RADCOM

AUTOMATED ASSURANCE FOR CLOSED-LOOP NETWORK OPERATIONS

OCT 2022

Prepared by:

TECKNEXUS

INTRODUCTION

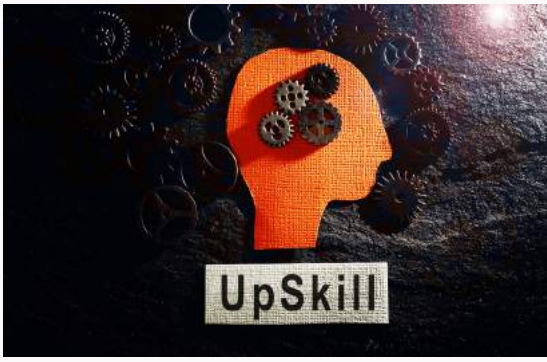
Industry digitalization has created new growth opportunities within the highly competitive telecoms market. Communication Service Providers (CSPs), in order to maximize their revenue potential in the value chain, are moving towards cloud-native technologies, including 5G technology, and introducing new services to consumers and enterprise segments.

The introduction of 5G, coupled with cloudification and open standards, also comes with its own set of challenges, such as:

- Transforming the workforce's skillsets to move to a more efficient and streamlined approach to managing network operations
- Isolation and troubleshooting of network degradations
- Prediction of service-impacting events, even before they affect subscribers
- RAN and core virtualization
- Hybrid cloud computing (managing the 5G SA core, as well as managing legacy networks)
- Maintaining a network of diverse vendors
- Securing the new breed of network architecture from threats

The emergence of the above challenges has made it imperative that CSPs focus on automation to stay agile and ahead, in order to maintain a competitive edge.

Before CSPs take a plunge into the automation journey, they must understand that this journey is complex, comes with a cost, and is driven by the business needs and issues it has to resolve.



RADCOM

BUSINESS DRIVERS
FOR AUTOMATED ASSURANCE AND CLOSED-LOOP NETWORK OPERATIONS

With the emergence of 5G, closed-loop automation has become critical. With networks becoming even more complex and consumer demands high, a customer-focused approach is required for managing network operations.

Let us take a deep dive into the business drivers for automated assurance and closed-loop network operations.

✓ 5G, Open RAN, and Cloud RAN

There is little doubt that virtualization comes with its own benefits, but the real payoff happens when virtualization can radically alter the economics of network infrastructure. With virtualization, the network architecture has become complex, and the economic benefit is entirely dependent on automation and intelligence to guide that automation.

The transition of networks from 4G to 5G will be complex and costly. There will be heavy investment by CSPs to procure 5G network equipment, enabling new use cases such as private networks and slicing, which will open up the market for both B2B and B2C segments. Maintaining the revenue stream for such diverse use cases will mean process re-engineering in terms of which networks are maintained. 5G will also bring in a larger number of cell sites for ubiquitous coverage.

Automation driven by real-time data from automated assurance will help in maintaining these cell sites more efficiently. If AI/ML is then applied by service assurance, CSPs can utilize automated anomaly detection to manage and optimize cell sites more automatically.

✓ Match customer experience and expectations

With the introduction of 5G and private networks, CSPs now not only need to compete with existing CSPs, but also with other technologies like WiFi. Existing automation caters to maintaining routine KPIs and fault correction from customer care offices.

But now, there is a seismic shift in the customer's expectations. With product offerings from CSPs in B2C and B2B market segments becoming homogenous, customers are not only interested in the products themselves but also the experience that differentiates the products from similar ones.

In these circumstances, it's the customer experience that enhances and retains the customers. To meet these changing demands, CSPs must plan for implementing closed-loop automation in their network.

This will play an important role in monitoring the KPIs, proactively predicting any faults, and triggering preventive maintenance.

In addition, focusing multi-level analytics on customer interactions, offering tailor-made plans, and providing insights across multiple services (such as video streaming and messaging) will help devise the best action plan for resolution, retention, and sales offers.

All this can take shape and mature if there is a high-end closed-loop automated system that will provide a cohesive customer experience that is proactive and unified. This will ensure revenue growth for the CSPs and will also help in reducing customer churn.

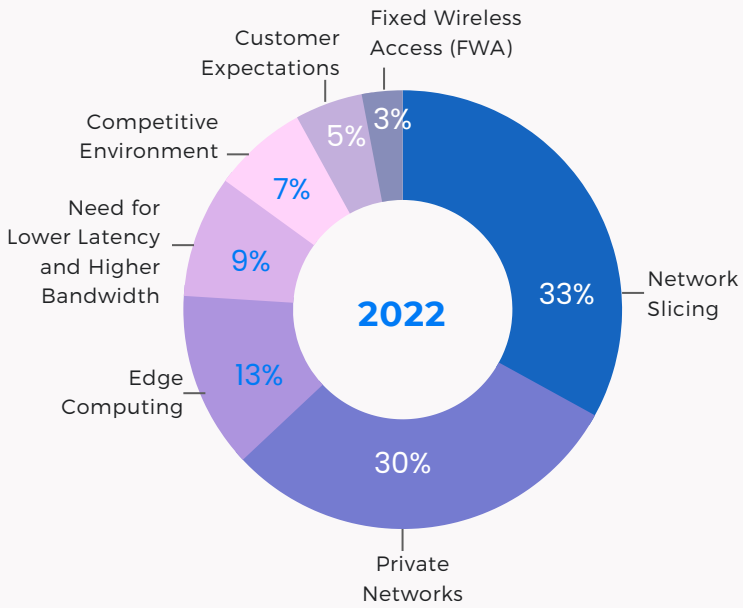
End-to-end monitoring from the RAN to the core (91%) and utilizing AI/ML to find network anomalies (83%) were the top two service assurance methodologies that organizations will be using to ensure the customer experience in 5G as per our recent survey of CSPs who have already launched or are in the process of rolling-out 5G services.

RADCOM

✓ Implementation of Network Slicing

Network slicing enables operators to dynamically divide the network into multiple virtual slices, with the ability to optimize each slice for a target application or service. For example, one slice might be for mission-critical services requiring constant connectivity, whereas another might be for video streaming requiring high capacity.

For CSPs to deliver guaranteed SLAs per slice to their enterprise customers, automation and service assurance are required.



✓ Be Future Ready

The aggressive way in which networks are transforming, being agile and future-ready, is now the “new normal” for CSPs. They should have flexible platforms supporting new standards and emerging technologies.

The best way is to have a network programmed to handle all eventualities, i.e., deliver on the promise of self-healing networks with closed-loop automation and automated assurance.

Network slicing is one of the top business drivers for standalone 5G deployments followed by private networks, according to our recent survey of CSPs who have already launched or are in the process of rolling-out 5G services.

HOW CAN CSPs ADDRESS BUSINESS NEEDS AND CHALLENGES?

Legacy service assurance systems deployed in existing networks are highly centralized. They cater to reactive faults based on fault and performance events.

The data generated by events are monitored in the Network Operating Center (NOC), where remedial actions like Root Cause Analysis (RCA) and trouble tickets are raised.

CSPs have made efforts and have introduced some automation, but these systems still lack real-time and predictive capabilities.

With 5G and cloudification, the new service assurance systems must have traits of low latency, real-time, dynamic, and distributed capabilities. In addition, these systems should have the functionality of continuous monitoring and predicting proactive actions using advanced analytics.

Service assurance for any CSP needs to be based on the framework below:

- **OBSERVABILITY**
  It will help CSPs to visualize and analyze real-time telemetry from a more complex, software-defined infrastructure.
- **AUTOMATION**
  Able to rapidly create and operationalize automatic analysis and task completion. AI and ML are going to be an integral component of automation.
- **SCALABILITY**
  A cloud-native design that scales smoothly as data volume increases.
- **CLOUD PLATFORM**
  A common foundation that will ensure the transition from today's network to more autonomous networks of the future.
- **MEANINGFUL DATA**
  Using the data generated from networks to create actionable insights in order to trigger preemptive and proactive actions.
- **INTEGRATION**
  Be ready for this new mode of service assurance to integrate with existing interfaces aligned with 3GPP and open standards.

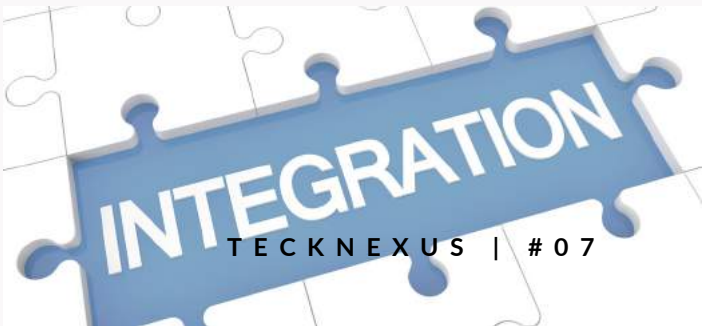
The CSP can devise a solution for implementing a service assurance model based on closed-loop automation using the framework mentioned above. These can help CSPs give customers a new dimension of experience and be agile to cater to future eventualities.

The way CSPs are making the transition in service assurance, is by slowly moving from an environment of open-loop automation to closed-loop automation.

In this context, CSPs will constantly assess to see if there is an issue or an error in the network, and implementing a closed-loop system can trigger proactive actions to mitigate the issues before adversely impacting the customers.

Closed-loop automation is an overseeing eye of a network's automation and management capabilities. The loop here refers to the numerous communications feedback between monitoring, reporting, optimizing, and calibrating the network's performance. This solution is paving the way for a self-optimized network.

Network Data Analytics Function (NWDAF) will be implemented by around 70% of CSPs in the next 24 months, which is critical for enabling closed-loop network operations and automated assurance. This is according to our recent survey of CSPs who have already launched or are in the process of rolling out 5G services.



RADCOM

BENEFITS OF AUTOMATED ASSURANCE FOR CLOSED-LOOP NETWORK OPERATIONS

Below are the key benefits that automated assurance for closed-loop bring to the CSP's network operations:

Service assurance challenges faced by CSPs	Solution provided by Closed-Loop Automation (CLA)
The operational expense for capacity expansion	CLA can automatically take care of capacity expansion by sensing congestion in the network.
Quality of experience in business-critical operations	CLA prioritizes use cases based on configured traffic shaping. An example is network slicing.
Allocating resources for 5G	CLA plays a critical role in scheduling resources for 5G services.
Customer experience in the IoT world	With 5G, the number of IoT devices will be high and will mean the transition of user plane services towards the edge. CLA being a distributed automation function, will help secure the quality experience.
Fraudulent transactions	CLA ensures agile policies are deployed, which can restrict fraud.

The rapid adoption of 5G across geographies will mean an explosion of IoT, and there will be a need to address the unknown. Closed-loop automation powered by artificial intelligence and machine learning will provide a solution to detect threats and changes automatically and mitigate them with split-second agility.

ROADMAP OF AUTOMATED SERVICE ASSURANCE

In the era of 5G, orchestration and maintenance of networks by conventional methods will lead to siloed deployments far from the cohesiveness needed in this era.

To sort this trending problem, CSPs are migrating to automated assurance, enabling shorter time for resolution, improved efficiency, and quicker time to market essential products and services.

But the big question is, what will the adoption rate be of these automation technologies? Of course, implementing holistic, next-generation service assurance frameworks will help integrate new and evolving technologies and enable future self-healing networks.

In the future, operators will be able to solve the problem even before that happens. Thanks to closed-loop automation, we are inching towards that goal.

Future automated service assurance will have the responsibility to:

- Manage the entire lifecycle of products and services to meet SLAs and QoE.
- Built-in AI/ML to automatically detect network anomalies, perform root cause analysis and synchronize with OSS/BSS solutions.
- Oversee the network layering systems via southbound interfaces.
- Remove the network complexity via northbound interfaces and expose data to BSS and OSS for revenue assurance and threat mitigation.

RECOMMENDATIONS FOR ECOSYSTEM PLAYERS

Now we understand that closed-loop automation if integrated with the right framework and intent, will free up CSPs to explore more exciting business opportunities. In reality, CLA not only solves problems but opens prospects of new revenue streams.

However, for CSPs to successfully implement CLA, they need an automated assurance solution that gives them real-time insights (using AI/ML) into what is happening inside their networks.

So, does it mean it will create more competition among CSPs? The answer is a big no.

The success of automation depends on collaboration and not competition. Collaboration among not only the CSPs but also across the CSPs, vendors, system integrators, and standardization bodies.

There may be fear among stakeholders with tasks and responsibilities being transitioned from manual to automation. But as an industry and an ecosystem, the goal is to build a network that is excellent.

CSPs can maximize their revenue potential by taking a larger role in the value chain of industry digitalization. For this, CSPs need to deploy a cloud-native automated assurance solution that has built-in capabilities such as network data analytics function (NWDAF) as defined by 3GPP standards. This would help CSPs to enhance customer experience and enable predictive and proactive network operations.

In the future, the networks will be driven by humans and machines working in tandem to provide the best quality of services. Therefore, the onus is on the CSPs to demonstrate how they will make the right choices and maintain balance in running the networks of the future.

Closed-loop automation and automated service assurance are just the beginning.

RADCOM is the leading expert in cloud-native, automated assurance solutions with AI and ML driven insights, to ensure a superior customer experience for telecom operators running 5G networks. When operators begin their journey to the cloud, they select RADCOM as their assurance partner. With over 30 years of experience at the forefront of assurance technology, we have been chosen by leading operators such as AT&T, Dish, Rakuten Mobile, Telefonica, and others as they transition to the cloud and 5G.

RADCOM delivers real-time network analysis, troubleshooting, and AI-driven insights to ensure a superior customer experience. Utilizing cutting-edge technologies, we are the operators' eyes into their network, supporting them as they transition to new network technologies such as cloud and 5G. RADCOM provides dynamic service assurance for an accelerated digital transformation.

We offer the most advanced 5G assurance portfolio for large-scale networks, providing an innovative, efficient, and on-demand solution to network monitoring. This enables operators to meet the challenges of assuring the customer experience in the 5G era and facilitating the transition to a more automated approach to network operations. Our leading solution, RADCOM ACE, is explicitly designed for telecom operators, delivering automated, containerized and end-to-end network visibility.

RADCOM ACE is a solution built for automated 5G assurance that seamlessly integrates into the 5G core as a Cloud-Native Function (CNF) and is compatible with any public cloud, such as Amazon Web Services and Microsoft Azure.

TECKNEXUS

5G MAGAZINES | 5G RESEARCH | CONTENT CREATION | ABOUT US

www.tecknexus.com contact@tecknexus.com