work with customers. Systems and processes that were focused only on B2C sales must now incorporate B2B scenarios to meet market demand. Service offerings that favor a network connection with partner contributions and that can be delivered by a few keystrokes from within a self-care application are becoming the new level of customer expectation.

The real-time and dynamic nature of 5G technology, especially pertaining to 5G network slicing at scale and the E2E service needs of a 5G SA architecture with MEC, is a significant cause for concern when any integration is needed involving earlier-generation technology. Previously installed systems supporting the legacy networks were never designed to address multipartner contributions to a service definition, nor were they designed to meet the increasingly real-time and dynamic needs of services delivered via network slices or 5G/MEC. It is why working with legacy systems is so challenging when new network technology is involved. Transforming operations processes and the systems engaged in these processes will be difficult and will most likely require new systems for select functions such as inventory, catalog, orchestration, service assurance, and convergent charging.

Hybrid network services are still the norm today. The VMware Telco Cloud Service Assurance team should be mindful of how network insight must be blended with existing processes and systems to meet current service offering challenges. This is a difficult task to engage in, but it is a likely step to take while new network technology continues to be placed into service and existing network technology continues to deliver customer value. The more important long-term path o f providing advanced service assurance insight as part of a new systems environment designed to meet the needs of enhanced business processes is still the preferred path for satisfying 5G operational readiness objectives. However, a new systems architecture will not always be the option of choice taken by many within the global communications SP community.

Dynamic and Real-Time Network Operations

Existing systems and processes, including most currently defined data collection processes, were built on the premise that once a service is defined using installed network technology, the service will continue to operate in its designed condition for the technology life cycle. In this environment, change is difficult and support systems are hard pressed to meet demand. In many cases, communications SPs today are limping along with partially automated processes trying to address changing technology and business needs.

In the 5G world, several modes of operation are possible, especially as network slicing gains favorability and practicality among both communications SPs and their business customers. It is staggering to note the large number of configurable data levers that can be positioned along with the levels of automation needed to manage 5G slicing services, as well as the number of slices some communications SPs are projecting to place into service.

New systems to address this dynamic need are available, especially for the service provisioning, assurance, and monetization processes. The data collection and analysis function will touch each of these domains and will have several points to correlate as service operability changes with each shift in how customers derive value from the services they buy. In this complex environment, dynamic data analysis and service management will continue to be challenging tasks.

Conclusion

5G technology coupled with MEC is a game-changing opportunity for communications SPs that can effectively provide their business customers with a very low-latency connection combined with partner-provided edge compute and data storage capabilities. While so much has been promised about new customer demand and new revenue streams from 5G services, one thing remains certain: growing complexity. Advanced business management and network operations solutions that capture customer imaginations and that offer simplified ways for customers to control how personalized business solutions satisfy their needs mean behind-the-scenes network and systems interactions must work flawlessly and, in some cases, autonomously. Insight about network operations and customer experience must come together at the right time to provide the highest value. Accomplishing this goal means automated processes and the insight derived from real-time data analysis are now more important than at any other time in the past.

About the Analyst

Karl Whitelock, *Research Vice President, Communications Service Provider Operations and Monetization*

Karl Whitelock leads IDC's Communications Service Provider Operations and Monetization global practice. He offers strategic insight and global perspectives concerning service operations and monetization functions, formerly known as operational support systems/business support systems (OSS/BSS). His research areas include rating and charging, policy management, partner management, customer experience, revenue assurance, fraud management, service assurance, network data analytics, service orchestration, and network operations.

MESSAGE FROM THE SPONSOR

VMware Telco Cloud Service Assurance is a cross-domain, multi-layer automated assurance solution that enables CSPs to holistically monitor and manage their complex infrastructure and services, from the core to transport to the RAN. It reduces complexity for Network Operations Centers and Service Operations Centers by providing a single pane of glass for Fault Management, Performance Management, Service Management, Root Cause Analysis and Service Impact Analysis in a multi-vendor, multi-cloud environment.

VMware Telco Cloud Service Assurance increases multi-layer visibility, automation and remediation capabilities across physical and virtual infrastructure, network functions (VNFs and CNFs) and service layers. It improves operational efficiencies and suppresses extraneous alarms with automated root cause detection across domains. Operations teams can immediately prioritize resolution based on business and service impacts, thereby ensuring a high availability network that meets SLA requirements.

Together with VMware Telco Cloud Automation, our integrated solution provides closed-loop automation, remediation and assurance that enables CSPs to deliver superior quality of service and user experiences for mission-critical and low-latency 5G services.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com