CASE STUDY

Assurance in a 5G World

EXECUTIVE SUMMARY

The roll-out of 5G has expanded the breadth of assurance requirements. Although, automation of assurance to create the self-healing network is still some distance away, 5G is pushing forward deployment of intelligent issue identification, prediction, and automated root-cause analysis. There is also a new need for assurance products provided to enterprise customers to enable them to understand the performance of the multiplying 5G services that they will take from telcos. This expanding list of requirements will require the telco to work with an increasing number of assurance vendors and to expand the types of vendors they typically work with to include specialists in areas such as assurance for their enterprise customers.

INTRODUCTION

In recent research[1], the requirements of telcos for 5G assurance were investigated via discussions with 12 vendors creating assurance products. This paper summarizes two of the focus areas: 1) The new types of assurance needed in a 5G world, and 2) The likelihood that telcos will need additional types of assurance not provided by today's vendors. It then moves on to discuss how telcos should prepare for this diversity of assurance needs.

Charlotte Patrick, *Telecoms Industry Analyst*
Charlotte has 24 years of professional experience in strategy, marketing and finance. Most recently in the largest global technology analyst firm and previously two of the world's largest global telecommunications companies. She is an electronics graduate and MBA with excellent business analysis, commercial and strategic planning skills.

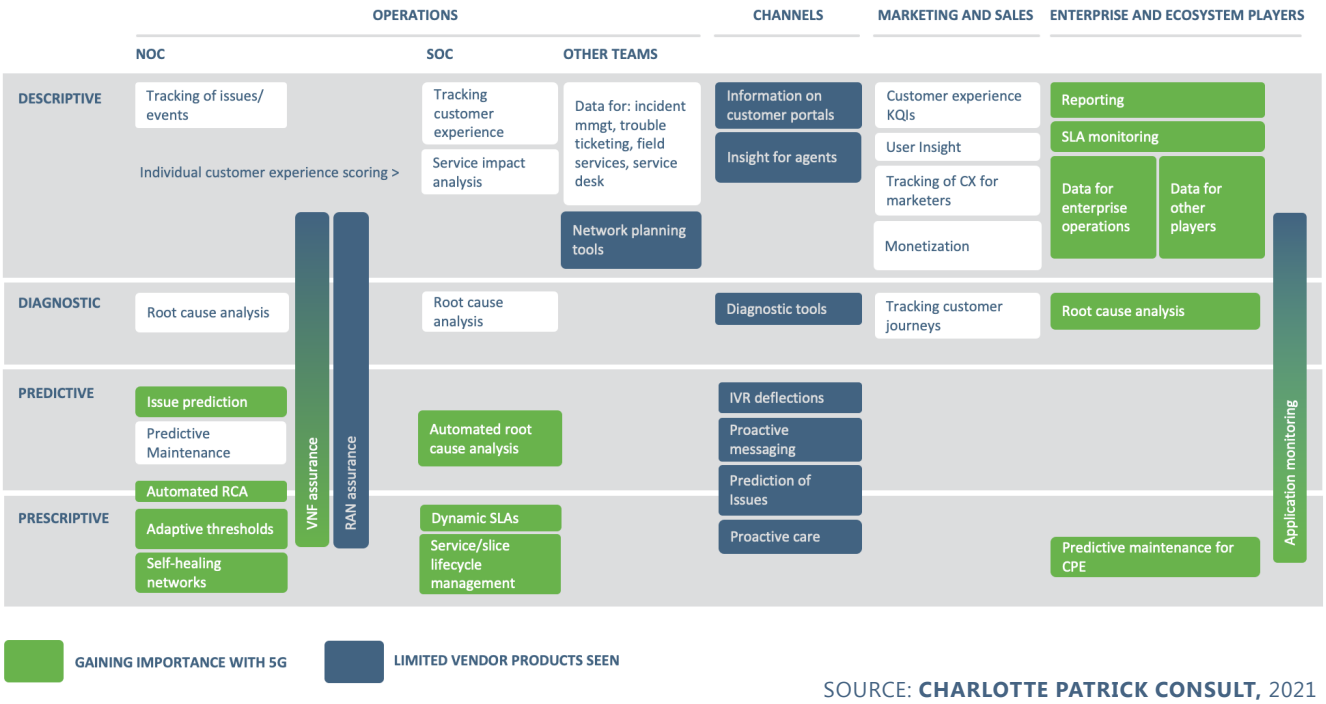
Chris Menier, *General Manager, VIA AIOps, Vitria Technology*
Chris Menier has more than 20 years of experience as an executive in the analytics space, with a focus on developing go-to-market strategies for early stage technology companies. He has an extensive background in industry-related technology with an emphasis on closed-loop automation, AIOps, machine learning, and big data.

[1] ASSURANCE NEEDS OF 5G, 2021; CHARLOTTE PATRICK CONSULT

Telco Assurance Requirements are Expanding

This diagram shows the breadth of uses for assurance data in the 5G world – split by the types of analytics needed (rows) and the teams requiring the data (columns). A description of the various boxes is provided in Appendix 1 at the bottom of this document.

FIGURE 1: 5G ASSURANCE FUNCTIONALITY



SOURCE: **CHARLOTTE PATRICK CONSULT,** 2021

The blue boxes show activities which increase in importance in a 5G network:

- Issue prediction, automated root cause analysis and adaptive thresholds for KPIs are not new - but more important due to hybrid networks and multiple new services
- Assurance of VNFs – including performance monitoring and fault management up and down the stack
- New requirements for RAN assurance including monitoring of service quality issues in the HetNet and capabilities to help assurance in instances of shared ownership between telcos
- Service/slice lifecycle management where assurance data is required within the design-deploy-assure activities of both services and slices

VITRIA

The green boxes highlight functionality which is not often included in the products of the 20 or so vendors tracked for recent research. VNF assurance and application monitoring are two non-traditional products which gain importance in 5G.

THE CHANGING NEEDS OF TELCO'S ENTERPRISE CUSTOMERS

The last columns for enterprise/ecosystem partners include a list of existing and newer requirements from third parties. Enterprise customers will require assurance of their telco services (for example private 5G networks for campuses, large office parks etc) and because private networks are “classic” telco services which are relatively easy for their sales teams to sell, this is likely to be one of the first “third party” 5G services needing assurance products. We therefore saw the provision of assurance products here gaining some traction with the vendors interviewed for this research. Seven out of the 12 had, at least, basic reporting products available. One vendor noted that enterprise customers were becoming more knowledgeable in wireless/radio technologies and networking due to the need for always-connected applications and services – leading to an expected increase in assurance needs.

5G assurance capabilities for enterprises include:

- SLA management providing quality of experience for end-users including latency, jitter, cloud infrastructure performance and RAN performance
- End to end, fine-grained application performance monitoring which maps to underlying network infrastructure
- The ability to understand whether issues are coming from the application or the network – and potentially the need to offer fault management in telco as-a-service offerings.

TELCOS WILL NEED TO USE AN INCREASING DIVERSITY OF VENDORS

Although there are benefits for telcos in using a limited number of vendors, the increasing diversity of use cases for assurance data is likely to require expertise from a larger rather than smaller number of vendors. Figure 2 demonstrates that “pockets” of capabilities will be developed by vendors wishing to play in the 5G assurance space. In summary:

- The left-hand column moves from traditional performance/fault monitoring to closed-loop self-healing networks.This is the natural place for existing network assurance vendors – although, smaller players will need to message against the bundling of assurance capabilities into larger network-equipment provider deals.

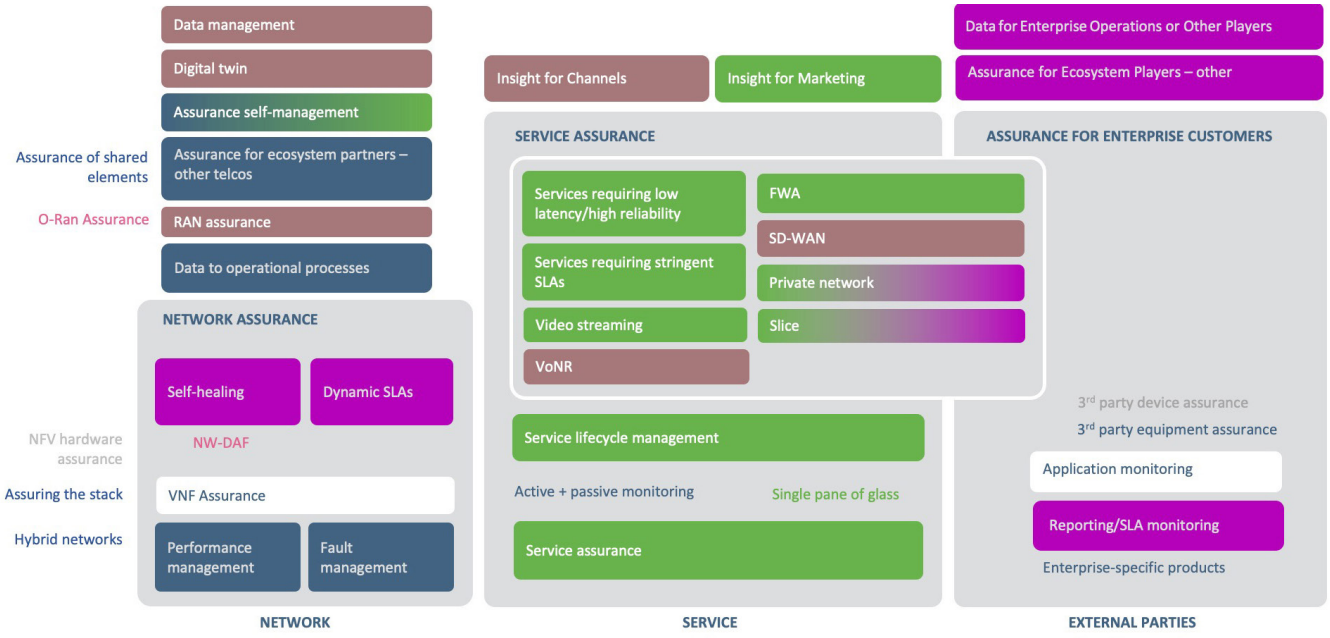
- Going up the column, there are several new capabilities which will be seen from these existing vendors. Although, there are some very new or niche capabilities in the pink coloured boxes which are likely to be available only from particular subsets of more specialist or sophisticated vendors.

- The middle column includes all existing service assurance but demonstrates the additional complexity of assuring new 5G services. All services will require a specific set of measurements for the telco – but could also require an enterprise-focused assurance product to be developed. Enterprise customers are thought to most likely require assurance around private network and slices.

- The green boxes in the middle column demonstrate a couple of areas where requirements are quite specific and, here, only certain vendors have previously chosen to create products – it is likely that these will remain as capabilities that telcos will need to source from these vendors, given the amount of new capabilities that are generally needed around 5G.

- The area of enterprise-assurance provided to parties outside of the telco (final column) will be one that interests several different telco-specific and non-telco-specific vendors (including those in the traditional AIOps space). There are benefits and drawbacks to entering this market for these vendors; but it does offer the opportunity of selling to enterprises directly if telcos are successful with their 5G/edge services.

FIGURE 2: CREATION OF "POCKETS" OF VENDOR ASSURANCE CAPABILITIES



SOURCE: **CHARLOTTE PATRICK CONSULT,** 2021

The colourings seek to group together 5 “pockets” of vendor capabilities.

DEFINING EACH CAPABILITY SET:

Assurance products in blue are focused on dealing with the complexity of hybrid networks and new stacks – and working towards closed-loop automation. The area currently has a mix of vendors - but NEPs are taking a good amount of business in the early days – bundling assurance with service design/orchestration. Challengers will provide niche analytics and machine learning to compete; plus, the ability to integrate with multiple vendors and work with various orchestrators.

Vendor products here are focussed on assuring a range of 5G services with the need for closed-loop automations in the service lifecycle. It is assumed that boxes in green on the diagram will be most attractive to existing assurance vendors as they require capabilities which are variations on their products sets. As previously, some of the boxes are a mix of green and purple – because they are more likely to need both products for the telco and for enterprise customers.

The pink boxes include a group of capabilities requiring specific skill sets:

- Some are already mature markets with existing specialist products which will need to be further developed for 5G – for example, RAN assurance and products for the contact centre using assurance data. These are likely to remain the domain of existing vendors – especially if the vendor has developed specialist data and analytics skills
- There are then a group of new capabilities (data management, digital twin, NW-DAF) which could see entry from several different vendors if capabilities augment their existing product set
- There are then a couple (SD-WAN and VoNR assurance) which require specific capabilities, and which may be something that only a few vendors choose to create.

Here, vendors will require new capabilities to assure hardware and software on telco or customer equipment to understand whether the issue is on the equipment or the network. This functionality is already developed/ being developed by parties such as the AIOps vendors and the hyperscalers. Application monitoring is also a necessary part of assurance in 5G/edge but has many existing specialist vendors.

Products focussed on enterprise customer assurance which may be sold directly to the telco, through the telco or directly to the enterprise. Most enterprise requirements should be subsets of vendor products but the purchasing parties in the telco/enterprise are different, and the market is nascent requiring emergence of successful telco 5G services and products at the edge.

VITRIA

How can Telcos Prepare for 5G Assurance?

Going back to Figure 2, telcos are already expanding their assurance capabilities in the network area (blue boxes). This expansion is held back by the need for more sophisticated capabilities (as shown at the top of Figure 2) and the need for orchestration capabilities from 5GSA. There are some moves seen in the service assurance space (green boxes) – however, these are typically waiting on telco's success in selling 5G services to generate a weight of requirements. Certain of the specialist requirements in pink
boxes are being rolled out (RAN assurance) but some are more niche or less well developed and will become available more slowly. There are then simple requirements delivered in the purple enterprise area, again waiting for a weight of requirements as 5G services become mainstream.

THE ACTIONS NEEDED FROM TELCOS AS THEIR 5G ROLL-OUT CONTINUES INCLUDE:

- Discussions with teams beyond networks about their requirements – particularly the product managers in marketing around the realistic opportunity of offering enterprise-focussed assurance.

- Agreement amongst stakeholders on the types of vendors that might be able to deliver new requirements:

    > Do those with the most understanding of the enterprise (eg. traditional AIOps vendors) really have the scale and flexibility to handle telco deployments?

    > Do network-focussed vendors have the knowledge of enterprise requirements and the background of working with the diversity of needs?

VITRIA

VIA AIOPS

The deployment of 5G and creation of a hybrid network environment generates significantly more data to be analyzed and multiple new assurance needs as reviewed in this paper. 5G providers and enterprises implementing private 5G networks must be able to rapidly identify faults and performance issues across service layers. Addressing and resolving service-impacting problems before subscriber impact is crucial in sustaining customer experience expectations. AIOps solutions bring more real-time analytics, machine learning and automation to detect and understand issues as well as enable the implementation of more automation in remediation and automated response.

VIA AIOps by Vitria is an end-to-end service assurance application with the following key features and capabilities.

Full stack observability provides the right information on a timely basis to the right people to improve their efficiency and effectiveness. Persona-based views are delivered through an intuitive and dynamic UI. Views and dashboards are generated based on the data, saving staff development time.

AI, machine learning, and advanced analytics reduce alert volume, detect service-impacting issues earlier, and distinguish symptoms from root cause across the technology stack and operational silos. VIA automatically determines the correct algorithm to use on collected data to generate baselines and detect signals. This enables operations teams to focus their attention only on the anomalies requiring action. False positives and true negatives are filtered out, improving operator effectiveness, and reducing operator fatigue from excessive alert volumes. Continuous learning sustains optimal baselines across billions of dimensions and metrics with dynamic baseline changes as new data is collected.

Real-time analytic pipeline collects, enriches, and analyzes streaming data in real time and delivers dynamic analysis and root cause identification across vertical and horizontal applications and workload layers.

Unified data collection supports the optimization of fault, performance, and change management processes and can be used for both traditional in-house and cloud-based application environments.

Open Core Foundation enables integration with existing service management and monitoring systems. Integration allows VIA AIOps to prescribe actions to these systems, including opening, closing, or updating a ticket, engaging the right fix agent, and notifying teams of the symptoms and probable causes of the event.

VIA now has a partnership with Cisco. Cisco reports that they chose VIA as their AIOps vendor based on their proven ability to tightly integrate with their offering, their agility to ingest and analyze data, and support massive scale infrastructures.

VITRIA

APPENDIX 1: DEFINITION OF BOXES IN FIGURE 1

Column	Diagram Box Name	Detailed Description
NOC	Tracking of issues/ events	Tracking specific topics in order to report or initiate alarms. In more complex hybrid networks, this includes understanding issues across domains and layers. Problems tracked can be broad and include illegal or excessive network usage, off-network issues (e.g. CPU problems of enterprise customers), customers issues as they move between countries. This tracking can be benchmarked against peers.
	Individual customer experience scoring	A single score per customer created by combining service assurance measurements – can be used for network planning and management, marketing and in the contact centre. Scoring may focus on particular services of importance to the telco.
	Root cause analysis	Analytics to understand common problems, understand "unknown unknowns" by correlating data sources and look for commonalities across systems in order to diagnose more complex issues. Insight is used to understand issues, how they affect customers and improve the prioritization of work done to resolve them.
	Issue prediction	Use of machine learning to understand issues and predict future issues with network, services, apps and device. trend and anomaly scores, seasonal.
	Predictive maintenance	Use of machine learning to understand issues with network equipment and alert operational staff or raise ticket.
	Automated root cause analysis	Automated incident detection, decision on importance of issue and sending of guidance to network or other systems for resolution.
	Adaptive thresholds	The use of ML to track network KPIs over time and "understand" what an appropriate level might be for particular times of day or for particular known situations on the network. Thresholds for alarms are then set dependent on these revised KPIs.
	Self-healing networks	General term for complete automation of problem resolution where assurance data feeds closed-loop systems using ML to understand issues and prescribe resolution.
	VNF assurance	Fault and performance monitoring of multi-vendor VNFs – including monitoring of VNF spin-up/down time, availability, inter-VNF latency and packet loss – also, view of vertical stack performance. Allows end-to end service modelling, creation of real-time topology models.
	RAN assurance	RF monitoring tools ensure that cells deliver expected latency, bandwidth, and connectivity; also optimizing cells as traffic patterns and topology change. Provision of end-to-end dynamic view of network topology, services, customer dependencies. Monitoring for quality issues from attenuation and interference from HetNet. In cases of shared ownership, observes the telco's own subscriber experience/RAN performance or observe traffic across the shared network.
SOC	Tracking customer experience	Reporting and alarming when issues seen. Can be about network (3G,4G,5G,roaming), services (video, content, VoLTE, voice, data), device (mobile, STB, peripherals) or OTT services (apps, websites). Reporting often segments customers to better understand those with particular needs or those that are most important to the telco. Correlates network and service degradation with customer experience issues.
	Service impact analysis	Assesses service impact of network-related issues (network alarms, KQIs, TCA alarms and service topology etc).

Column	Diagram Box Name	Detailed Description
SOC	Root cause analysis	Analytics to understand service issues, including correlation of these issues with underlying network (or other end user equipment such as the MEC) issues. Insight is used to understand issues, how they affect customers and improve the prioritization of work done to resolve them.
	Automated root cause analysis	Automated detection of service degradation, decision on importance of issue and sending of guidance to network or other systems for resolution.
	Dynamic SLAs	Monitoring for assurance of each enterprise service: calculates minimum amount of resources needed under low, normal peak workloads to meet SLAs. Assurance then provides orchestrator with any changes needed to meet these SLAs and also predicts expected peak needs to allow resource management ahead of time.
	Service/slice lifecycle mmgt	Inclusion of assurance data within the design-deploy-assure activities of both services and slices.
Other Teams	Dated to other teams	Information and triggers related to issues arising on the network, devices, apps and services sent to trouble ticketing, alarm management, field services and other operational units.
	Network planning tools	Inclusion of assurance data on customer experience into planning tools to provide additional granularity. Data such as customer value from billing data also added. May include "individual customer experience scores" going forward.
Channels	Information on customer portals	Information about network or service affecting issues provided on customer portals (eg, web, mobile or as part of chatbot roll outs)
	Insight for agents	Insight from network and other data to improve troubleshooting capabilities of Level 1, 2 and 3 agents. Answers questions such as "what is responsible for the customer's issue?" Provides details of the issue including root cause and tracking of particular events.
	Diagnostic tools	Tools on customer portals and mobile apps that allow customers to run checks - enabling possible causes of problems to be understood. This can include providing analysis to interfaces such as chat bots or social media.
	IVR deflections	Creation of messages or routing in the IVR dependent on the status of the network and services.
	Proactive messaging	Provision of a message pushed to a customer when a customer-experience effecting issue occurs, for example, a network outage in their area. This can be integrally linked with more prescriptive actions below.
	Prediction of Issues	The prediction of issues from assurance and CRM data (e.g. there is a network fault and the last time it occurred it created a significant volume of traffic to the contact centre). Prescriptive actions are sent to humans or machines.
	Proactive care	The creation of more personalized and/or prescriptive customer engagements. Care history, products purchased and other insight used to provide better interactions with agents; or predict issue and create workflow and tickets to field services, operations teams, etc. Assurance data is one feed which can be used.

APPENDIX 1: CONT'D

Column	Diagram Box Name	Detailed Description
Marketing	Customer experience KQIs	View of customer's experience and achievement against targets. May use mapping to show geographic issues and bring in data from other sources such as customer value from billing data. Customers may be segmented based on needs (e.g. gaming customers).
	User insight	Assurance data provided to marketing to improve their understanding of customer usage of digital services. Insights can be customer-centric and at a group or individual level. Can be used in analysis of competitive threats.
	Tracking of customer experience for marketers	Specific tracking for marketers – including CX of devices for the device team or particular services for product managers involved in launching new products. OTT services also tracked for discussions/negotiations with OTT players. Can include ML to identify churn risk/upsell potential/customer support needs.
	Monetization	Monetizing customer insight by using predicative algorithms to understand what the customer might do next and offering a product.
	Tracking customer journeys	Data sets for looking at customer journeys on the network or with devices, apps or services.
Enterprise and Ecosystem Players	Reporting	Enterprise-specific performance monitoring for services such as VPNs. May include application monitoring of performance of equipment managed by the telco. If reporting is for ecosystem partners, may include insight such as RAN assurance.
	SLA Monitoring	On-demand reporting for monitoring of SLAs and management of issues arising. More sophisticated tools allow creation of flexible parameters for warning/violation, excluding things such as maintenance periods or historic/active alarms.
	Data to enterprise operations	This is a catch-all category – where assurance data is provided to customer systems, for example, via API to their own assurance tools or into other systems such as trouble ticketing, their contact centre or alarm management.
	Data to managed service players	In more complex ecosystems, where enterprise customers use managed service partners, assurance data may need to go to them rather than directly to the enterprise.
	Root cause analysis	Analytics to understand issues, provided directly to enterprise customers.
	Proactive maintenance on customer premise equipment	Prediction of potential future issues for customer CPE – could create trouble ticket for telco's field services, account management or provides automated response addressing the issue before it occurs.
	Application monitoring	Monitoring tools for application usage, availability and response time metrics. Provides details of location of errors in the network or stack and root cause analysis. Will include automations and predictive capabilities. May require automated identification of apps and correlation with slices, private networks etc to correctly understand issue.