Automated Network Slice Assurance on 5G

5G introduces support for new and exciting use cases. Enhanced mobile broadband brings ultra-high throughput. Ultra-reliable low latency communications enables instantaneous communication for services such as factory automation, autonomous driving, and remote surgery. Massive machine-type communications delivers the ability to support a huge network of connected devices or as it is more famously known the Internet of Things (IoT).

In the diagram below you can see what types of applications need more speed, more throughput or massively more connections.

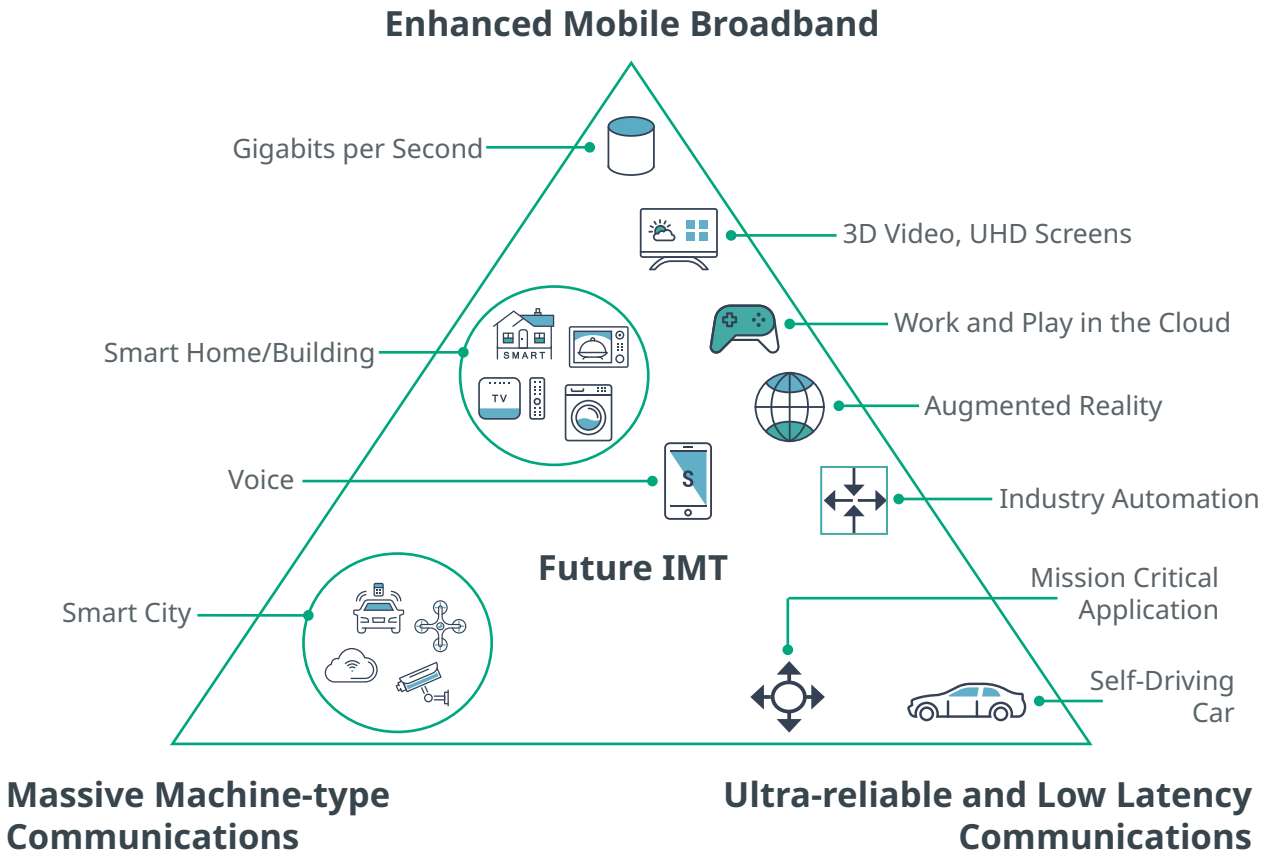
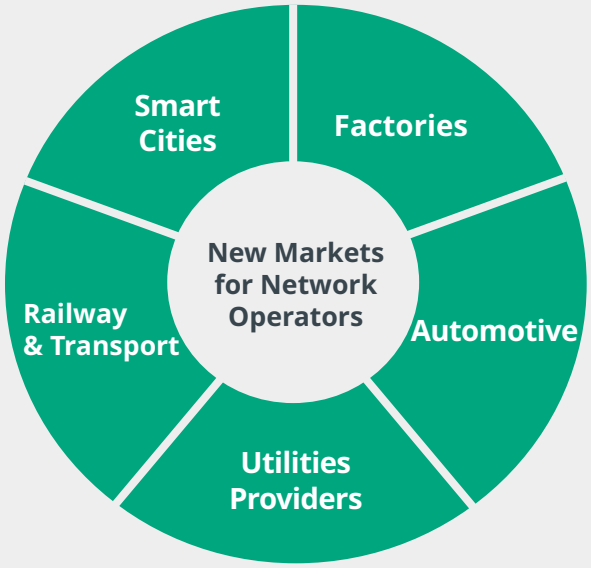


Figure 1: ITU-T IMT 2020 Requirements [1]

[1] Source: ITU Recommendation M.2083-0 (09/2015)

5G's enhancements provide new opportunities. Network operators can address new market segments and create innovative services across new industry verticals with guaranteed performance and separated networks. For network software vendors[2] it allows them to target new market segments, with different business models to their traditional customer base, wishing to use the enhanced network capabilities introduced by 5G.



- Municipalitites for Smart City initiatives
- Factories for digital transformation and automation
- Automakers for autonomous cars
- Railways and public transport for traffic and schedule optimization
- Utility providers (gas, electricity, water) for metering point analysis

- Network operators building new 5G networks
- Manufacturing with 5G private networks for production facilities optimization
- Railway operations efficiency and advanced internet services

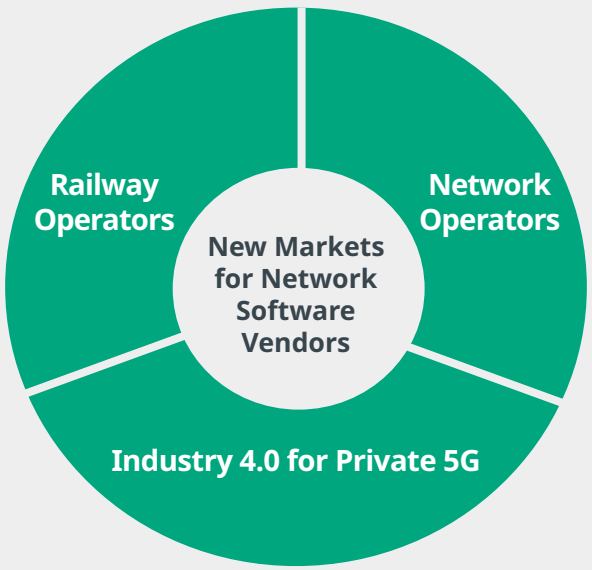


Figure 2: Potential new markets for Network Operators and Network Software Vendors

[2]We use here the term "network software vendors" instead of the more popular "network equipment vendors", as Software, much more than Equipment, will be the key value holder of the 5G proposition.

Network Operator's customers, which include consumer, enterprise and a plethora of industry verticals, will benefit from enhanced network capabilities. New innovative use cases are predicted as the 5G adoption rate increases. The biggest beneficiaries of the 5G revolution will be the industry verticals where 5G networks will act as the catalyst for the so-called "4th Industrial Revolution" bringing the advanced capabilities of 5G to industry and manufacturing.

However some will see 5G networks as an opportunity where they can build a private 5G network, run as they see fit and optimized for their own needs. Private 5G will be of keen interest to railway operators and large industry manufacturers who have the purchasing power and technical expertise to deploy and manage networks.

Challenges and Opportunities

One of the biggest hurdles that network operators will face when deploying their new service-based, cloud-native network functions is how to operationalize them. Network operators will discover that a 5G network is not just another "G" or technological leap to manage and assure as before, as it adds more complexity, radically new requirements and stricter SLAs (service level agreements) when compared to previous generations of networks.

Increased Network Complexity

Overlapping changes taking place at both the infrastructure level (where the network functions are hosted) and at the network elements level (how the network functions are deployed and how they behave) are contributing to the manifold increase in complexity. The infrastructure is replaced by industry-standard IT servers and the network functions are re-architected to behave as cloud-native applications, mimicking the architectures used on the internet and popular services such as Facebook, Twitter and Reddit.

Private Cloud Infrastructure

At the infrastructure level, Network Functions Virtualization (NFV) requires operators to host and manage a private cloud infrastructure in their own data centers. Private clouds are considered to be part of the IT domain: built, managed and maintained by dedicated IT operations teams. This is at odds with the current way that appliance-based network equipment is managed where network teams are responsible for the entire lifecycle. Transitioning from the status quo to the desired end-state requires careful organizational changes and massive re-skilling of engineers either on the IT/Network side or on both sides.

Service-Based Architecture & Encrypted Communications

At the network elements level, 5G introduces the concept of Service-Based Architecture (SBA) and Cloud-Native Network Functions (CNNF) which pose their own challenges around troubleshooting and understanding network status.

In SBA, which is a middle ground between microservices and Service-Orientated Architecture (SOA), the key concept is that each service is built, run and scaled independently of every other service. Services communicate with each other through well defined “contracts”, implemented using APIs. This decoupling gives a lot of flexibility on how each service is implemented and allows network software vendors to build resilient networks.

Adopting this software architecture to the network as an “app” is expected to offer many benefits to the network operators, such as simplified management, better resilience and automatic scalability.

However, as usual, the devil is in the detail. An SBA will work well as long as communication “contracts” are well defined and well respected by all services looking to communicate in the service mesh. In single-vendor environments, interoperability issues are less of an issue as vendors test and validate using their own equipment. However many networks choose multi-vendor environments for commercial reasons. This multi-vendor approach has a side effect meaning the interoperability and testing between network functions becomes even more important. Additionally 5G core reference points, which are the interfaces between functional blocks, have been rewritten from scratch adding to the complexity.

Another unexpected side effect, led by growing cyber-security concerns inside network operators, is that the APIs used by the services inside the 5G core network will need to use modern HTTP2 encryption protocols. The use of encryption makes sense with the shift to “IT industry best practice” architectures. However, where you have well-known standard protocols and communications, you will also have hacking. It is recommended to protect the network and the content with encryption. This security, however, comes at the expense of visibility inside the network communications, which, in turn, will make troubleshooting 5G core network issues more difficult. Combining multi-vendor network difficulties with encrytion requirements will make Service Assurance more challenging.

Cloud-Native Network Functions (CNNF)

In the pre-5G era, the network was relatively static. A topology map outlining the network nodes

and static data collection systems, that were manually updated from time to time, were more than adequate to help operations discover and troubleshoot network issues. Driven by the increase in network services offered, such as VoLTE and VoWIFI using IMS, these operational tasks had become cumbersome even for static deployments, due to the increased complexity.

Cloud-Native implies that the apps live in the public or private cloud. CNNFs are containers within those clouds using microservices. These contribute additional abstraction layers to an already complex architecture mix which makes it even more difficult to detect, triage and troubleshoot issues. Given the complexity and layers of abstraction a network-centric approach will not yield the same expected results. 5G changes what you need to do to be able to assure your network.

Self-healing, AI-driven Networks

CNNF enthusiasts will argue that the 5G network of the future will heal itself and therefore should require significantly less maintenance and operational overhead compared to traditional networks. This ambition requires significant effort and so is true when applied to organizations which are practised in the needed methodologies. Organizations need services to have been designed and deployed cloud-natively. DevOps methodologies are required to update the network and configuration on the fly. So for many network operators, these ambitions are the desired end-state with a learning path full of challenges in the interim.

Network Slicing

How then can you maximize 5G, with high speed, low latency, and massive connection capabilities and high expectations around supporting use cases? Those needs have to be met most of the time, simultaneously, using the same limited radio spectrum, hosted on the existing IT-standard private-cloud infrastructure, and relying on the same operations teams.

Here we borrow a concept from virtualization called containers but apply it to the network. In the IT world, a physical server (which is a finite and discreet resource) is carved up in thin slices which are known as containers (or virtual machines). These containers create the illusion that each slice exists on its own dedicated piece of hardware. Each slice can then be maintained, and adjusted based on the resource needs of the slice. This optimizes the finite resources, almost like the way a skilled player organises blocks as they fall in a game of Tetris.

When the same concept is applied to 5G networks, the analogy can be expanded like this: the radio spectrum, the network services and the physical infrastructure hosting them become

the finite resources, the utilization of which need to be optimized and thus the network slices become the containers.

If we take the analogy further, we can consider each of the network slice characteristics (required throughput, latency, a minimum number of devices to be handled, mobility function,

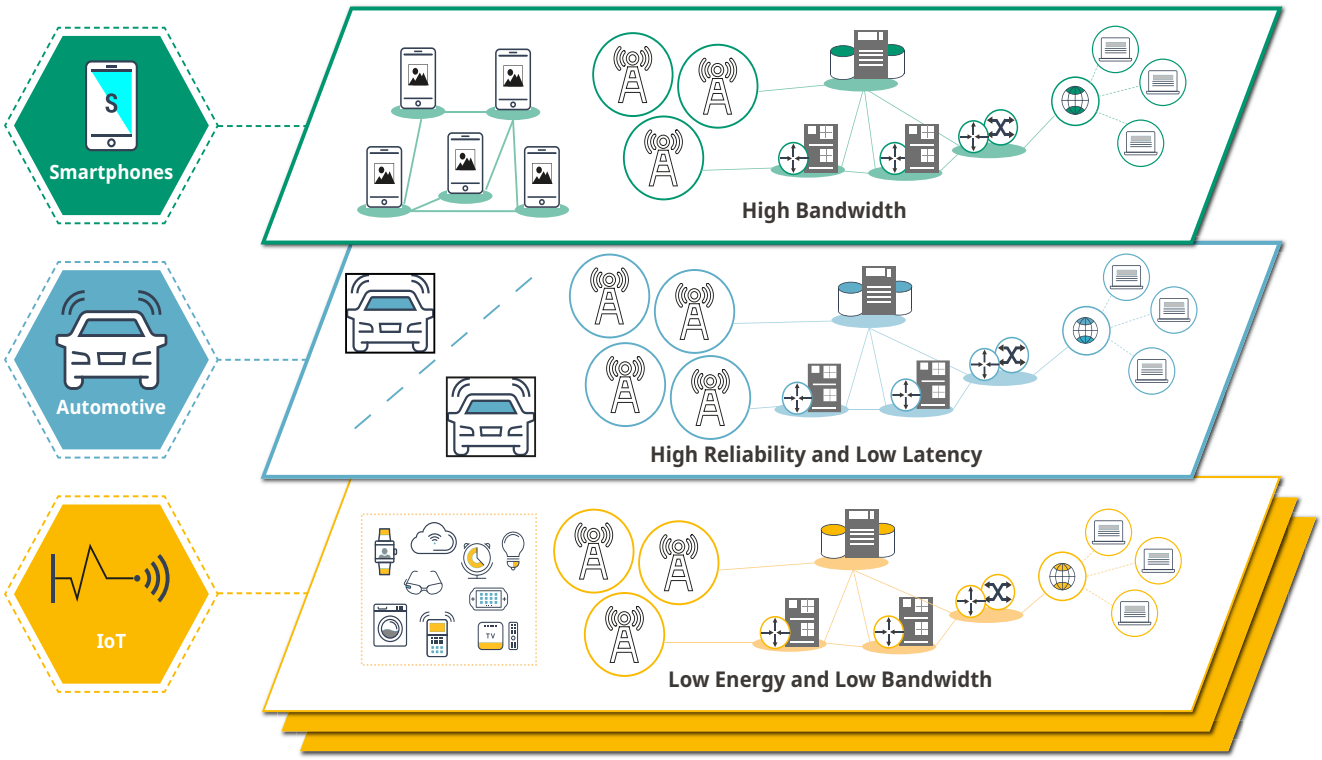


Figure 3: Network Slicing

etc.) as the equivalents of the abstracted hardware resources of a virtual machine (vCPU, vRAM, vNIC, disk, etc.).

While virtualization and containers are mature and stable technologies, network slices have just been introduced as a concept. It will take time to reach the maturity level required by the heavily regulated and SLA-conscious telecommunications industry.

Today, network operators already face difficulties meeting enterprise customers' SLAs with the current network configurations and relatively few KPIs. So, for enterprise customers, network slicing, and the concept of owning a container of resources is expected to have a strong appeal. Many enterprise customers use their own quality-of-experience (QoE) tracking software and some have their own NOC teams that make sure each device is connected, is communicating and is properly maintained. In case of disputes about availability, throughput levels, latency and other network slice characteristics, the 5G network operators will need to understand slice performance, the behavior of their enterprise customers on the slices,

and have strong evidence to support their case. To deliver on promises of premium levels of support and service for enterprise customers, savvy network operators will need to have premium assurance and reporting with insights for 5G services.

Massive Throughput, Low Latency and Massive Device Numbers Still Needs to be Supported

In addition to all these requirements, the 5G networks of the future should gracefully handle the diverse needs from its various potential users: higher throughput for video streaming, VR and AR, ultra-low latency for machine-type communications related to Industry 4.0 initiatives, and the hundreds of thousands of “mice” flows coming from all the connected sensors which serve smart cities, utility providers and connected cars.

Apparent Solutions

Approach 1: Same old, same old: bits and bytes, network-centric

5G can be viewed as just another new network version to monitor, troubleshoot and assure and that applying the same methods and using the existing monitoring frameworks will cover requirements to assure customers and corporates.

Network Operators and Network Software Vendors taking this approach will try to shoehorn and force-fit previous ways of working to the new paradigm and will most likely discover that it will outright fail or that it will not scale to the level required. The result being, either way, unsatisfactory.

This is because 5G networks sit at the intersection between modern IT software delivery architectures (service-based architecture, containers, cloud-native, private cloud) and traditional, ubiquitous mobile connectivity (voice, data & text). Trying to bridge these two worlds has new challenges.

This previously unseen intersection between IT SDA and mobile networks requires a new breed of tools to make it fully manageable at scale.

Approach 2: Rip and replace: cloud-native functions, cloud-application monitoring

Another approach would be to consider the 5G network as just another cloud-native application and use emerging cloud-native tooling and instrumentation to ensure that the "services" used to run the network are always up and healthy.

Going down this route is very appealing because it is aligned with the whole cloud-native ethos but, even with this approach, there are some things to consider:

- All monitored network functions should be CNNF, which as of now, is not the case. Look at the distinction made between Control Plane—fully cloud-native and User-Plane—more monolithic, but geographically distributed.
- All cloud-native network functions coming from different Network Software Vendors should implement the same instrumentation frameworks. It is rare to find this kind of alignment across vendors, especially given the plethora of options available in the market.

  And we should not forget:

- The monitoring and instrumentation framework of choice should be capable of giving relevant metrics for a mobile network service, not just generic IT/cloud-related metrics. Every framework can be customized and adapted to match the specific monitoring requirements of each mobile network operator, however, this is often at the expense of time-to-value and requires an additional budget for professional services.

The Real Solution

A pragmatic approach is to focus on outcomes, not on output. One must realize that the bulk of services to be provided by a 5G network need to continue to be centered on mobility, connectivity, and human-focused experiences.

If this realization occurs, the path forward is less of a haze and becomes clearer: 5G network operators must focus on the service level agreements between them and the customer. They must ensure that devices and humans can access their network, remain connected as needed

and that when a service is used, that service is available and meets the required SLAs every time.

This approach is top-down so as long as the network customers don't feel, don't experience the effects of outages and service failures, they are none the wiser to the fact that those outages occurred in the background. So by focusing only on customer-impacting metrics, a 5G network operator can optimize their spending on capacity, redundancy, and tools.

5G networks are supposed to heal themselves, to be more resilient and handle failures with grace. This, however, does not mean that running a 5G network is going to be a hands-off business. Customers, especially enterprise customers that will be able to buy slices of the network with bespoke characteristics and SLAs, will demand detailed reports about how their share of the network is behaving and how it behaved in the previous days, weeks and months.

Enterprise customers' demands are very different with requirements for deterministic SLAs. Enterprise customers also have the budgets to pay for more complex data analytics/reporting including historical or predictive trends which helps them to justify the business decision for premium service. Providing this type of customized reporting and analytics at scale requires something that could be called Service Assurance as a Service or SAaaS. This approach bridges traditional assurance with cloud-native 5G networks.

Key Takeaways

Network slicing will be a key benefit for operators in 5G. Anritsu recommends that all operators look at monetizing the slices with an aim to deliver premium assurance and reporting for high value business cutomers.

Enterprise and industrial network customers come with their own set of challenges, especially when it comes to 5G network operators meeting the SLA and contractual obligations which define the bespoke network slices. To keep these SLAs within thresholds, Anritsu recommends a new approach to service assurance, an approach that is top-down, outcome-focused, customer and slice-centric, and cloud-native.

Anritsu recommends Service Assurance as a Service to sit at the intersection between traditional network "assurance" solutions and future cloud-native 5G network slicing assurance, enabling network operators to offer differentiated services at scale.

About Anritsu

At Anritsu we are working on the future vision of Service Assurance and Automated Assurance with a frictionless assurance solution that is cloud-native and grows with your network.

5G brings new opportunities, new customers, and new use cases. We support you in your mission to reduce the time it takes to introduce new, high quality offerings, to differentiate in the market attracting new customers and to do this at scale.

Anritsu is a partner for operators around the world. Talk to us about how we can help with your 5G journey.