altice labs

Towards autonomous private 5G networks

Private networks; Autonomy; Virtualization; OSS; Closed-loop; As-a-Service; Business models

White paper

Version 1.0, March 2021

Introduction

Many service providers are undergoing the digital transformation process, and they understand that automating operations and management are crucial steps. According to a survey conducted by TM Forum, "*92.5% of those surveyed (...) were in the process of their transformation, and nearly a quarter (24%) 'were well on the road and reaping significant benefits.' Yet 44.5% were just starting their journey.*" [1]

The emergence of new technologies, the growing number of internet of things (IoT) devices, and, consequently, the gathered data creates enormous pressure on the network architecture and its management to provide greater efficiency. The Ericsson Mobility Report 2019 [2] points out that global mobile data traffic volume is projected to grow by a factor of around 4, from 35 exabytes per month in 2019 to 160 exabytes per month in 2025. By 2025 there will be a total of 100 billion connections around the world, according to Huawei's Global Industry Vision (GIV) 2018 [3]. Although this means a great opportunity, service providers will struggle to respond to the high demand level, mainly due to lack of integration, the inefficiency of their operations, and their network architectures' complexity and fragmentation [4].

One of the most relevant aspects is that the network must be autonomous to deal with the mentioned complexity. That is, the network must be able to configure, monitor, and maintain itself independently and without much human intervention [5]. New technologies – such as cloud infrastructure, programmable and virtualized networks, artificial intelligence (AI), and big data – must be leveraged to obtain the best global solution with an architecture as simple as possible. Automation will transform network management, with the end goal of creating cognitive network operations, enabling self-x scenarios like self-configuration, self-healing, and self-optimization.

Introduction

Automation is a key aspect in autonomous networks and is deeply related to efficiency, like replacing manual tasks, integrating systems, and implementing programmable end-to-end (E2E) processes. All this culminates in cost reduction at both CAPEX and OPEX levels.

Figure 1 presents the main automation benefits sought by operators, according to MIT research on "Network automation: Efficiency, resilience, and the pathway to 5G" [4].

To achieve autonomy, AI should be deeply integrated with automation to learn, predict, build, and evolve all the processes and rules. The implementation of an intelligent autonomous network requires a strategy and must be phased in order to succeed. Typically, at an advanced implementation stage, it should be possible to predict service and network behaviors as well as customer experience. It should also be able to implement closed-loop management, thus enabling operators to proactively solve network faults, consequently reducing service interruptions and customer complaints, as well as improving customer satisfaction.

Figure 1 – Automation benefits according to MIT research

With the challenges mentioned above, 5G positions itself as a technology that allows service providers to harvest the benefits of enhanced mobility, flexibility, reliability, and security. According to a recent whitepaper from 5G Alliance for Connected Industries and Automation [6], "*the 5G vision is one of a true multi-service network which can address the connectivity needs of virtually any application imaginable in the consumer, enterprise and industrial IoT spaces. To this end, 3GPP has specified 5G to support enhanced mobile broadband, massive-scale IoT, and ultra-reliable and low-latency communications. 5G networks are also expected to provide unprecedented levels of flexibility compared to previous technology generations, enabling the cost-effective delivery of new services thanks to virtualization, network slicing, and edge-computing capabilities.*"

Private 5G networks are gaining importance, consequently attracting the attention of network vendors, service providers, and other entities, while enabling the creation of new opportunities for their businesses. The operation of these networks can be challenging if those who choose to implement it don't have the necessary skills since it's not their core business.

The proliferation of private 5G networks can lead to their possible use in crisis scenarios – such as natural disasters, fires, pandemics – and in operators' core network or public services failures, where communications are essential to ensure safety and fast response by the public services.

Why private 5G networks?

Private 5G networks were idealized and designed to answer different business entities' specific requirements – the verticals, offering optimization opportunities impractical or even impossible through generic cellular, wireline, or Wi-Fi technologies. The main business advantages include:

- the ability to provide specific services to the customer, according to their business and operational needs;
- ensuring data and traffic privacy/security in the customer's premises;
- efficiency improvement and costs reduction (with backhaul, multi-access edge computing, etc.);
- reduced latency.

It is expected that private 5G networks will, in most cases, be provided by telcos as a service to business entities/sectors (in a telco-offer-aaS model). Additionally, some large business entities/enterprises will decide to operate their own 5G standalone network by themselves (a self-managed model). Despite the mentioned business models, other models are also possible such as a multi-party model involving a telco provider (although not necessarily an incumbent carrier), the network vendor, the customer, and often other strategic partners (e.g., vertical industry specialists). Finally, there are projects led by a new class of competitors who specialize in providing custom mobile networks for enterprises (a non-telco offer model). The role of major cloud providers (hyperscalers) should not be ignored, as the trend points out to an aggressive go-to-market with their own business models fitting into either multi-party or non-telco offer models. **Figure 2** depicts the private 5G mobile models. Regardless of the business model, it is a fact that networks must be managed and as autonomous as possible.

Figure 2 – Private 5G mobile business management models

The main requirements for private 5G networks are [7]:

Availability: High availability means that the end-user can always have the service available depending on the negotiated service level agreement (SLA). In practice, the network must be built so that the downtime is virtually zero (6 or 7 nines) and any system maintenance can be controlled, guaranteeing maximum availability. This will include robust solutions and redundancy constructions of critical network elements.

Reliability: Reliability refers to the capability of transmitting a given amount of traffic within a predetermined duration with high success probability. It requires sufficient network coverage and capacity, as well as robust handover functionality.

Interworking: Interworking with public networks is an important capability. Many critical services (e.g., emergency vehicles) need session continuity while moving from one network to another, for instance, from a private network to a public one. This requires integration between both networks.

Quality of service (QoS): QoS management is based on measures and key performance indicators (KPI) referring to throughput, latency, jitter, packet drop rate, and more. Operating private networks on a dedicated spectrum offers the possibility to control each one of the KPI easily. Scenarios of shared spectrum will require strong monitoring. Intrinsically 5G networks allow a better QoS and performance on resource usage for the different services, and that can be tailored to the specific needs within private network deployment (for example, by using slicing).

Security: Private networks are expected to provide full E2E security to ensure that information, infrastructure, and people are protected from threats. This requirement involves implementing measures to preserve the main security principles as data confidentiality, integrity, availability, and sovereignty.

The scenarios presented below are among those that extract value from private 5G networks' deployments:

IoT for industrial environments (Industry 4.0) - by introducing industrial internet of things (IIoT) devices allows having tight control over the industry value chain, such as monitoring the correct functioning and/or identify any potential issue before they occur, improve quality control processes and so on. All the generated data must be collected and analyzed, leveraging on ML algorithms, to provide guidance and insights for the E2E factory's operation optimization.

IoT for campuses: colleges/universities, hospitals, or transport hubs (airports, railway stations, ports) demand connectivity, security, and low-latency and could benefit from the capabilities offered by a private 5G network. In fact, almost any enterprise building or public place could be a candidate for a private 5G network.

Remote areas with reduced or even no network coverage: enterprises, public places, campuses in areas where the infrastructure needed to deliver public 5G simply doesn't exist could benefit from deploying a private 5G network.

Working on collaborative mode: current non-mobile networks supporting collaborative activities in several sectors tend to be replaced by mobile ones. These networks support use cases related to automation, tracking, and monitoring in real-time while enabling video streaming and augmented reality (AR) for real-time sharing [8].

Mission-critical capabilities: decisive for scenarios in which the workers' safety is essential (ex., high-risk missions in remote and dangerous areas) or for efficiency improvement in multidisciplinary teams requiring mobility. Public networks may not be designed/dimensioned for such types of missions, or even they may occur in areas with little or no public network coverage. Despite 4G already supporting the implementation of these scenarios, 5G ultra-reliable low-latency communication (URLLC) will improve their response. .

Any entity expects to transparently access private 5G networks, with almost zero impact on its core business. Therefore, even if new players gain access to a dedicated spectrum, depending on regulators, and implement a vertical solution, they are unlikely to have the in-house expertise to plan, build, operate and manage these networks, at least in the short term. Operators can play a major role, managing "private-networks-as-a-service", even beyond their own spectrum and infrastructure.

How to assure autonomy?

The demanding ecosystem that arises with the emergence of an all-digital era becomes a big challenge for the network operations, which must improve its efficiency while promoting processes' automation, agility, and network autonomy.

Today, networks are mainly managed in an incident or event-oriented approach, meaning that they are driven by network faults or issues that clients experienced in their services. In fact, network operations are fundamentally reactive, responding to events or fixing problems.

The exponential growth of managed devices (mainly IoT) and the increase of related management information require solutions in the traditional operation support systems (OSS) area, able to integrate big data, AI, and ML technologies, thus bringing high value for network operations and customer quality of experience (QoE). As so, operations should be reshaped, incorporating cognitive and autonomous abilities that will enable predictive analysis, real-time decisions, and accurate actuation. The main enablers of cognitive and autonomous operations are highlighted in **Figure 3**. This add-on block has two main components:

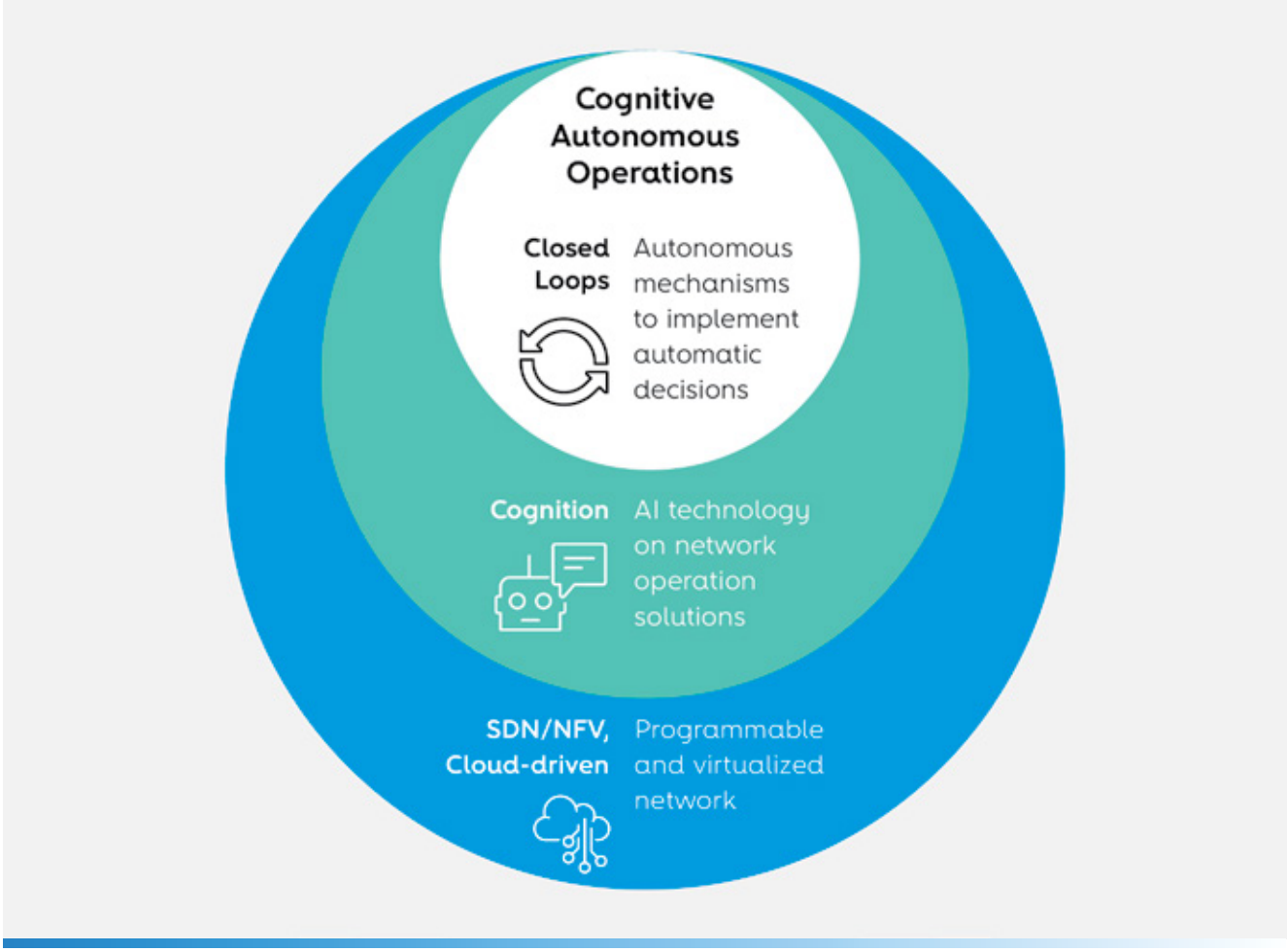


Figure 3 – Cognitive autonomous operations – high-level logical view

The closed-loop capability should include the following main activities:

- **Sensing:** collecting of service and network data from all layers, like physical network elements (NE), virtual infrastructure, software-defined network (SDN) controllers, etc., to feed assurance activities;
- **Analysis:** analyzing, in real or near real-time, of network and service's data, potentially enriched with other data sources (inventory, catalogs, etc.), that will allow obtaining information on network and service's health;
- **Decision:** decision mechanisms determining actions for self-optimization, self-healing, and self-protection;
- **Acting:** fulfillment E2E orchestration process, with service configuration and activation over physical or virtualized resources.

The value added by these activities depends on theThe value added by these activities depends on the network agility, such as the network's ability to program itself, as well as the implementation of AI for data analysis and identification of insights that will enable the creation of new rules for actuation and decision-taking. Technologies such as SDN, IT, and network functions virtualization (NFV) will allow the increase of automation, critical for digital transformation.

Cognitive autonomous operations will enhance automation and efficiency in real-time scenarios, either in the proactive domain, like problem detection, diagnosis, service/network degradation, and actuation in order to prevent the occurrence of faults and impact in the customer experience, or in the reactive domain, enabling faster response, as automatic and autonomous as possible.

Figure 4 presents the operation's add-on block that integrates with the assurance solutions (for collecting relevant data), inventory solutions (storage and information owner), and fulfillment solutions (for acting) to provide scenarios that will "close the loop" and enable to achieve an autonomous network.

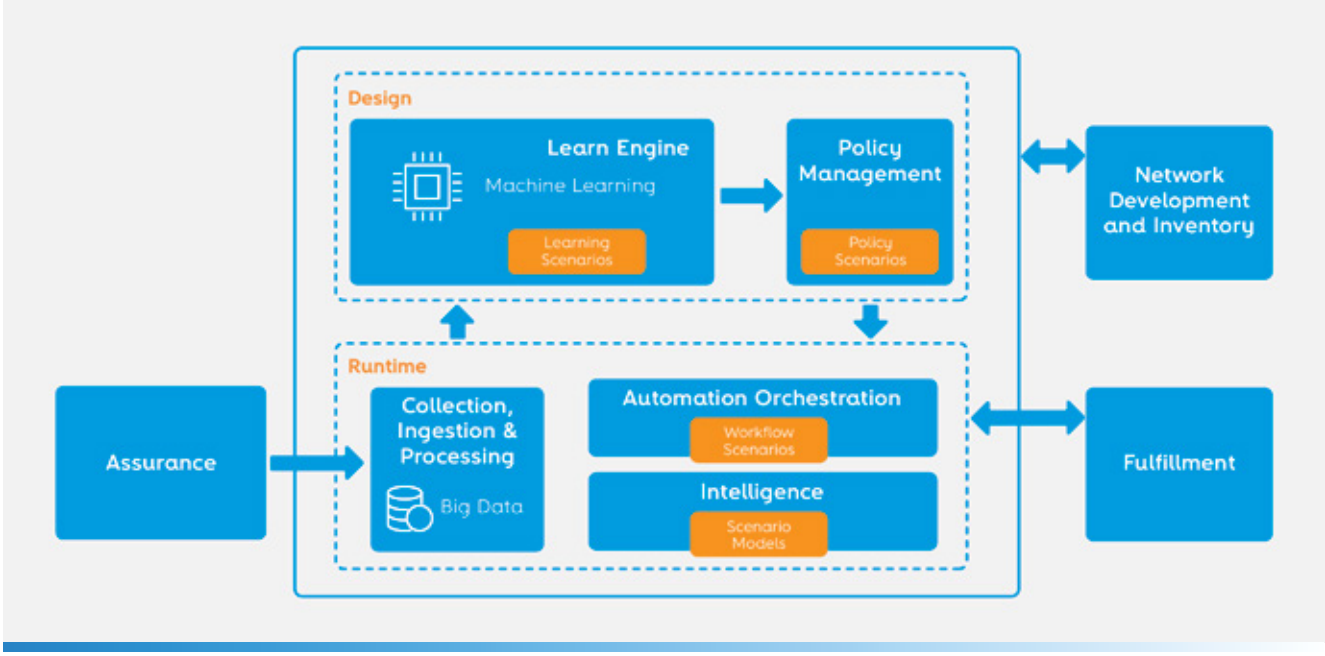
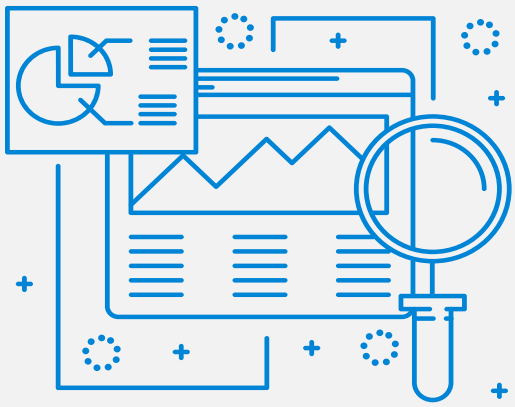


Figure 4 – The autonomous operation architecture

This add-on block has two main components:



Design

To train the selected scenarios, using ML to analyze relevant collected data and generate new or enhanced policy decisions (like predictive failure alerts, diagnosis algorithms, corrective activities) that will influence runtime automation decisions.

Runtime

To collect, store, and process all data, enabling the execution of programmed workflows for the closed-loop identified scenarios and supported by intelligent decision rules available from the design component.

An automated orchestration enables the creation of services across different network domains, and together with analytics AI, allows the full closed-loop automation, reducing the operation cost of the network and services, and minimizing human intervention. Networks will monitor themselves in real-time within a feedback loop in order to permanently adjust to the services' real needs and implement self-healing while proactively fixing any detected problems.

Although autonomous networks present themselves as the way forward, there are some difficulties and challenges that need to be analyzed on a case-by-case basis, like:

- the slow return of investment typically leads to de-prioritization;
- the existence of silo systems with no integration leads to processes without an E2E vision;
- the lack of business cases and process definitions;
- short-term thinking, without an automation strategy;
- the non-existence of a centralized and secure data lake.

It is important to identify possible constraints in implementing the different autonomy levels in order to work out the right methodologies to overcome them. Iterative approaches could help with cost control and getting the pulse on the incomes, as depicted in **Figure 5**.

Assessing the network, processes, systems, and operations will improve the identification of the measures to be implemented, executed in small steps throughout several iterative cycles. Whenever possible, a strong planning component to keep the balance between costs and earnings is also advisable.

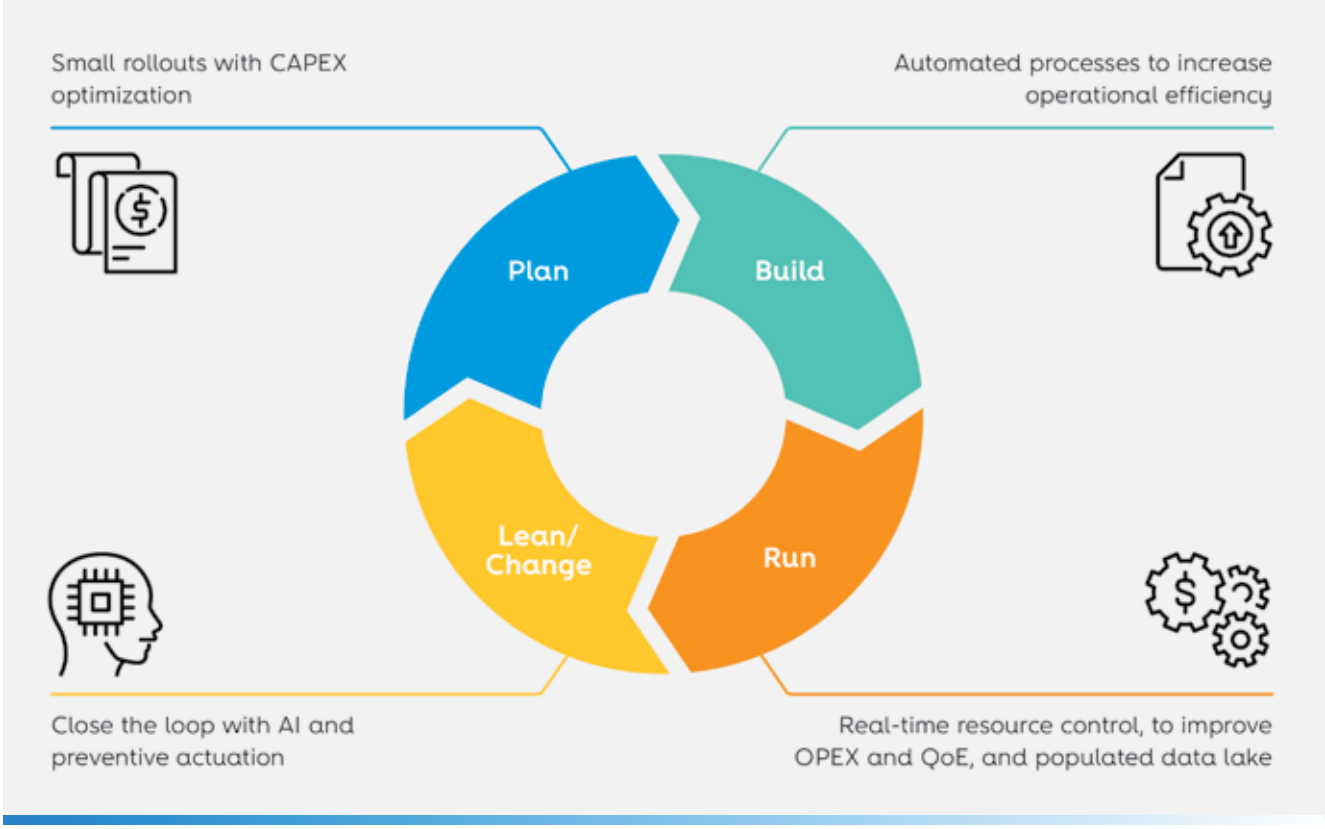


Figure 5 – An iterative approach to achieve network autonomy

The mask for facing crises

At a time when masks are becoming essential to prevent the spread of COVID-19, it makes sense to question whether autonomous private 5G networks could help the creation of "masks" to minimize the effect of natural disasters, fires, and other crisis scenarios where citizens' safety is at risk.

One example, taking advantage of autonomous private 5G networks, would be a city's infrastructural data (communications network, water, energy network, traffic lights, etc.) combined with weather events, gatherings, scheduled events. Based on this cross-referenced information, networks will be able to make decisions in real-time, or near real-time, that reinforce and improve the response capacity in the most impacted areas. Having gathered all this information, the network and the operating systems will be able to resize themselves and move to answer an anomalous event or predict the need for more communications resources.

Communications are essential in everyday scenarios, having a huge impact in crisis events, namely those associated with natural disasters such as earthquakes, hurricanes, forest, and fires, among others, either before, during, or after their occurrence. This is most obvious in cases such as ensuring communications between civil protection and security forces, enabling the communication between the affected population and their families and friends, as well as carrying out rescue operations. However, in addition to the direct victims, it should be noted that rescue teams also expose themselves to risks that must be minimized. In fire situations, for example, it is becoming commonplace for firefighters to use cameras on helmets and other sensors related to their body's response, like body temperature, heart rate, or movement. At the same time, they are also able to receive real-time information of, for instance, weather conditions, satellite images, and maps, eventually even deploying AR technology in eyeglasses or mask visors. All these types of usage generate huge amounts of data, making it essential to have a network able to separate the least critical traffic from the most critical one and respond autonomously to these needs by adding the necessary resources.

Foreseeing a potential proliferation of private networks, operators/authorities should address technical solutions for resource sharing between different entities' networks to ensure a better response in crises or catastrophe scenarios.

By highlighting different ways of leveraging autonomous private networks in crisis events while taking advantage of their autonomy, intelligence, and reactive capacity, it is essential not to minimize the importance of evolving the respective operating centers in order to be crisis-proof.

Conclusions

In the era of 5G and IoT, operators need to evolve to a model in which the network, and its capacity, is centrally programmable, enabling the virtualization of several functions and providing low-latency communications, high data rate, among other characteristics. This new model requires an intelligent E2E network orchestration driven by closed-loop automation. Such a shift requires both significant financial and operational investment and a transformation in the organizational setup, processes, and skills.

Operators who fight for a central role in providing value-added services to business customers, namely out-of-the-box OSS functions in an as-a-service model, will need to redefine and reshape network operations' solutions. This requires an OSS evolution to enable open and easier automation while adopting cognitive mechanisms that bring autonomy to the network. The cognitive and autonomous operations concept and architecture, presented in this article and pursued by Altice Labs, advocate a new generation of OSS that suit the most challenges herein exposed.

Although private 5G networks could become a trend in solutions for different scenarios and specific industry needs, they will certainly not be the answer for everything nor be the only technology on the market.

Despite all the advantages associated with private 5G networks, its implementation demands investment costs that must be weighed against the benefits and the value they add, namely ROI and business outcomes. Therefore, it is important to gain skills in this field to help customers make good decisions in their networks' evolution, focusing on their own digital transformation.

From an operator's point of view, as a potential provider of private 5G network solutions, it is natural for these solutions to include services by design, namely in the cognitive operations' domain, to support their automatic operation and ensure their autonomy.

5G deployment has been impacted by the COVID-19 pandemic, as many enterprises faced unexpected and severe difficulties in their business. Also, regulatory entities have chosen to postpone the 5G license auctions during this period. However, this pandemic also reinforced the understanding that resilience, automation, and overall digitization – delivered by solutions such as private networks – are key enablers for successful and future-proof businesses.

References

[1] Aaron Richard Earl Boasman-Patel, Dong Sun, Ye Wang, Christian Maitre, José Domingos, Yiannis Troullides, Ignacio Mas, Gary Traver, Guy Lupo; "Autonomous Networks: Empowering Digital Transformation For the Telecoms Industry"; Release 19. TM Forum; May 2019. Available: https://www.tmforum.org/resources/standard/autonomous-networks-empowering-digital-transformation-telecoms-industry/

[2] Fredrik Jejdling; "Ericsson Mobility Report", Ericsson, Nov 2019. Available: https://www.ericsson.com/en/press-releases/2019/11/ericsson-mobility-report-5g-subscriptions-to-top-2.6-billion-by-end-of-2025

[3] Huawei; "Global Industry Vision (GIV) 2025"; Huawei; 2018. Available: https://www.huawei.com/minisite/giv/en/

[4] MIT, Ericsson; "Network automation: Efficiency, resilience, and the pathway to 5G"; MIT Technology Review; May 2019. Available: https://www.technologyreview.com/2019/05/16/135332/network-automation-efficiency-resilience-and-the-pathway-to-5g/

[5] Ciena; "What is an autonomous network"; Ciena; 2020. Available: https://www.ciena.com/insights/what-is/What-Is-the-Adaptive-Network.html

[6] 5G-ACIA; "Exposure of 5G Capabilities for Connected Industries and Automation Applications"; 5G-ACIA (5G Alliance for Connected Industries and Automation); May 2020; Available: https://www.5g-acia.org/publications/exposure-of-5g-capabilities-for-connected-industries-and-automation-applications/

[7] Anna Larmo, Peter von Butovitsch, Patricia Campos Millos, Patrik Berg; "Critical capabilities for private 5G networks"; Ericsson; Dec 2019. Available: https://www.ericsson.com/en/reports-and-papers/white-papers/private-5g-networks

[8] Jeff Travers, Bob Gessel; "What is the operator opportunity for private mobile networks?"; Ericsson; Jun 2020. Available: https://www.ericsson.com/en/blog/2020/6/opportunity-for-private-networks-for-operators

Authors

Catarina Mónica

Head of OSS Provision Solutions

Altice Labs, Portugal

catarina-s-monica@alticelabs.com

Dulce Teles

Senior OSS Architect

Altice Labs, Portugal

dulce@alticelabs.com

https://www.linkedin.com/in/dulce-teles-a9b364b1/

Paulo Ferro

Product Manager

Altice Labs, Portugal

paulo-j-ferro@alticelabs.com

https://www.linkedin.com/in/paulo-ferro/

Pedro Antero Carvalhido

Team Leader

Altice Labs, Portugal

pedro-a-carvalhido@alticelabs.com

https://www.linkedin.com/in/anterosousa

Contacts

Address

Rua Eng. José Ferreira Pinto Basto
3810 - 106 Aveiro (PORTUGAL)

Phone

+351 234 403 200

Media

contact@alticelabs.com
www.alticelabs.com