

InnovAction

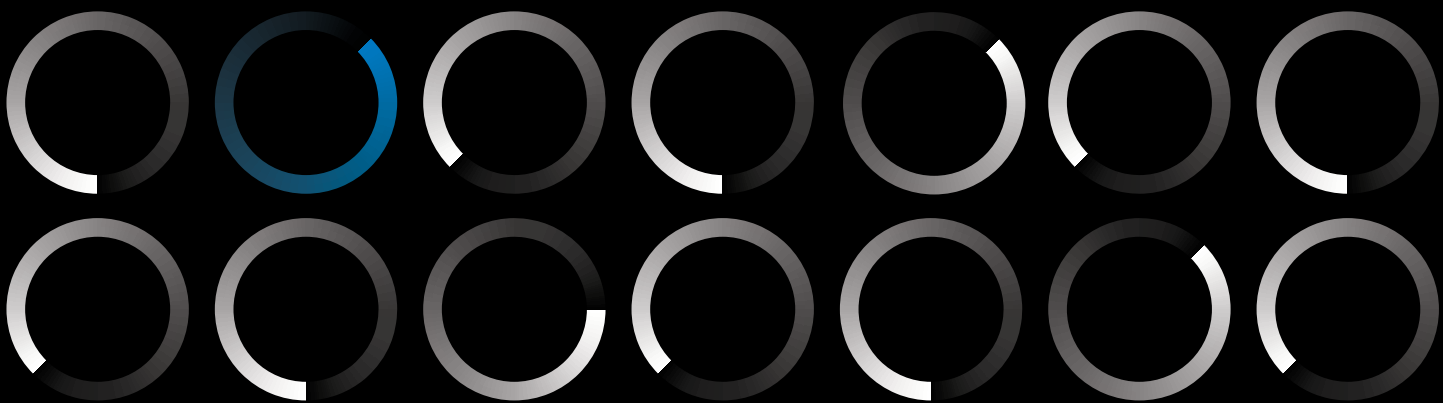
#5 | 2020

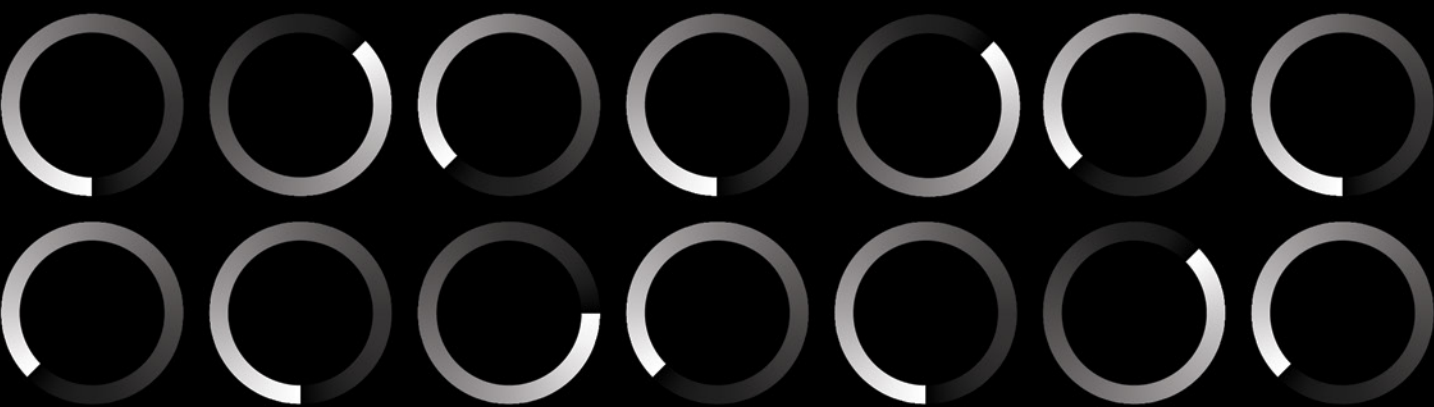
“

It is precisely in these contexts—not in stable times—that the real opportunities lie to gain competitive advantage through strategy.

”

- *Pierre Wack*






InnovAction

#5 | 2020







The need for a new operating system

For many of us, 2020 was the horizon of a new decade where 5G was to play the most significant network transformation and opportunity for operators and industries in general. 5G was also seen as the main factor to define technology priorities, not only in terms of evolution but also in terms of investment.

However, on the other side of the horizon was something that most of us could not foresee, which affected every industry, leaving transformation strategies paused for further evaluations having in mind a new (societal) reality. COVID-19 pandemic was totally unexpected and forced all industries to rethink their strategies and dynamics fast. Amid this unexpected crisis, businesses and industries digitally more advanced are the ones that will survive and overcome the current hostile scenario!

From this “new normal” on, corporates will live in a new societal organization. A new operating system will combine several infrastructural dimensions with several technologies to make companies overcome unforeseen crisis that can strongly impact their normal operations, making them emerge stronger in the day after!

This is precisely where Altice Labs expects to help. Through its R&D&I ecosystem, which gathers academic knowledge combined with enterprise expertise and experience, develops exploratory projects that will promote the infusion of emerging technologies into its own solutions, creating new approaches to build highly valuable solutions for the market. This edition of InnovAction highlights some of those approaches and evolutions.

Once again, Altice Labs publishes InnovAction, a technological magazine strategically designed to share the most relevant research and technical knowledge to help digital service providers reinforce their innovative capabilities and surpass present and forthcoming crises!

I hope you enjoy reading it, as much as we enjoyed writing it.

Alcino Lavrador
General Manager of Altice Labs

Editorial note



Since the COVID-19 pandemic, those more digitally mature have proved to be more resilient and capable of faster changes to cope with the crisis impact and, especially, to timely unveil uncertainties that may block their operations. Communication service providers are one of the best examples of it, having proven their ability to help societies to be connected, work, and move to (almost) fully-digital contexts.

They were also artful enough to perceive the opportunities behind uncertainties, using them as driving forces to reshape their operating system, creating a new one capable of outmaneuvering these strange times! Altice Labs did the same, and the following articles point out some of those opportunities and how we are addressing them:

- 1. Leading through (and after) a crisis:** analyzes the crisis impact on business continuity, proposing how to overcome it and how to act by defining a new operating system and promoting strategic foresight to overcome future crises.
- 2. The after-pandemic market:** tries to anticipate the impact COVID-19 pandemic will have in the near-future market while offering some suggestions on how to make the most out of this new turbulent scenario, where operators play a significant role.
- 3. Industrialization and mass production challenges:** details and provides an integrated view of the manufacturing process while analyzing the importance of its resilience to risks and adversities.
- 4. Artificial intelligence impact on operational models:** proposes some answers on how the incorporation of artificial intelligence into existing organizational and operational management practices will help organizations to be better prepared to embrace frequent and rapid changes, a constant in modern societies, and highly reinforced with the current crisis.
- 5. eXtended new Reality:** addresses some critical aspects of the potential of extended reality technologies in the context of digital transformation and widespread adoption of teleworking, distance learning, and virtual conferences.



6. Addressing privacy regulations for a new world: tackles the regulation of privacy worldwide, showing it is essential to assess the available responses to emergencies and the ensuing new world.

7. Data: the good, the bad and the ethical: highlights the opportunities, problems, and best practices of using data, especially in turbulent times.

8. SmartAL is adopting PETs!: introduces some promising privacy-enhancing technologies and how they can help data be securely and privately processed, eliminating vulnerabilities that may be critical during crisis scenarios. It also showcases its practical application in an assisted living platform.

9. Operators' role in next generation MCX: enumerates a set of services requiring low latency and reliable communications in crises while explaining how 5G and edge computing will support them and ensure they continue running in stressful scenarios.

10. Redesigning the network edge for a new era: explores an approach towards the

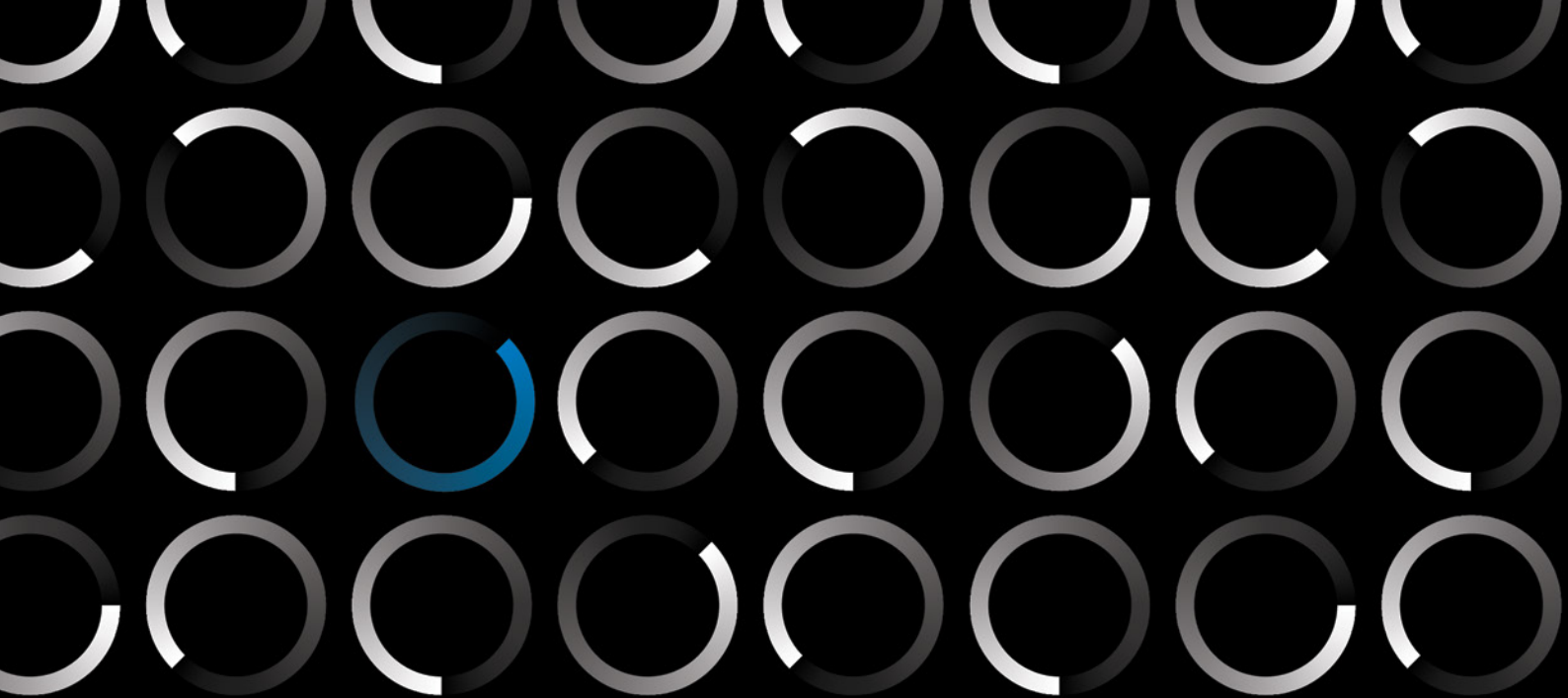
automation of the service provider network with a special focus on the cloud central office where a significant part of the network infrastructure resides.

11. Towards autonomous private 5G networks: describes the technical and business benefits of 5G private networks, showing how to ensure their autonomy and how to prepare them best to surpass crisis scenarios.

12. 5G radio units towards virtualized RAN: presents the opportunities that open and integrated radio units, combined with a passive optical network portfolio, may bring for small cells and 5G densification.

Under the topic of the need for a new operating system, these twelve articles gather, once again, Altice Labs insights to reinforce the Altice Group's capabilities, resilience, elasticity, and portfolio, as well as build up our Customers and Partners' strength. Welcome to the fifth edition of InnovAction!

Ana Patrícia Monteiro
ana-p-fonseca@alticelabs.com



Contents

01

Leading through (and after) a crisis

(p. 8)

02

The after-pandemic market

(p. 20)

03

Industrialization and mass production challenges

(p. 26)

04

Artificial intelligence impact on operational models

(p. 34)

05

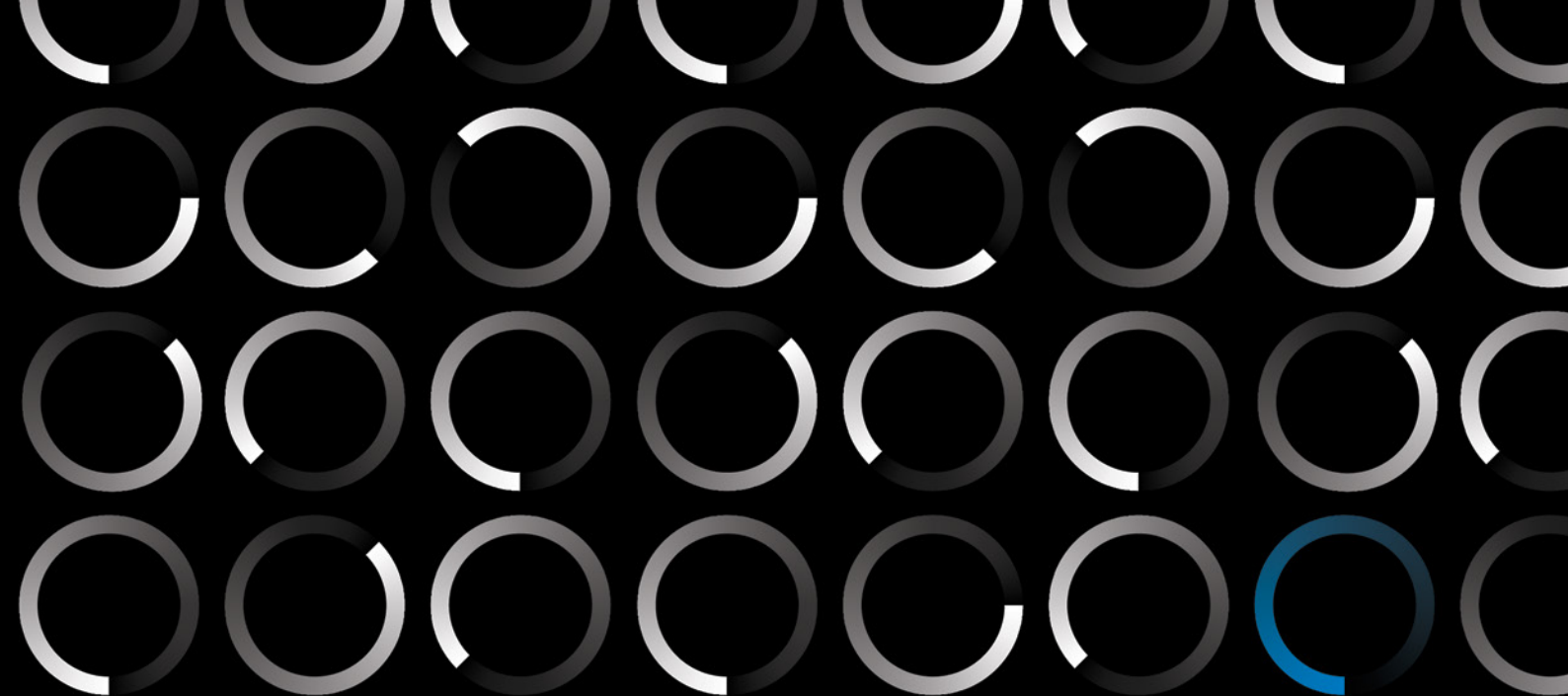
eXtended new Reality

(p. 46)

06

Addressing privacy regulations for a new world

(p. 56)



07

Data: the good, the bad
and the ethical

(p. 70)

08

SmartAL is adopting
PETs!

(p. 80)

09

Operators' role in next
generation MCX

(p. 92)

10

Redesigning the network
edge for a new era

(p. 102)

11

Towards autonomous
private 5G networks

(p. 116)

12

5G radio units towards
virtualized RAN

(p. 126)



01

Leading through (and after) a crisis

Manuel Aguiar, Altice Labs

aguiar@alticelabs.com

Nuno Honório, Altice Labs

nuno-m-honorio@alticelabs.com

Paulo Pereira, Altice Labs

paulo-s-pereira@alticelabs.com

João Pias, Open Labs

jpias@alticelabs.com

João Paulo Firmeza, Altice Labs

pfirmeza@alticelabs.com

Gil Brito, Altice Labs

gbrito@alticelabs.com

Jorge Pinto, Altice Labs

jpinto@alticelabs.com

Keywords

Crisis; CSP; DSP; Operating system; Digital maturity;
Strategic foresight

Lead-in: crisis impact

Crisis, by definition, is a time of danger and difficulties. It is usually unexpected, impacts the normal, and creates uncertainties that conditions, or even blocks, our ability to predict what will happen and the best strategy to overcome it. A crisis can vary in the extent they affect: an individual, a family, a company, an economic sector, a country, or even the whole world, as shown in **Figure 1** when analyzing the impact of the COVID-19 outbreak.

The COVID-19 pandemic crisis reshaped, or is still reshaping, the society to a level that other recent major events, such as de 9/11 or the 2008 financial crisis, didn't: with the imposed lockdown, the physical distance to our relatives was overcome with the use of the internet and social media; our workspace turned into a web conferencing environment; our children shared the classroom on their computers, and other examples could be mentioned! Like never before, enterprises and government services adapted their businesses, rushing the shift to digital as a way to survive, stressing the network with a rise in data traffic (see **Figure 2**) while driving for new high bandwidth and low latency services demand.

It is common to say that every crisis brings new opportunities; it's just a matter of paying attention and investing while others deplore the situation. In fact, "amidst the gloom and doom of the early months of the COVID-19 crisis, something surprisingly uplifting started to happen: Companies began to come together to work openly at an unprecedented level, putting the ability to create value before the opportunity to make a buck. The German multinational Siemens, for instance, opened up its Additive Manufacturing Network to anyone who needs help in medical device design. Heavy truck maker Scania and the Karolinska University Hospital have partnered, too: Scania is not only converting trailers into mobile testing stations, but also directed some 20 highly skilled purchasing and logistics experts to locate, acquire, and deliver personal protective equipment to health care workers. Similarly, Ford is working together with the United Auto Workers, GE Healthcare, and 3M to build ventilators in Michigan using F-150 seat fans, portable battery packs, and 3D printed parts." [3]

Crises are challenging and demanding periods that can lead to disruptive changes for those willing to embrace it!

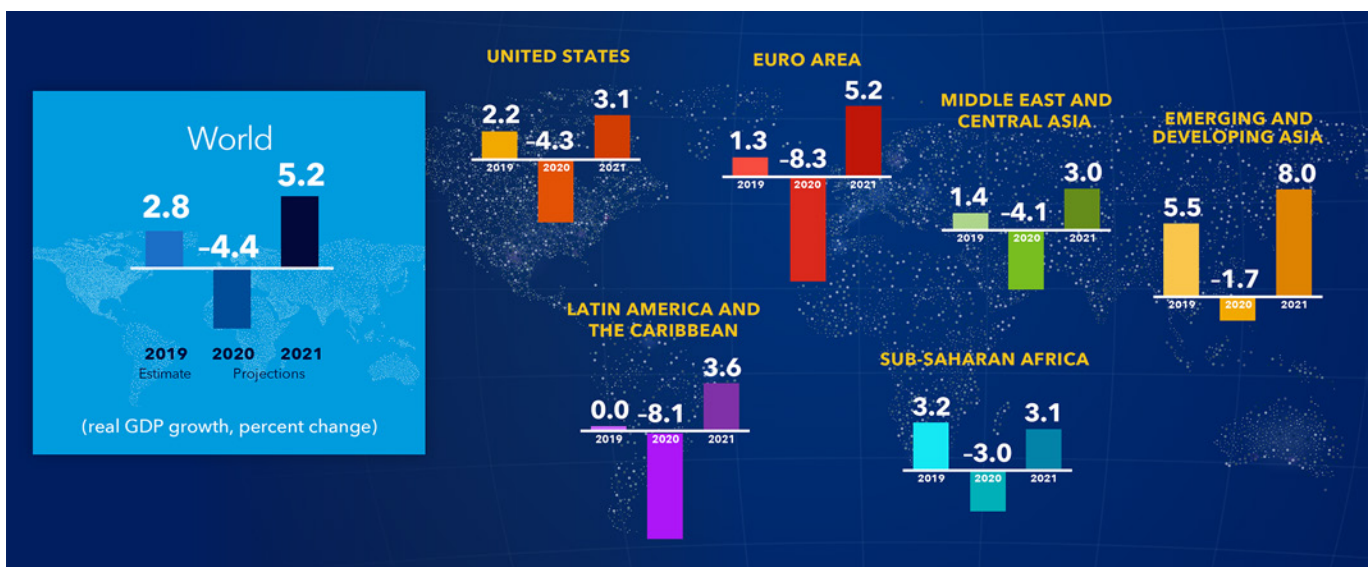


FIGURE 1 – Latest world economic outlook growth projections, as of October 2020 [1]

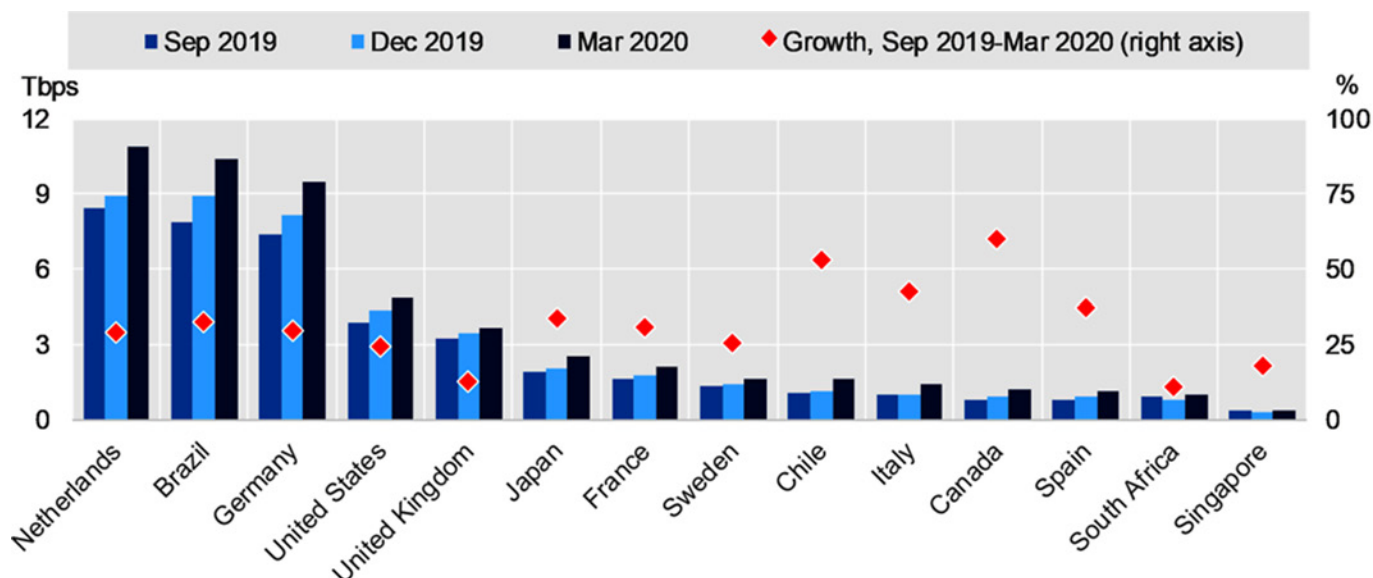


FIGURE 2 – Median Internet exchange points peak traffic aggregated by country in September 2019, December 2019, and March 2020, published by OECD based on data from Packet Clearing House [2]

The case for CSP

When the communication service providers (CSP) were under huge pressure, risking seeing its position diminishing due to the disruption brought by web-scale players, the ongoing crisis showcased that the investment in innovation for and in communication networks are of very high

return for the society (see **Figure 3**). Although there are multiple players able to provide end-to-end communication services that allow us to overcome these challenging times, if it weren't for the continuous investment in innovation made in the last decades by CSP, we would probably be in a very different situation. Suddenly, something heading into a pure commodity stage became of

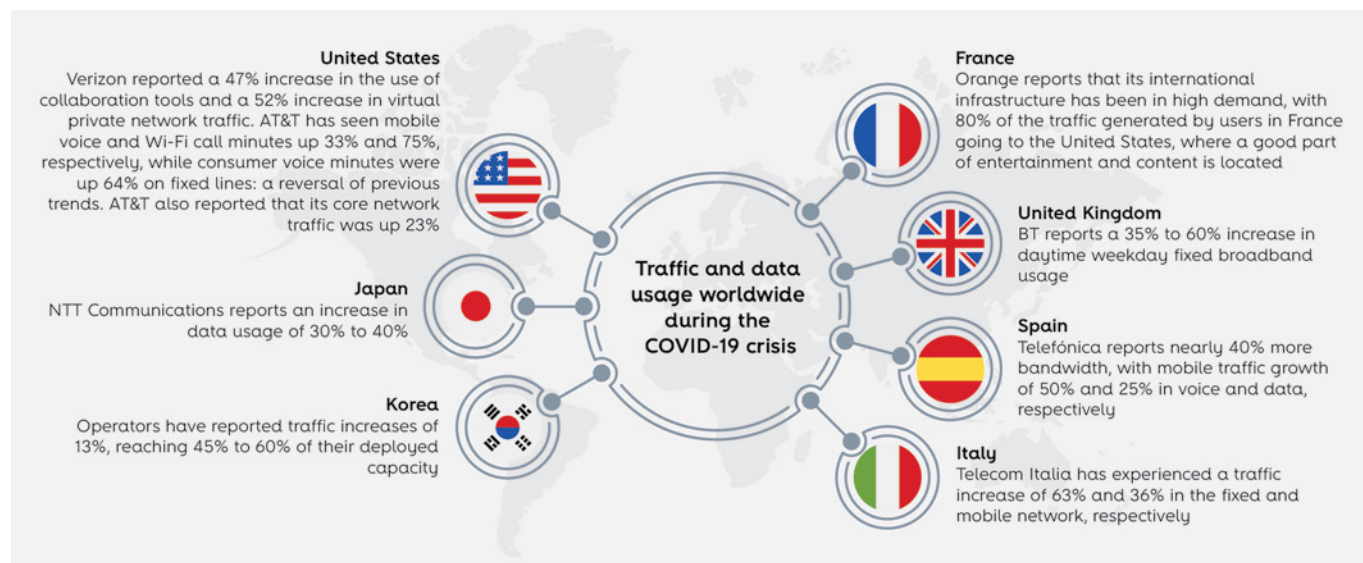


FIGURE 3 - Some key figures about the increased demand for traffic and data usage worldwide during the COVID-19 crisis [2]

most critical importance, minimizing the adverse pandemic effects.

One year ago, no one could ever imagine telecommunications' role in these last few months, with the worldwide lockdown. All over the world, CSP had to improve their networks, the characteristics of their services, and had an increased demand for reliable services, with a focus on the fixed ones. As mentioned in the Digital Leadership Summit, promoted by TM Forum, "globally, most telecom networks are seeing a rise in internet usage of between 30% and 45% with peaks being around 20% to 40% higher than this time last year (Source Nokia) and a 700% increase in videoconferencing apps" [4]!

When considering the current crisis's impact on CSP revenue, according to a report and the **Figure 4**, both released by GSMA Intelligence [5], "seventeen of the 27 groups recorded revenue growth year on year for Q1 2020, despite macroeconomic pressures triggered by the COVID-19 pandemic. Group performances were largely influenced by their geographical footprints, as the spread of the virus has varied by region. Total group revenue declined by 0.5%

year on year, compared to a 1.7% decline in global GDP over the same period, suggesting the telecoms industry has been less affected than many other sectors".

Such a soft revenue impact may result from the focus on innovation and the investments continuously made by CSP in their broadband accesses in fiber and mobile networks and enterprise digital transformation. These efforts allowed them to quickly support their Customers to fast adapt to the (current) crisis context enabling remote working, studying, and the definition of new business models, resulting in more/new revenue sources.

Indeed, CSP's focus on the last years in the digital transformation of their processes, channels, and portfolio made them more robust to surpass the current crises. It was also the reason they were (and still are!) better positioned to support their Customer digital journeys during this adverse time, being seen as Digital Service Providers (DSP) able to help Customers be more resilient, flexible and better surpass uncertainties and difficulties.

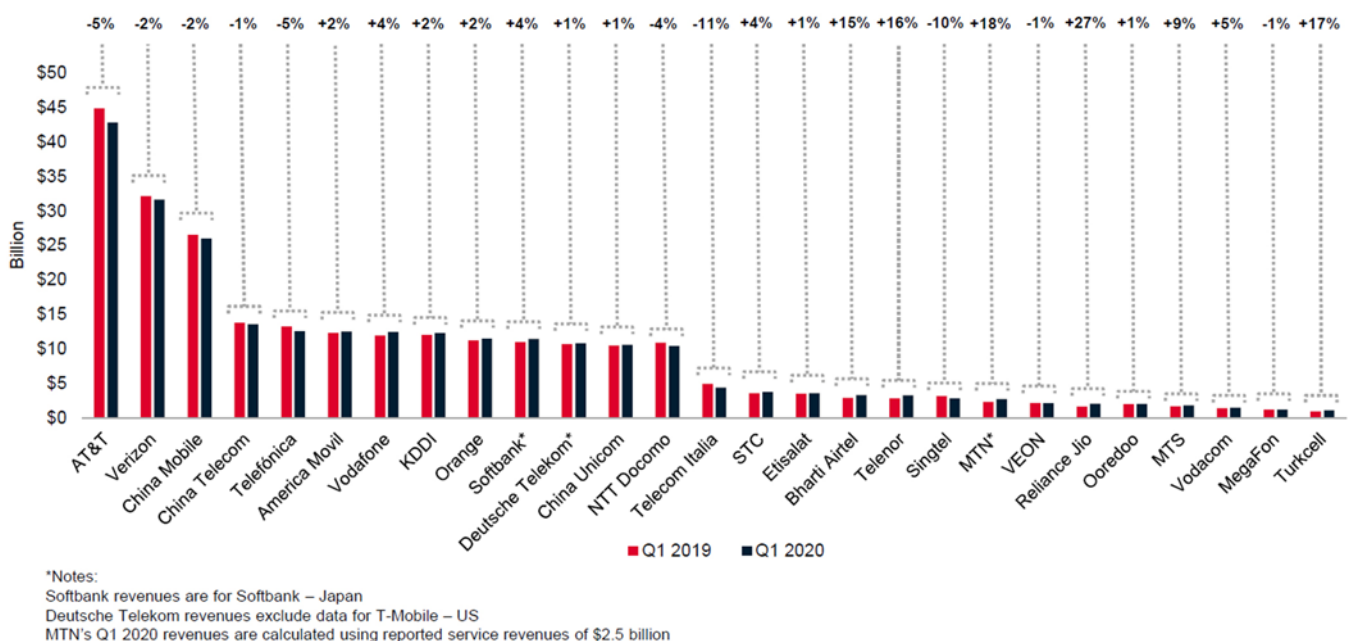


FIGURE 4 – Global financial benchmarking: total revenue, as of July 2020 [5]

Leading through: the new operating system

If there is something well known - but many times forgot - is that crises happen recurrently (see **Figure 5**). The sanitary crisis that we face today tends to obliterate the financial crisis that the world faced back in 2008, and before that, many others (including two global wars lived in the past century).

According to some surveys seen on the industry when discussing crisis, the best way to deal with those disturbing events (black swans sometimes called) is to be well prepared in terms of leadership (so that leaders inspire others and shape their actions) and guidance/directives (so that is clear where companies are going and that people are aligned on how to get there).

However, surviving successfully during and after a crisis also implies the capacity to innovate and transform. No matter the type of situation being faced, DSP (and even countries!) need to be prepared to react quickly and adapt their operating systems (OS), creating a new one that will rearrange their building blocks on top of agile digital processes and workflows.

This new OS will promote the necessary digital maturity to be better prepared to overcome difficulties and uncertainties that can strongly impact their everyday activities and operations, making societies outpace unforeseen crisis!

The importance of digital maturity

The readiness of a DSP's network and systems will directly contribute to a nation's resilience. For that

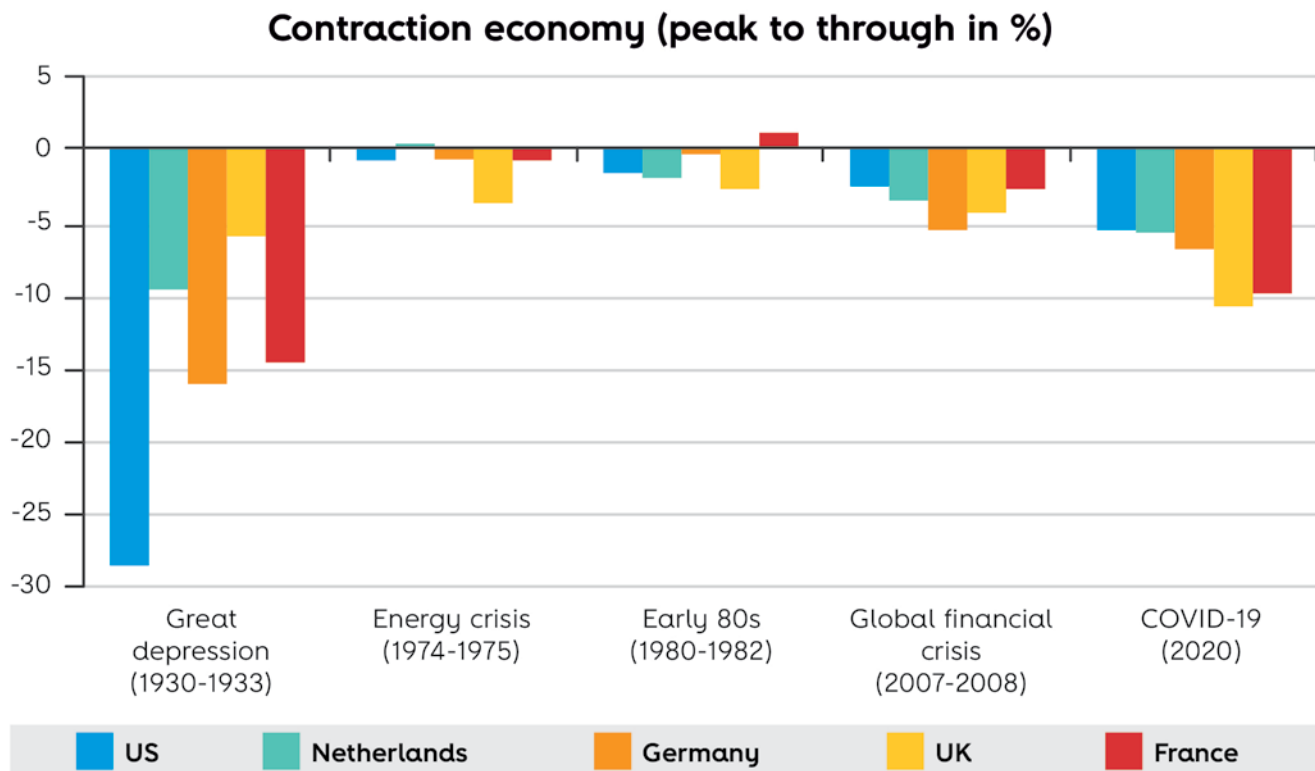


FIGURE 5 – The most profound economic crisis since the 1930s [6]

14 Leading through (and after) a crisis

fact alone, it is quite relevant that investment in resilient and better-performing networks is brought into the light spot. Conditions for making ultra-broadband networks, both mobile and fixed, accessible throughout the territories must be created, alongside investing in innovation that can make it more cost-efficient and easier to deploy and operate. On top of these networks, quickly deployable and highly scalable digital platforms to respond to society and business needs are fundamental to help build and maintain a resilient society during a crisis.

As seen in **Figure 6**, the COVID-19 crisis reshaped the world and pushed the massive use of digital services to a level never seen before:

- Transformed online shopping from a nice-to-have to a must-have around the world, which needs to be supported by a robust logistics system and contactless delivery services;
- Contactless digital payments quickly became the recommended payment method to avoid the spread of COVID-19. Massive adoption of

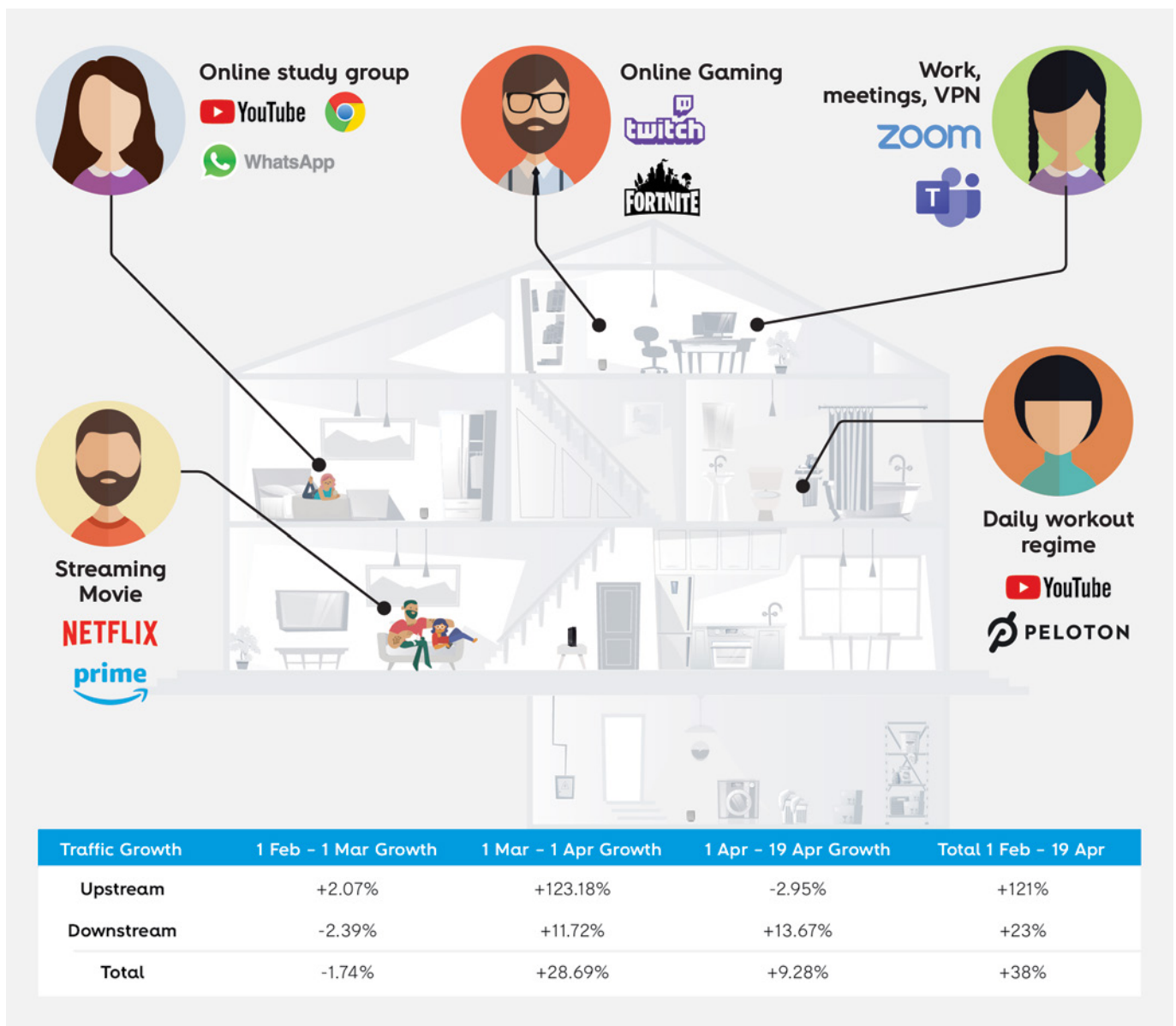


FIGURE 6 – Overview of the significant traffic types during the early stage of COVID-19 pandemic, each with different impact on overall bandwidth usage [7]

digital payments is enabling people to make online purchases and payments much safer and faster;

- Work from home became the rule and not the exception. Remote work is enabled by technologies already mature such as virtual private networks (VPNs), voice over internet protocol (VoIP), virtual meetings, cloud technology, working collaboration tools, but also mass-marketed other technologies such as facial recognition technologies that enable a person to appear before a virtual background to preserve the privacy of the home;
- As of mid-April, 191 countries [8] announced or implemented school or university closures, impacting 1.57 billion students. Many educational institutions started offering courses online to ensure quarantine measures did not disrupt education. Technologies involved in distant learning are similar to those for remote work but also can include virtual reality, augmented reality, 3D printing, and artificial-intelligence-enabled teaching;
- Telemedicine and telemonitoring are other examples of mature technologies that demonstrated to be very effective when containing the spread of COVID-19 while still providing essential primary care. Wearable personal IoT devices can track vital signs. Chatbots can make initial diagnoses based on symptoms identified by patients;
- As the last example, we could look at online entertainment. Although quarantine measures have significantly reduced in-person interactions, human creativity has brought the party online (see **Figure 7**). Content produced exclusively for OTT, cloud parties, or online streaming of live concerts have gained traction worldwide. There has also been a surge of online gaming traffic since the outbreak.

What we have just described can easily be translated as a level of digital maturity of a society: its capability to timely create conditions

Global application category total traffic share



FIGURE 7 – Global application category total traffic share during the early stages of COVID-19 pandemic [7]

to have a native digital society and to ensure security and trustiness of its use. It also reinforces the importance of stable, high-speed, and affordable internet. Regarding mobile access, 5G is expected to strengthen digital infrastructure and speed up digital transformation, allowing the growth of other multiple technologies, such as edge and cloud computing, artificial intelligence, mixed reality, and many others, all of them already being explored.

Once again, communication technologies play an increasing and decisive role in augmenting human society capabilities and empowering the fastest adaptation to (digital) change.

The new operating system

Just like the device's OS, which provides basic functionality for the device and affects how you interact with it, the DSP's OS is also of the foremost importance. It will define how infrastructural dimensions interact and integrate with different technologies and enterprise platforms, controlled by smart processes, to take the best out of its advanced capabilities – people – to produce the highly adapted (or at least flexible) outputs – portfolio.

This new OS must address to solve or, at least, to mitigate the negative impact of some of the following DSP fragilities:

- **Business inefficiencies** due to aggregation of services approach instead of services-oriented architecture approach, making it easier to adapt, grow and reuse existing assets to create new simpler and readily set up offers;
- **Network complexity, heavy and lengthy workflows** due to “growth by addition”, with onerous legacy. To enhance the Customer's experience, the solutions offered must be agile, and the answer must be timely;
- **Sizeable OPEX** due to poor network automation and low intelligence and self-adjustment, as well as the reduced freedom Customers still face when trying to autonomously configure a specific offer;
- **High occupancy rates in a call center** with basic issues due to low integration of autonomous and intelligent software agents, like virtual assistants, that can interact with users or other systems to solve low complexity issues or automate processes that had an increase on demand;
- **Reduced cloud approach environment and portfolio** due to the misfit of the current ones. The move to this type of environment facilitates networks, services, and portfolio automation and allow for a more flexible and agile capacity to respond to the increase of telecommunications and digital services demand while granting the scalability and elasticity needed in a time of crisis;
- **Lasting “not invented here” syndrome** where the open innovation concept is not welcomed since it implies sharing the revenues. In fact, “Open innovation has the potential to widen the space for value creation: It allows for many more ways to create value, be it through new partners with complementary skills or by unlocking hidden potential in long-lasting relationships. (...) During (the COVID-19) crisis, it could be wise to focus more on creating value than capturing value [3].

Alongside addressing the topics abovementioned, since this OS will hopefully be embedded in a deeply digital internal and external ecosystem, security and privacy concerns must also be safeguarded. As people use more and more digital services, security must continue to be a central goal, without impacting users' online freedom. Today cybercrime is a sophisticated and powerful reality, always looking for the right opportunity to emerge and negatively impact those using and providing digital services. This is true for citizens, enterprises, and countries, and therefore it should not be neglected when defining processes, choosing and integrating technologies, and exposing portfolios online.

Finally, the definition of a new OS must safeguard the most crucial asset available in any company: people! The brainpower's right engagement will instigate the necessary mindset to make the defined OS a well-success strategy that leads to real change. How to deploy, how is the workflow, how do we have a cross-collaboration among the different groups, it will all dictate the power and outcomes produced by the OS.

Leading after: strategic foresight

"War", "health", "climate", "money", "disaster" are usually words that easily come together with "crisis"! People, families, nations, and even the entire world may be affected by a crisis. Still, in the hardest of times, human ingenuity, solidarity, and innovation play a significant role in pushing forward so that a more resilient, advanced, instructed, and fair society emerges. For all these reasons, the COVID-19 pandemic, or other future crisis, should not be treated as a step back, a pause in progress, but as a transformative crossroads where DSP (and other companies and societies) can redefine itself through the previous described OS. This OS will, on the one hand, benefit from the learnings got from the unprecedented uncertainties brought by these

strange times and, on the other hand, for the DSP's ability to perform strategic foresight, a technique that will create conditions to plan for the known unknowns – see **Figure 8**.

Complementary to other predictive tools, *"strategic foresight also enables us to identify opportunities and amplifies our ability to seize them. (...) Moments of uncertainty hold great entrepreneurial potential. As Wack once wrote in these pages, "It is precisely in these contexts—not in stable times—that the real opportunities lie to gain competitive advantage through strategy." [9]*

In its turn, the constant identification of the known unknowns will help improve the assessment and selection of which emerging technologies a DSP should invest and integrate into its building blocks, and portfolio and which skills their teams must reinforce to be better prepared for the future. It will also promote the continuous adjustment of business processes and workflows.

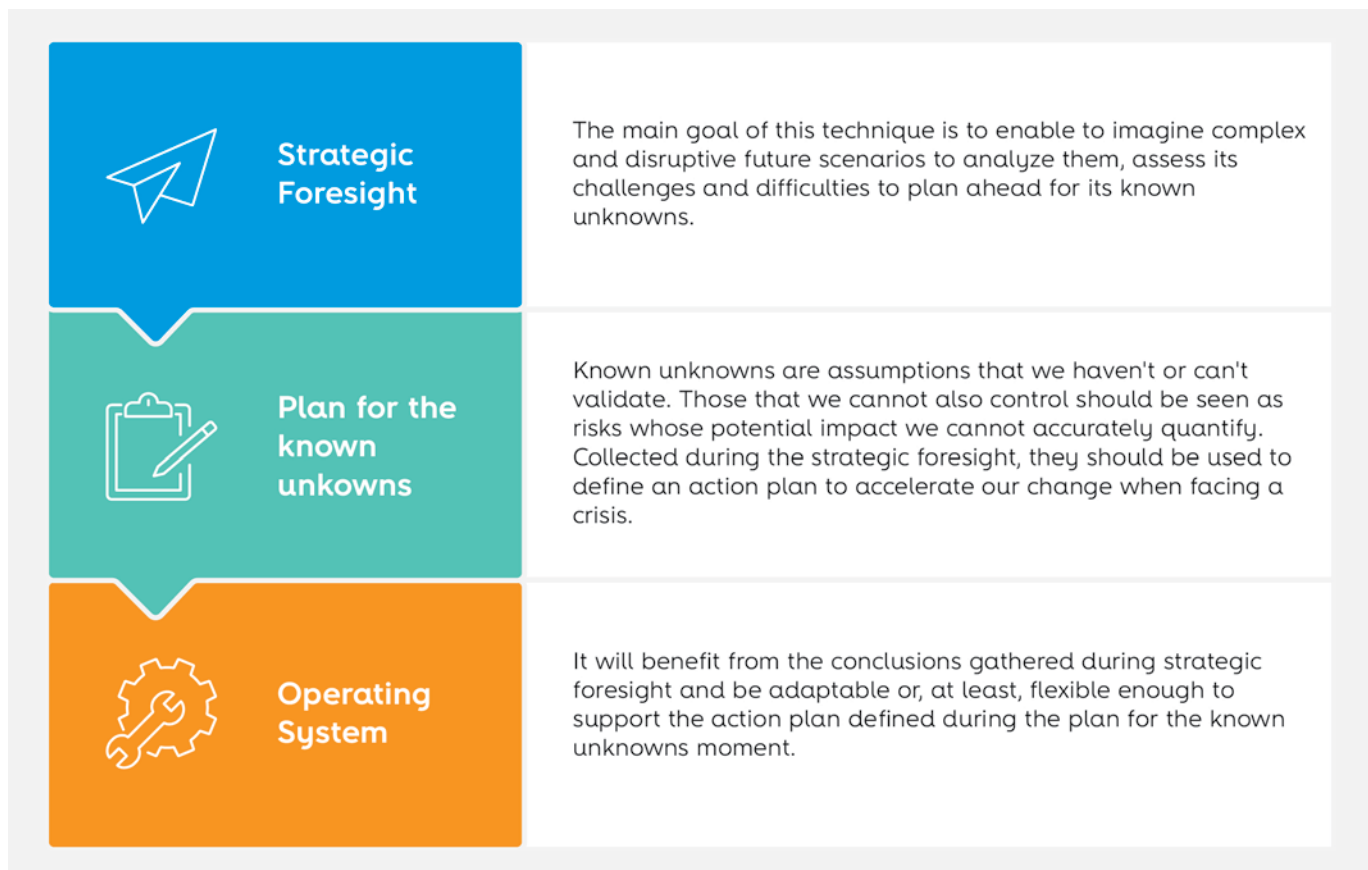


FIGURE 8 – How DSP's OS benefits from the "strategic foresight" and "plan for the known unknowns" techniques

Wrap-up

The definition of a new OS will allow DSP to boost network and service transformation journeys towards more efficient, dynamic, automated, intelligent and, above all, more crisis-tolerant workflows and operations. It will also strengthen DSP's ability to innovate and continuously self-transform not to survive but to overpass crisis together with its Customers, offering products and services that will:

- Have infused intelligence to anticipate how to react to possible new issues or to adapt to each one of our preferences as users;
- Foster the usage of augmented, mixed, or even virtual reality as a means to empower

humans on their activities, allowing to face the challenges either with more powerful tools or even without being there at all;

- Accommodate the gigantic leapfrog we have been seeing on data creation and bringing technology in hand to transform it into useful information that will continue to drive our businesses, our lives;
- Continuous get ubiquitous ultra-broadband network access at a lower price and empowering others to continue to add value on top of it.

That's what defines a future-ready DSP, and those are the ones making the difference whenever there's a need to tackle a crisis. 🌐

References

- [1] International Monetary Fund, "World Economic Outlook, October 2020: A Long and Difficult Ascent," International Monetary Fund, October 2020. [Online]. Available: <https://www.imf.org/en/Publications/WEO/Issues/2020/09/30/world-economic-outlook-october-2020#Chapter%201:%20Global%20Prospects%20and%20Policies>.
- [2] OECD, "Keeping the Internet up and running in times of crisis," 4 May 2020. [Online]. Available: <https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/>.
- [3] L. Dahlander and M. Wallin, "Why Now Is the Time for "Open Innovation"," Harvard Business Review, 05 June 2020. [Online]. Available: <https://hbr.org/2020/06/why-now-is-the-time-for-open-innovation>.
- [4] TM Forum, "Digital Leadership Summit: Transforming the customer experience: Pragmatic steps in the journey," in *Digital Transformation World Series 2020*, (Online), 2020.
- [5] A. Shabelnikova, A. Sawhney and A. Jha, "Global financial benchmarking: total revenue," GSMA Intelligence, 2020.
- [6] H. Erken, R. Hayat and M. van der Veen, "Global economic outlook: Coronavirus will cause the sharpest contraction since the Great Depression," 2020. [Online]. Available: <https://economics.rabobank.com/publications/2020/june/global-economic-outlook/>.

- [7] Sandvine, "The Global Internet Phenomena Report COVID-19 Spotlight," Sandvine, United States, 2020.
- [8] UNESCO, "COVID-19 - Education: From disruption to recovery," UNESCO, 2020. [Online]. Available: <https://en.unesco.org/covid19/educationresponse>.
- [9] J. P. Scoblic, "Emerging from the crisis: Learning from the future," Harvard Business Review, July 2020. [Online]. Available: <https://hbr.org/2020/07/learning-from-the-future>.



02

The after-pandemic market

Carlos Rodrigues, Altice Portugal

carlos-rodrigues@telecom.pt

Luis Mestre, Altice Portugal

luis-mestre@telecom.pt

Manuel Dinis, Altice Labs

manuel-dinis@alticelabs.com

Ricardo Ferreira, Altice Labs

ricardo-j-ferreira@alticelabs.com

The COVID-19 crisis arrived without knocking. The economic damages are here to stay for the years to come. The way people use to live and even the markets suffered transformations that may remain for an extended period after the crisis is overcome. Among other sectors, telecommunications played a vital role, minimizing and mitigating the crisis's impact on the economy and people's physical and mental health. However, this hostile event is not an end but the beginning of a new way of living and doing business that impacts everyone worldwide.

Keywords

Crisis; TELCO; CSP; DSP; Market; Digital; Network; Resilience

Introduction

In a global crisis, like the one caused by COVID-19, the orientation beacon for companies and authorities alike must be the immediate protection of people's health – both physical and mental – along with the safeguard of the economy. The avoidance of market disruptions and the consequent economic downfall, with severe and dramatic side effects for businesses, people, and global social welfare, is crucial.

Therefore, business continuity digital strategies are of paramount importance, allowing the companies to operate in stringent conditions. Telecom operators play a crucial role in this action scene, being the survival bridge among companies, institutions, and consumers by allowing the needed connectivity for a digital society to strive (whether or not in a crisis context).

In the next sections, we tried to anticipate the impact of the COVID-19 crisis on the market and emphasize telecom operators' role in these turbulent and dangerous times.

An already challenging time for TELCOS

Until early this year, the wish for an ever more digital world forced the TELCOS dynamic business landscape through continued incremental evolution on networks, service delivery platforms, and consumer devices towards ubiquitous availability of broadband connectivity.

Societies pushed telecom operators to offer resilient, trustworthy, flexible, and efficient broadband connectivity to effectively support market demands. From personal communications to real-time video and entertainment, up to the most diverse and challenging business-to-business use-case products

and services (cloud, data and analytics tools) all perceived at the level of a commodity – taken as granted by both individuals and companies alike:



Fuelled by ever more powerful devices, such as smartphones, mobility integration with multimedia and productivity tools brought convenience and efficiency, propelling the services market and leveraging the virtual economy where a growing number of over-the-top players promoted the growth of entertainment services.



Companies continued with the journey for work-life balance by experimenting with telework, expanding their market through improved market knowledge, potentiated by robust data and analytics tools on top of telco services. They also start to adopt incremental digital transformation processes (often cloud-based and in real-time) that favored e-commerce and online transactions and the efficiency of the production, supply, and distribution chains.



Digital social networks also created new real-time social dynamics, new markets, and commercial channels, opening space for virtual global debate that helps develop and shape society.

In a nutshell: individuals were enjoying a vast panoply of multimedia services; the companies' digital transformation was taking place in all business sectors; and telecom operators were playing a fundamental role in that course of evolution.

The crisis earthquake

The emergence of the present COVID-19 pandemic brought a new societal reality. This abrupt and unexpected public health crisis spiraled into a severe worldwide economic, social, and psychological turmoil that we all involuntarily plunged into:



From the public health perspective

The COVID-19 pandemic provoked psychological isolation, distress, the feeling of hopelessness, and the ramping of psychopathologies, namely depression, among the most vulnerable.



From the economic perspective

The industry supply and demand curves became unbalanced or disrupted; the physical commercial channels threatened to collapse; the supply chains and production operations were interrupted or delayed.

Governments are struggling to devise innovative regulations to face these challenging times, focusing on extended social support strategies to prevent massive unemployment and economic standstill due to temporary crowds control regulation, physical commerce shut down, and the closing of borders. Suddenly, we witnessed what will be studied in History as the fastest forward life transformation of all times. Wars, natural disasters, and economic crises always derived societal changes, but never before was the world exposed to such simultaneous challenges! The globalized world plan became real; the movements of goods and money created an economic and a social interdependence never seen before! Unfortunately, the economic globalization proved not to be supported by strong supranational institutions that could manage better the outbreak in its early

stages before becoming global. Companies proved to be more agile than states, anticipating the lockdown and changing drastically in a few weeks! Although this digital transformation was already (slowly) happening, it was greatly accelerated by COVID-19, forcing companies to reinvent themselves in a short period to compete or merely survive in the current market conditions.

TELCOS were one of the main enablers of this transformation. The investments continuously made in the massive diffusion of broadband accesses in fiber and mobile networks demonstrate their extreme importance for providing services and technological platforms that streamline processes with less investment, allowing the fast emergence of new business models. The robustness and resilience of these networks allowed, without constraints, the sharing of information and drove the implementation of new contactless digital solutions for different sectors, allowing the professional activities remotization, social life continuity, and the enrichment of family lives with mobile, Internet, and TV services.

Although the crisis footprint will cause damages for the years to come, we will handle it. Its legacy and lessons will make us stronger and more prepared for similar events that we all know will come again.

A new normal emerging

This crisis contributed to a new societal reality, named "the new normal", where some of the changes we now experience came to stay, leaning people's behavior and needs towards the virtual as a way to substitute physical experiences. Contactless social interaction will likely continue to be preferred, remote collaboration and mass remote work will be the new norm, and the increasing need for digital services will foster the massive uptake and usage of new tools and services. Without any doubts, the recovery will be digital, and only the most flexible, agile, and efficient players will survive in this fast-moving environment.

The pandemic created a once-in-a-lifetime opportunity to transform business models, namely in the services area. The reality showed that both customers and suppliers are prepared to receive and deliver high-quality services upon digital platforms, with productivity gains for those prepared to embrace this new challenging world:



Schools and universities

reinforced online learning and digital classrooms



Globetrotters

discovered how video calls could be more efficient in significant issues



Restaurants focused on takeaway, and groceries stores concentrate on online and home delivery as their primary channel



Banks shifted to remote sales and evolved its digital self-care to allow mortgage and flexible payment arrangements



Doctors embraced telemedicine



Manufacturers are actively developing plants for "light out" factories



Retailers are reshaping its shore chains, creating better store experience driven by omnichannel while closing their less profit stores



Major corporations are evaluating the need to have expensive headquarters

The disruption in the way services are currently provided, with the need to adopt digital tools without sacrificing quality or even losing security, will continue. Actually, although they force the population to take a different approach, they are generally more effective, and the preferential adoption of virtual channels will tend to be accelerated as soon as some prejudices/ issues related to security and privacy are overcome.

Telecom operators will surely attend this transformation, and new technological solutions are already available or being developed to allow:

- Broadband access with even higher speed and lower latency;
- Massive data integration systems prepared for internet of things and big data scenarios;
- Cloud-based offers to speed-up availability to the final customer, with the best guarantees of cybersecurity.

Opportunities and defies fountain

Just like the societal changes mentioned above, emerged customer behavior changes are here to stay: the pandemic bridged to digital "late majority" and "laggards" segments that probably will continue to use digital from now on, with higher expectations without equivalent willingness to pay. The return to pre-pandemic demand levels is highly improbable and will be different across sectors.

Therefore, the economic agents must revisit the legacies (people, process, and systems) and continue to reform their business, becoming more cost-effective to survive the storm but ensuring they keep the muscle to the bonanza when it arrives. The skills gained during the pandemic cannot be lost: after the global health crisis will emerge a global economic one, and only those who can best adapt will survive and emerge even stronger. As customers embrace digital interaction with their sellers, their reference will not be the seller industry, but the best in class digital native

providers like Uber, Netflix, Disney, and Amazon. So, every company must redesign all customer experiences for a new world with less and safer human contact.

Every business must reassess its fundamentals; the recovery will extend far beyond digitalization:



Data collected during years from customers and their interactions are the main leverage that the legacy companies have to face the newcomers.



Digital analytic capabilities can not only drive top-line but also improve efficiency and efficacy across all value chain.



Industry 4.0 can unlock significant value in this new age using the tools already available (big data; artificial intelligence; machine learning; IoT; robotic process automation, and chatbots) to increase productivity, decrease downtime, and increase overall quality.

Yet, as companies expose their systems to the web, cybersecurity became even more critical. The phishing campaigns and the cyber-attacks that traditionally targeted the big companies are now a threat across all sectors and company sizes.

In short, operations must be optimized; the traditional business rules and forecast will not fit in the new blink changing world. A clear vision from

the management must be second by execution focused on the agile framework to deliver systematic improvement in a high cadence. The old way will not work anymore; these turbulent times will separate the chaff from the wheat.

Conclusions

The COVID-19 crisis arrived unexpectedly, but History showed us that it is not the first time and certainly will not be the last. After an initial panicking period, people gradually retook their activities to avoid a severe economic downturn. Although the crisis did not end and the economic damages are not yet fully known, we already see and expect that in the future these changes will remain, namely, a more digitized society where shopping, work, and entertainment will never be the same.

The humans' resilience will help turn this page, and the lessons and learnings will stay engraved in our behavior. Technology proved, once again, to be one of our most important allies, covering all fields, from the pharmaceutical to the telecommunication sectors, and helping to reduce the virus faster spread. Telecom operators have emerged as one of the most critical sectors among food, water, and electricity during this crisis. Resilient broadband connectivity allowed the world to "keep moving" from work@home to school@home, shopping@home. Still, the experience was not perfect since no business was fully prepared for the lock-out, living room for digital improvement in the years to come.

This event is not an end, but the beginning – the beginning of a new way of living, a new epoch that will lead us stronger to the bonanza again. 🌐



03

Industrialization and mass production challenges

Hélder Alves, Altice Labs

halves@alticelabs.com

José António Carvalho, Altice Labs

jose-a-carvalho@alticelabs.com

Nuno Balseiro, Altice Labs

nuno-balseiro@alticelabs.com

Pedro Luís Ferreira, Altice Labs

pedro-l-ferreira@alticelabs.com

Sérgio Domingos, Altice Labs

sergio-c-domingos@alticelabs.com

To overcome unexpected constraints, it is vital to completely systematize and organize the whole industrialization process. It will ensure that the manufacturing process is as portable and adaptable as possible to enable the manufacturing site's change whenever and when circumstances require, even without a local presence at the factories, as has been the case during the current pandemic crisis.

Keywords

Industrialization; Manufacturing; Mass production; Quality assurance; Hardware; Crisis

Introduction

Industrialization is transforming a prototype into a product that can be manufactured and the subsequent training to manufacture it competitively: cost, time, reliability.

This article aims to provide an integrated view of all the industrialization process, from development to product delivery, summarizing the manufacturing process and quality aspects while also analyzing the importance of its resilience to risks and adversities, such as the COVID-19 pandemic crisis that we are facing.

Industrialization

Industrialization as a process (see **Figure 1**) starts with defining the product's requirements for hardware, software, mechanical and other factors, which will have to consider all client and industry needs.

The next stage is to develop all the elements necessary to build the first prototypes, which include schematics, printed circuit board (PCB) layout, bill of materials (BoM), 2D and 3D models of all modules, enclosures, labeling, gift box, flyers, packaging, among other details. The right choice of materials is essential since it dramatically impacts cost, reliability, repair, and maintenance.

In parallel, embedded software starts to be developed, and unitary tested to ensure that as soon as the first units come out from prototyping manufacturing, the combination of the hardware and the software bring-up is performed. At this time, all main tests start, including but not limited to the streams described in **Figure 2**.

Part of the software includes the internal requirements to support the manufacturing tests, providing tools for the programming and test of all the hardware functions and interfaces. These tools will ensure the maximum test coverage either at the mass production stage or at the return merchandise authorization (RMA) process (refurbishing).

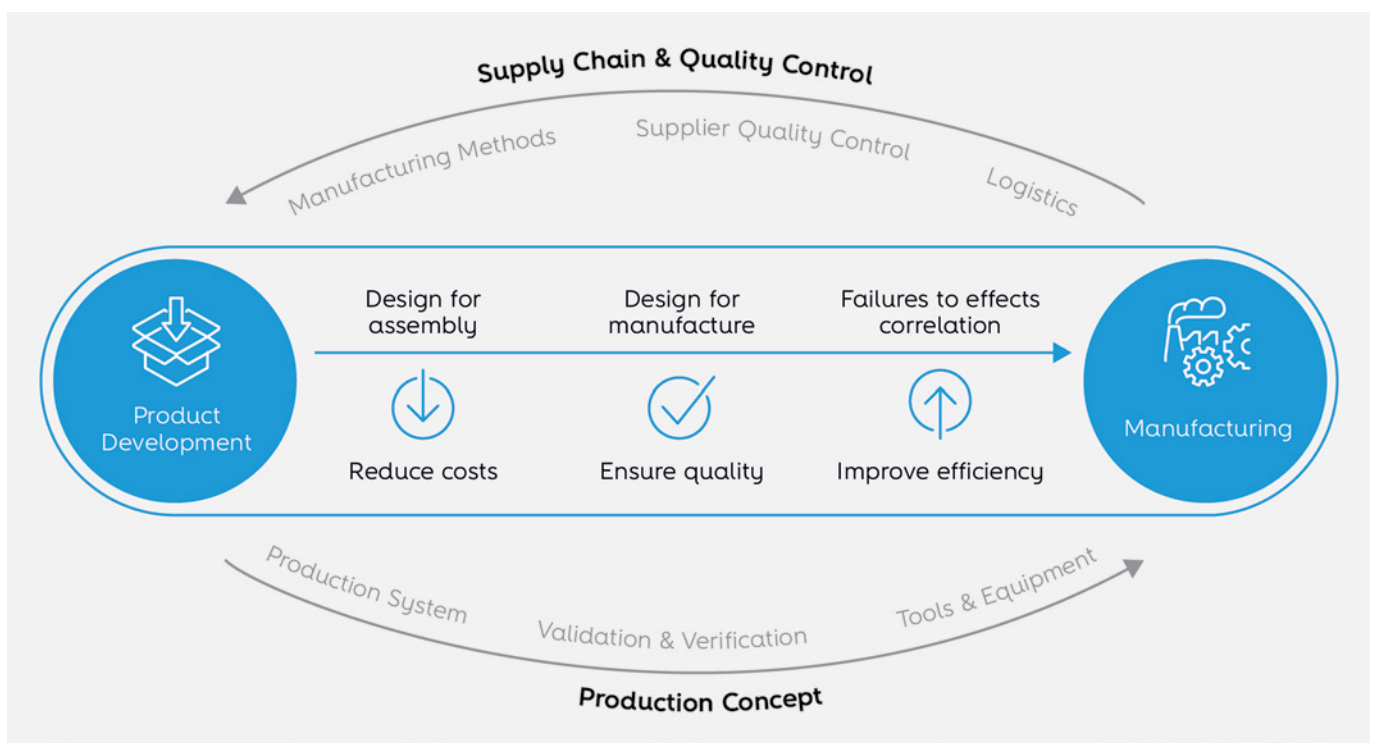


FIGURE 1 – Industrialization & Design for Manufacturing

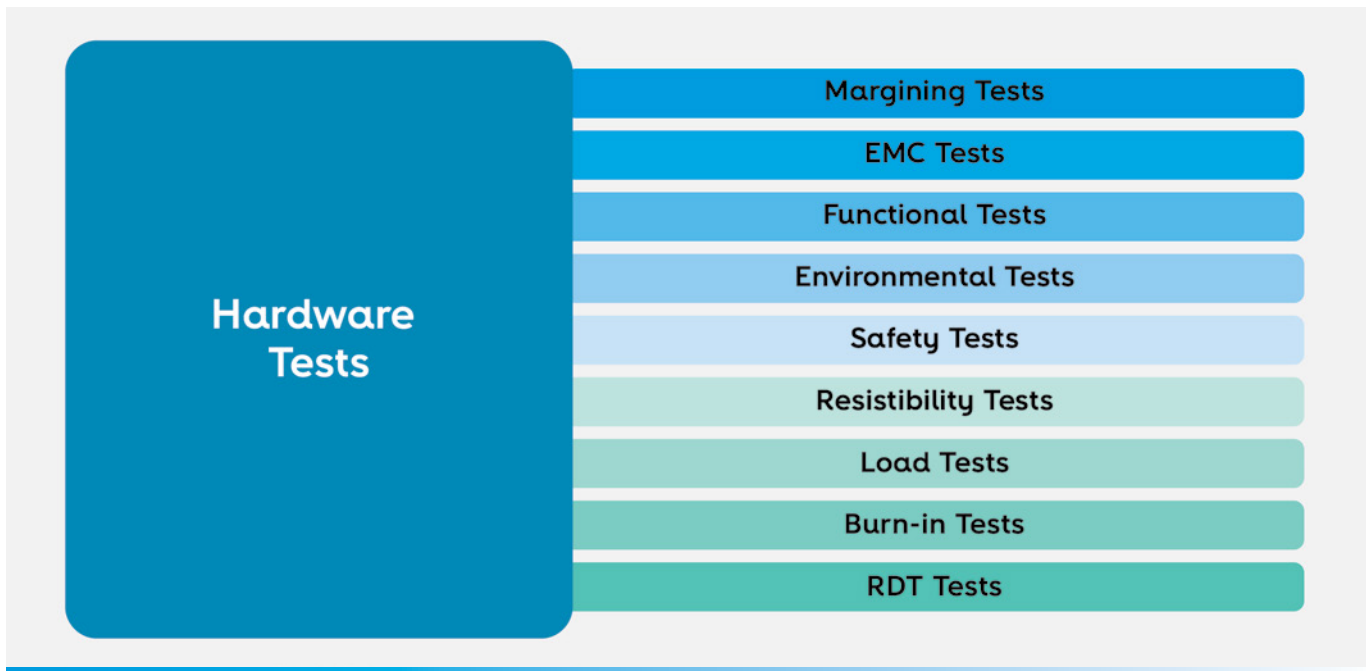


FIGURE 2 – Main hardware test streams

All the information required for industrialization and manufacturing is collected to create the specific product technical database during each stage. In other words, industrialization starts when the product is conceived and, along the way, a collection of all the technical data needed for the manufacturing process is gathered. The industrialization process's quality will impact the manufacturing process, contributing to achieving cost and time reduction while improving margins.

Manufacturing is the final stage of the industrialization process, defining workflows and procedures to manufacture a product with the suitable components in the shortest period while guaranteeing quality by performing a full test coverage.

Although during the current pandemic crisis, with imposed travel restrictions, the maturity of Altice Labs' industrialization process enabled the manufacturing of new products, with new technical specifications, in factories located abroad, without the need to perform on-site inspections, we continuously work to improve all the methodologies and tools to go even further.

Mass production

The mass production goal is to reproduce many samples of a given product with quality, in the shortest time and at the lowest price, in a business where the margins are small and very dependent on the overall process quality (see a factory ground floor example in **Figure 3**).

The more the manufacturing process is automated, the greater will be the repeatability with less likelihood of errors. In mass production, the operator should not need to make any decisions, limiting himself to comply with the work instructions set for his station.



FIGURE 3 – Factory ground floor for mass production of hardware

Process smoothness relies upon the design for manufacturing (DFM), starting with the product's requirements fine-tuned in the prototype production, which is the perfect time to validate and correct all the negative aspects that may impact mass production. Sometimes, however, a short time to market (TTM) leads to a lack of time to incorporate the changes requested by the DFM. In this case, a rigorous risk analysis must be observed and weighted to decide whether to bear the costs of delaying the product's availability or, instead, move forward, compromising the DFM's perfection.

Although there are duly standardized and transversal processes and instructions regarding production and inspection, all tasks must be adapted to the assembly line, whether in the context of facilities, equipment, tools, and human resources.

Besides the DFM process, it is highly recommended to implement a new product introduction (NPI) phase, with a smaller production, to validate and adapt the entire line setup process, production tools, and procedures according to the manufactured products. A good analysis of the whole production dossier carried out in the pre-setup phase allows predicting process times and production rates. However, only the NPI phase will allow getting close to reality, having already implemented all the optimization possibilities either in terms of:

- Automatic assembly equipment;
- Sequencing of tasks based on operators;
- Definition and adoption of line layouts.

Manufacturing tests are part of the mass production, from the raw material inspection to the final quality control analysis. Before the first delivery of a new product to any Customer, it is necessary to demonstrate the product's mean time between failures (MTBF) goal through live cycle acceleration, in a process called reliability demonstrations test (RDT). With RDT, a predefined set of product samples is exposed to the aging caused by multiple temperature cycles inside a climatic chamber while running a set of functional

tests. Newer products can only be delivered after having completed the first customer shipment (FCS) without failures. This step is essential to commit to an annualized failure rate (AFR) of less than 2%, required for all Altice Labs hardware products.

Manufacturing tests and quality assurance

Quality is the most crucial factor in mass production. The goal is to find the best balance between production costs and times while improving the quality, resulting in better reliability.

Control points start very early in the manufacturing process (see example in **Figure 4**), beginning with the selection and inspection of the raw materials, and including steps to ensure the product's integrity throughout the production phase until it reaches the tests. Solder paste inspection (SPI) and automatic optical inspection (AOI) pre-flow and post-flow are examples of the steps mentioned above. These checkpoints allow the immediate identification and correction of errors during the process, avoiding the recurrence of issues.



FIGURE 4 – Automatic optical inspection

Complementary, all the preventive maintenance based on manufacturing equipment calibrations and correct verification of their configuration

guarantees the proper operation, resulting in flawless manufactured products.

Concerning quality assurance in mass production, Altice Labs tests all the manufactured units instead of sampling, performing electrical and functional tests. Test plans are designed to maximize hardware test coverage, widen the automated tests that decrease testing time and costs, and improve the final quality and business margins. All test scenarios are built taking into account portability, scalability, reliability and high availability, including equipment backups.

Another concern is related to the documentation that must be complete, structured, and easily understandable to communicate the essential knowledge to the workers involved. Training is also a critical point in the knowledge transfer process. Altice Labs usually provides on-job training for its products in the production lines and ensures test setup validation on site. During manufacture, production partners perform regular testware verification and calibration in the manufacturing test lines, retesting their golden samples, a set of products previously produced that conform to all the requirements and can be used for comparison later in the process.

The availability of the appropriate information systems and the effective management of the teams that integrate the entire process are the basis of the business's support and resilience. Likewise, ensuring traceability by keeping per device records of the machinery used in the production, the lots of the raw material assembled, and the testing pass/fail complete results is a crucial step to understand and close the quality loop.

It is not possible to ensure both quality and competitive prices in the products without high 1st pass yields (number of good vs. defective units produced without rework). Therefore, maximizing results and other key performance indicators (KPI) is a permanent priority. Manufacturing partners are committed to providing periodic reports about the entire manufacturing processes, including direct visibility about testing yields and live

analysis. Regarding test criteria, initial thresholds are defined according to each product's complexity and historic and afterward adjusted as production evolves.

Whenever the yield is less than 100%, even the smallest failure entails understanding the cause and its immediate correction since it is in the efficiency of the business margin. In addition to an increase in costs, rework requires a second intervention subjecting the affected components to complementary thermal stress that may not benefit the product.

Recurrent failures should be given the maximum attention, as they may indicate a systemic problem (manufacturing, design, or other) that is only perceived in the presence of a larger number of samples during the manufacturing process than the prototyping phase.

During the pre-industrialization phase, prototypes are verified, and in-circuit tests (ICT) project specifications are prepared, when required, by verifying, analyzing, and maximizing coverage and placement/distribution of test points. Boundary-scan can also be used in compatible boards to increase test coverage with a very accurate diagnosis in case of failure. Finally, it is essential to perform BoM analysis to optimize it to mass production and remove unnecessary components, sometimes used only for development or validation purposes, and not need in the final BoM.

Test applications used in the manufacturing of Altice Labs' products can either be designed and developed by Altice Labs or specified by Altice Labs and developed by the manufacturing partner with Altice Labs validation. The advantage is taken on the knowledge and experience acquired during the validation tests and re-use in manufacturing test lines (know-how, test scripts, scenario designs, auxiliary test equipment integration like traffic generators, spectrum analyzers, power meters, for example). Altice Labs develops specific test applications for each product, ensuring maximum coverage and minimum test duration, helping to decrease test

costs. These applications must allow full control of manufacturing test line parameters like thresholds and provide all required information like results, cadence, yields, KPI.

The next phase is to deploy and follow-up. When a new product comes to the manufacturing test line, a functional test application is deployed, and pass/fail thresholds are adjusted if needed, considering the test results with new units from the production line. Altice Labs usually has a close follow-up on the manufacturing test line, on-site, monitoring all the test stations using golden samples as reference. Remote monitoring takes place as soon as a high confidence level in the process is reached.

Finally, it is time for the NPI production itself. Using a control run with a smaller quantity of units, Altice Labs can validate product quality and evaluate its stability. Besides, by analyzing data collected during the control run, both product and manufacturing tests can be improved to prepare mass production with the highest efficiency.

Upon the manufacturing process's conclusion, a set of random samples of finished products are collected for the out of box analysis (OBA) - see **Figure 5** - in a quantity that depends on the lot size. This last test phase will verify all product stages, from the visual inspection of the external packaging and labels (gift box) to the product's internal arrangement and its accessories and user guides. It will also verify the performance of a set of functional tests to ensure that all the products are effectively working as required.



FIGURE 5 – Random selection of products for the out-of-the-box analysis

In parallel, additional tests are performed in other product samples to ensure the products' continued reliability. The ongoing reliability test (ORT) phase is designed to capture defects that are not necessarily detectable by the standard manufacturing tests or OBA. This phase includes a set of non-functional tests, namely thermal shock, high temperature and humidity storage, burn-in, vibration, and drop test.

In these last stages, no failures are allowed. If any occurs, Altice Labs must be immediately notified by the manufacturer, and the production line must be stopped until the failure root cause is found, and preventive measures are adopted to prevent it from happening again.

The manufacturing process is not static and is usually fed with information from the after-sales service to ensure the constant improvement in the performance and quality of Altice Labs products.

Challenges, risks, and threats

Cutting edge technology companies such as Altice Labs face several challenges:

- Shorter innovation lead-times;
- Time to market competitiveness;
- Cost reduction;
- Mass customization demands;
- Increasingly complex products;
- Geographical dispersion;
- Inventories subject to rapid depreciation;
- Immediate fulfillment needs.

The COVID-19 pandemic increased these challenges, bringing new risks and threats with substantial impact on businesses. Transport freight costs increased the logistic costs and the

delivery time, thus affecting major products and services. Manufacturers of electronic components that depend on raw materials also felt the pandemic effects and, consequently, have higher lead times and suffer temporary supply chain disruptions.

Resiliency must be grounded on contingency plans to overcome the significant risks with high impact, identifying the actions to be taken if an unexpected event or situation occurs to recover normal business operations. These plans exist either for negative or positive events, such as many purchase orders that overload business delivering capacity and may lead to a decrease in quality or increase in delivery times that may damage the company's image.

Typical major risks include fire, flood, earthquakes, main power failures, loss of big clients to competitors, data loss/hacking/theft, and critical employees leaving to competitors, to name a few. In the manufacturing industry and mass production, additional risks must be considered (see **Figure 6**), such as the inflation of raw materials or labor prices, high lead times for raw materials delivery, product demand variations, and geopolitical constraints in accepting hardware manufactured from specific countries.

How to be resilient in the face of these significant risks?

In the case of raw materials, the DFM must include, whenever possible, at least three alternative options for the components of the BoM to ensure negotiating capacity as well as to mitigate longer delivery times. Other options may include using alternative distribution channels, having short/mid time forecasts from the clients,



FIGURE 6 – Major risks associated to the manufacturing industry and mass production

and as a last resource, stocking, with the inherent risks and costs.

To overcome any geopolitical constraints, it is vital to completely systematize and organize the whole industrialization process. It will ensure that the manufacturing process is as portable and adaptable as possible to enable the manufacturing site's change whenever and when circumstances require, even without a local presence at the factories, as has been the case during the current pandemic crisis.

Although the strategies adopted to mitigate these risks are regularly evaluated and updated, we are continually challenged with new variables and threats that have to be considered in the business strategy, contributing to improving the companies' success in this area. 🌐



04

Artificial intelligence impact on operational models

Luís Cortesão, Altice Labs

luís-m-cortesao@alticelabs.com

Pedro Miguel Neves, Altice Labs

pedro-m-neves@alticelabs.com

Rui Filipe dos Reis e Sousa Pedro , Altice Labs

rui-d-pedro@alticelabs.com

The dynamic and ever-changing telecommunications industry is nowadays under huge pressure! To succeed, communication service providers must be ready to quickly cope and adapt to a continuum of technological context and usage patterns due to the rapid network technology evolution, societal evolution, and unexpected life-changing events.

Based on these changes, service providers must prepare to address new challenges that will impact systems' development and deployment methodologies and the established organizational and operational management practices. This is where artificial intelligence comes to play!

Keywords

AI; Operational model; Autonomous; Data; Analytics; Systematic operating model

Introduction

The infusion of artificial intelligence (AI) technologies is a centerpiece in the evolution of processes of organizations in multiple sectors. AI makes it possible to build software systems able to reason and decide better than humans or legacy software systems, and to extract previously undiscovered knowledge dimensions from data. These new software systems leverage the creation of a new generation of work processes: fully automated (obviating human activities in the process workflow), highly adaptable to changes without requiring deep process reengineering, and highly predictive of future happenings.

This new generation of work processes will become the foundation of a new era of operational models, which will be autonomous, intelligent, efficient, self-organized, and predictive. A set of models will make organizations prepared to embrace frequent and rapid changes in their domains, a constant in modern societies, and highly reinforced in the new normal after COVID-19. A new operational model that will pave the way to restructure traditional operations towards unparalleled levels of efficiency.

Concretely for the telecommunications industry, the new operational model must be ready to quickly cope and adapt to a continuum of changing technological context and usage patterns due to the very rapid network technology evolution, societal evolution and extraordinary, and/or unexpected life-changing events. Based on these changes, service providers must prepare to address new challenges that will impact systems' development and deployment methodologies, as well as the established organizational and operational management practices.

In this article, we will elaborate on the necessary changes that will allow business and data science fields to meet, how AI literacy and data culture play a crucial part in this AI infusion process, and, last but not least, how existing organizational

and operational management practices must be equated and restructured to achieve an autonomous operational model.

Business and data science

AI literacy

With the advent of digital transformation and the advances in computation power, AI is becoming a more accessible technological area and gathers enormous attention. It is clear to see that, alongside the tremendous industry traction that AI has gained, there is also a proportional, if not larger, amount of hype around it. This extravagant perception of AI is often a product of individual ignorance and exaggerated publicity, one of the key contributors to the failure of AI projects [1] [2]. As natural as it is, this lack of awareness occurs on the dark side of our education, a gap that exists between the intricate details of technology and the business cases tackled by organizations. However, this gap can be covered with an increase in literacy around the subject, providing a level of understanding about AI similar to what we have today regarding computers. Nowadays, most people are comfortable around the idea of owning and interacting with a computer. They understand its impact on their lives and how they fit in everyday life, something that wasn't that common forty years ago. That is the shift that we are currently in need of. It regards the education of our general population, people who don't necessarily develop technological products or services. A group that will be, and a part of it already is, impacted by AI technology. It is paramount that they know what AI is, its benefits, how AI systems generally work, and how to engage with them [3].

Despite the effort needed to educate the general population, AI literacy needs to be pursued even further. The leaders who stand on top of

companies need a good understanding of AI in order to start measuring the impact on the markets they currently find themselves in and what internal changes are necessary to cope with this reality. Companies' products, services, and operations need to mutate in order to merge with this future. Their teams must be transported to this new reality, but this change is not enough. Organizations need to clean up their houses and focus on a systematic approach to information architecture. This translates into building a solid data culture that brings down their massive data siloes and harmonizes data access with carefully documented catalogs. Understanding that AI needs a good quality set of data is as important as knowing how it works.

Business-driven AI

Nowadays, it is strategic for any digital-related organization to achieve business impact with data and AI techniques. Although the AI discipline itself is not new, the rationale for the current wave of disruption is three-fold:

1. More and more **data** from heterogeneous natures and sources is becoming available and ready to use, mostly due to the digital transformation worldwide;
2. From a technical point of view, advanced **data analytics** and **data science** disciplines are getting more and more advanced to turn this ocean of raw data into insights;
3. **Computing power capacity**, which is paramount to store and process the available data, is, on the one hand, significantly increasing in terms of capacity and, on the other hand, decreasing from the investment perspective.

Organizational restructure

Although the AI-discipline enablers are already in place, it is commonly accepted in the industry that AI-based solutions monetization and impact are still a step behind. Moreover, it is also clear that the AI adoption technical enablers – data,

analysis and data science techniques, and computational power – are starting to get their space in the organizations. Accommodating and monetizing this new discipline poses new challenges to the organizations' structure and dynamics in order to involve all the business units in the process. This will increase the final impact, as well as the return on investment (ROI).

Following this line of thought, a significant transformation of the organizations' structural parts should be done to start monetizing the AI investment. For the sake of simplicity, we highlight the following two main barriers from our point of view:

- **Data and business separation:** in many organizations, the data science and the business execution units are individual silos that do not intersect and do not communicate as they should. As a result, the produced data science solutions, which are usually very interesting from a technical perspective, do not contribute to evolving the company products, and therefore the associated business is not impacted;
- **Insight and impact gap:** generating insights is very important and is the first deliverable to be addressed by a data science team. Well-conducted proofs-of-concept (POC) take place and share valuable insights into organizations. Nonetheless, in order to create real impact from the business perspective, it's mandatory to integrate the obtained insights in concrete operational actions, therefore challenging the existing processes and working methodologies, mostly reactive and manually achieved.

To obtain significant business impact, the AI discipline must be a tool serving the organization's business. Therefore, the first thing to do when onboarding AI in the organization is to define a clear vision and business strategy. That will guide the transformation on the organization's other structural areas, as illustrated in **Figure 1**. Following this approach will guarantee that AI is being done "for" and "with" the business.

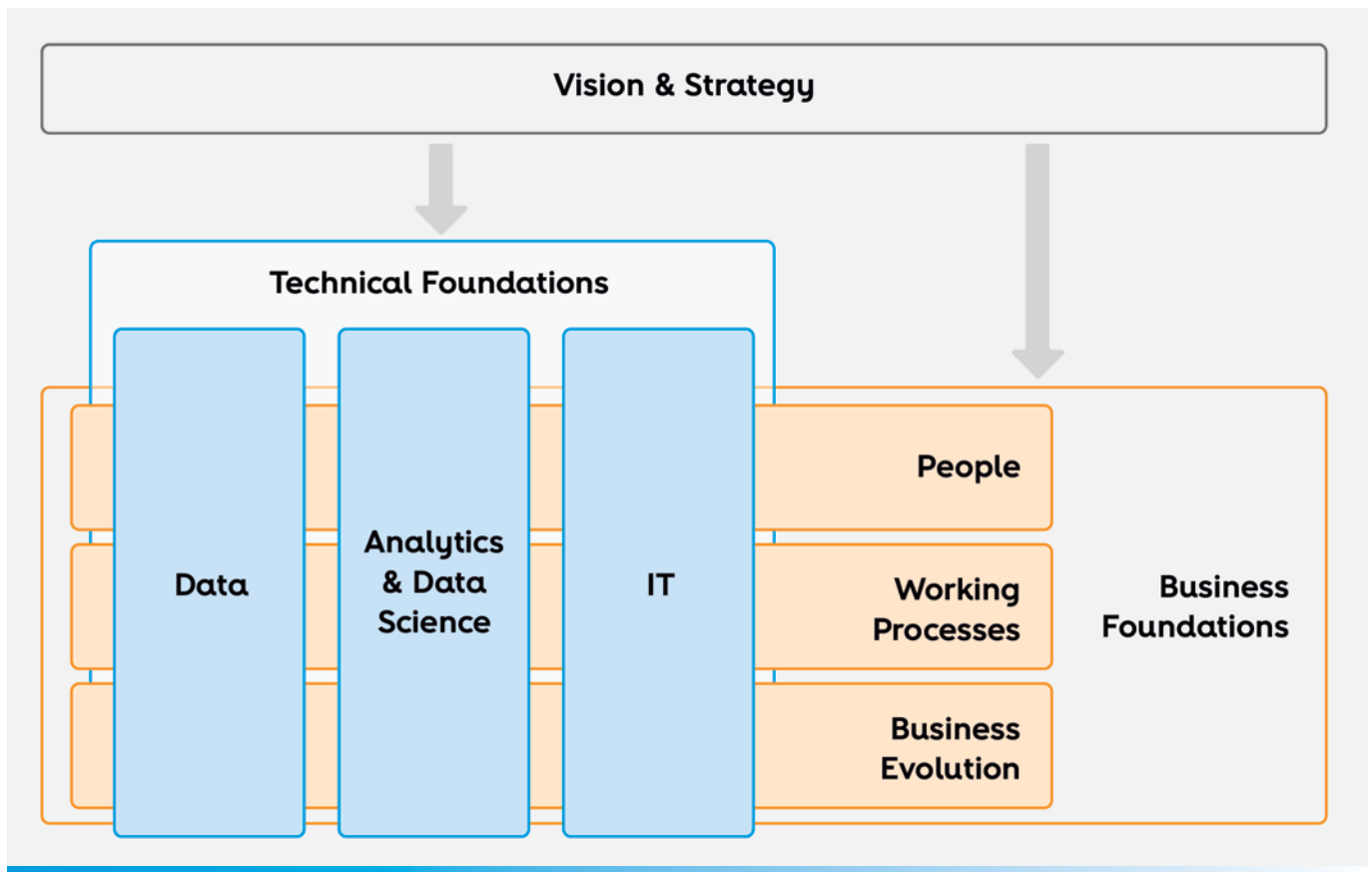


FIGURE 1 – AI-oriented organization

Thereafter, several technical and business areas should be adapted and transformed. Starting with the structural business-related evolutions, which are transversal to the technical foundations, we highlight the following:

- **People:** since AI is an instrumental tool serving the organization's business, one key topic is the relationship between the data science team and the business units. Herein, the most suitable approach is to create a data science center of excellence in the organization, which is responsible for AI-related activities, as well as for recruitment and ongoing training. Furthermore, AI knowledge cannot live only in this center of excellence. It's fundamental for achieving the desired business impact, that the people from business units involved in the AI value-chain (e.g., sales, enterprise architects, directors, domain experts, etc.) are capable of processing and translating analytics insights into business implications and concrete actions. This is a continuous learning process that will, over time, increase the data science knowledge by people from business units and facilitate the adoption of AI-based solutions. Therefore, data science teams and business units have to work together during the whole AI lifecycle process;
- **Working processes:** working methodologies must also be revised to accommodate this stringent requirement of having the data science center of excellence and the business units working closely. Old processes might need to be adapted and/or automated to guarantee the continuous involvement of the data science team and their mirrors on the business units. A data science systematic approach across the whole organization should be well-defined and clearly presented to the several stakeholders involved in the

AI value chain. More details about this are presented next, in the systematic approach process section;

- **Business evolution:** together with the business units, identify which portfolio solutions and/or procedures can be optimized through the infusion of AI capabilities. This raises one of the most critical challenges to the business units' decision-makers – define the impact of AI on their business, which is materialized in concrete products or solutions of the portfolio to be evolved, or in a set of insights-based operational procedures that can be monetized. In any of the abovementioned scenarios, the result will be the definition of the AI use-cases.

Besides the business evolutions, technical adaptations are also required. We briefly highlight the following ones:

- **Data:** the process of data collection, persistence, cleaning, etc., to support the AI use-cases. Security and privacy issues related to the data must also be handled (e.g., the European General Data Protection Regulation);

- **Analytics & data science:** includes the set of procedures required to transform and obtain insights from the data;

- **IT:** infrastructural resources (e.g. servers, GPU, etc.) to enable the AI-lifecycle operation.

Systematic approach

Besides the organization's structural adaptation described before, it is also key to have a systematic working methodology well-defined and communicated along all the actors to address this discipline. **Figure 2** illustrates a very simple perspective of a business-driven systematic approach to ensure AI results have an organizational impact.

The following three phases are depicted:

- **Data ingestion:** It is a well-known fact that AI without data is impossible. Unprecedented amounts of data are available nowadays to be collected and persisted for obtaining insights. Nevertheless, it's impractical, or at least very expensive, to collect and save all the data generated within an organization.

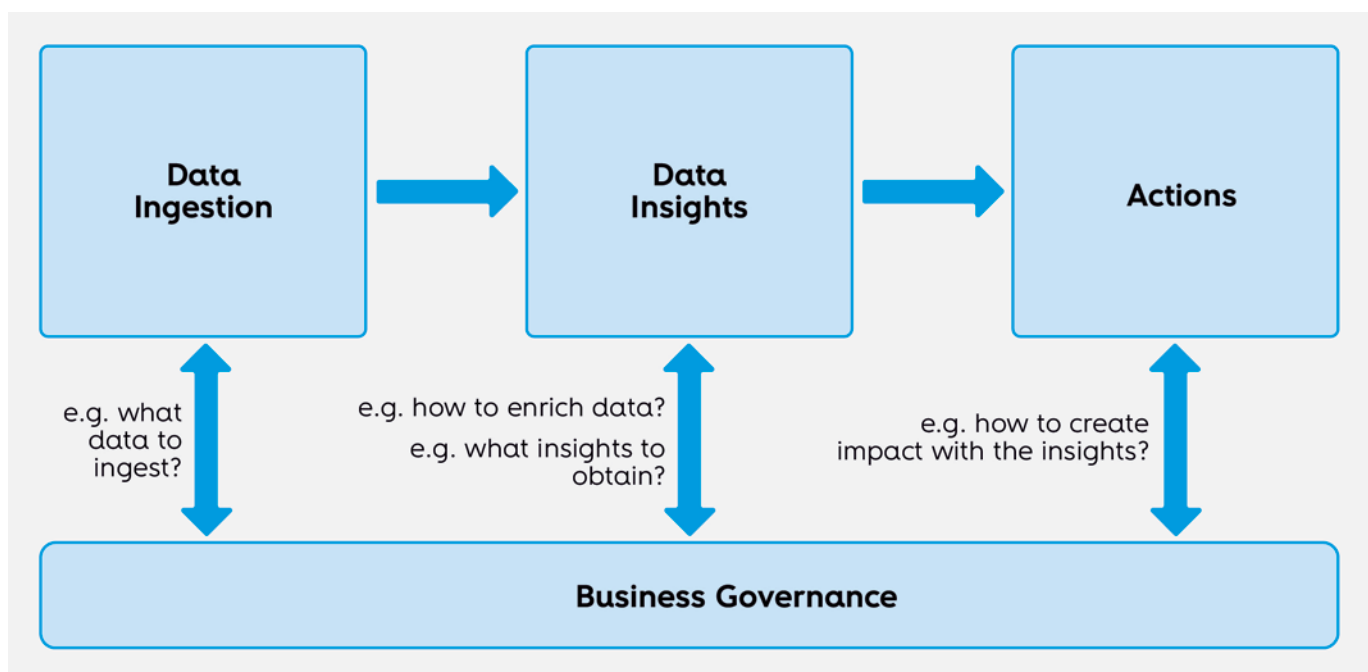


FIGURE 2 – Systematic operating model

Therefore, one of the first questions to address is what data to collect. The answer to this question is simple: we should collect and store the data that is relevant for the AI use-cases on the organization's strategic roadmap. Having the use-cases to be addressed clear will allow the definition of a strategy to collect and store the required data;

- **Data insights:** After collecting and persisting all the required data, the next step is to generate insights. This is the principal phase in which data science is concerned. One of the key tasks at this stage is, together with the business domain experts, to define the required data transformation and enrichment to represent the reality (features). Since the business domain experts are the ones that know the data and the business itself, it's crucial that they are involved in this stage of the process and help the data science team identifying the most relevant features that should be included in the dataset. After that comes the insights extraction phase. Herein, a large number of AI-technical approaches can be used by data scientists to produce the desired insights;
- **Actions:** Finally, after insights produced by the AI models, specific actions should be defined to translate the technical insights into business value. This is much related to the specifics of the AI use case addressed. For example, when producing insights about a failure of a mobile network operator, it's important to update the operator's processes when such an insight is produced – e.g., automatically re-allocate the field-force team.

bear fruit. It is the basis of all your analysis and models. Without it, there is no value to be extracted. The underlying value that your data holds is, of course, leveraged by the technology and software that you produce, and although it may often feel like a bundle of complicated and hard to understand processes, it is not the biggest obstacle to success. The challenge does not lie on software but on data, teams, and process silos, and that is why companies need a strong data culture.

A data-driven culture is a decision culture [4], where data becomes the core of your business and supports your products, operations, services, internal decisions, and business plans. It is indeed a deeper way of engaging with business, but not only that, it is a way of cultivating a sense of purpose that allows companies to establish their future with clear motives, making your data support your operational decisions and not the other way around.

Implementing such a culture is an arduous task. It involves creating a communication space that often does not exist, a clear channel that allows informed conversations to exist between your C-suite members, top decision-makers, and those who lead AI strategy and initiatives. All this effort to create the habit of making decisions anchored in factual data.

Given that a good foundation for culture has been laid down, the next challenge to tackle regards technology. The mission is to enable a close proximity between the business strategy and the operations, where data is the connecting tissue. This means quickly fixing your data access issues [5]. However, the chances that your company's data is scattered throughout several silos, or data fiefdoms as some refer to them [6], are high, thus creating the monstrous task of assembling all necessary technology and processes to transport all of this data into its new home, the pristine body of water that we call data lake. Unfortunately, this exodus only addresses the underlying data isolation problems. Now you need your teams to interact with each other, hopefully in a transparent and

Impact on operations

Data-driven culture

In the AI field, everything starts with data. Data is the fundamental centerpiece that will allow your data science endeavors to flourish and

clear way, in order to figure out how to connect data from silo A to silo B, and silo C, and up to silo Z. The final product should be a mint condition data lake with a carefully crafted, and maintained, data catalog that every team in your company can have access to. In this way, data can be used as evidence to back up business hypotheses free of unsubstantiated claims, and to measure the uncertainty that clouds your analytical judgment.

Towards autonomous operations

Typically, the current operations paradigm in communication service providers (CSP), whether they are network, service, or business operations, is mostly reactive. Globally, very few automation procedures are present in current operators. Nevertheless, this mentality is changing, and nowadays, in the digital transformation context, CSP are strongly introducing in their strategy the infusion of AI in their operations - AI in operations (AIOps). AIOps is an approach to use AI technology in order to automate CSP network, service, or business operations. With such an approach, it will be possible to provide fully automated, self-healing, and self-optimizing

capabilities to improve customer experience and service enablement. **Figure 3** depicts this evolution.

AI impact on operations

According to a report study published by TM Forum [7], CSP already have a clear idea about the key areas that will be optimized by the integration of autonomous operations. As illustrated in **Figure 4**, the top three areas are i) customer experience improvement, ii) capacity optimization, and iii) service performance analysis.

Customer experience is the most impacted area (91%). This is somehow expected since the customer journey process has several subdomains that can be improved through AI. For example, all the chatbots-related use-cases for customer care will improve customer experience by solving customer issues faster and more precisely and, in parallel, reduce operational costs at call centers. Additionally, AI will be very important to analyze and profile the customer behavior, hopefully preventing churn.

Immediately after the customer experience improvement, capacity optimization and service performance analysis are equivalently (77%)

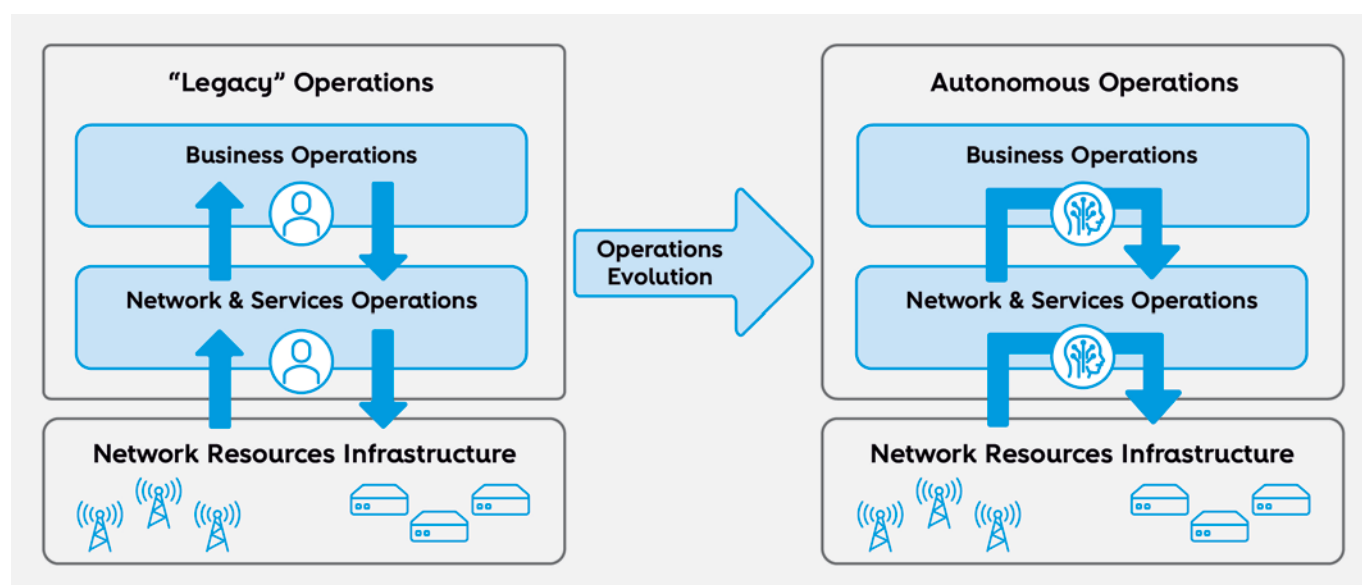


FIGURE 3 – From “legacy” to autonomous operations

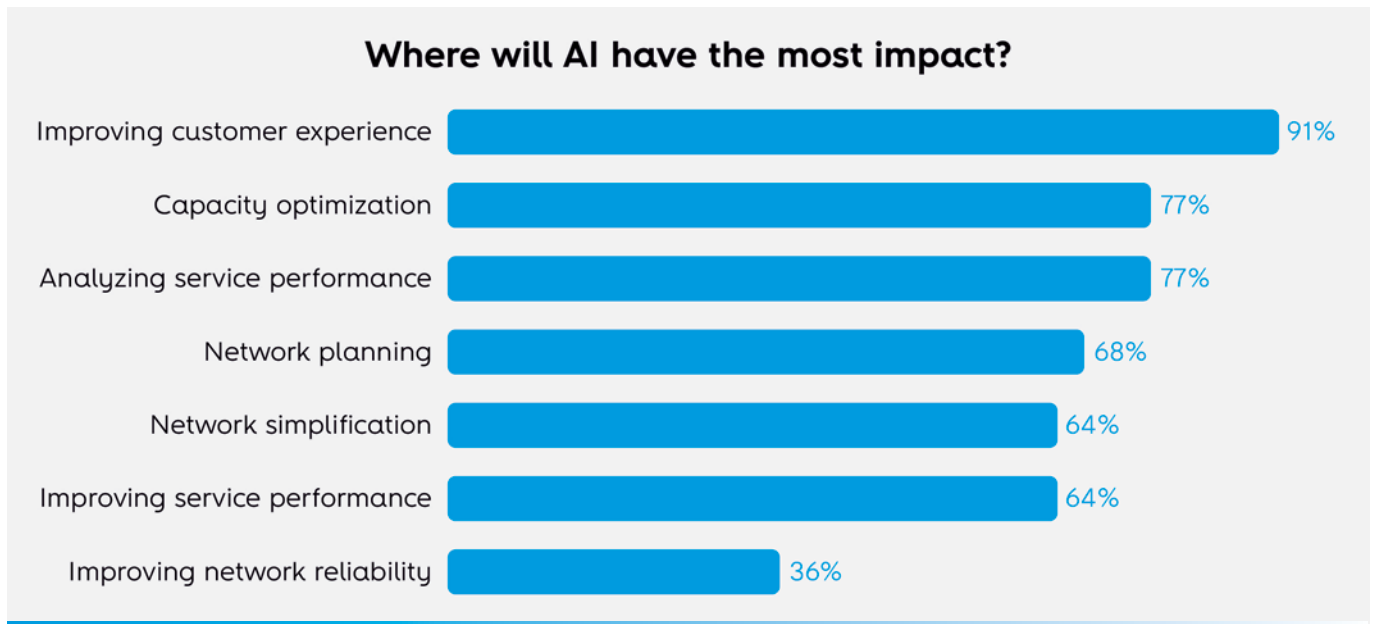


FIGURE 4 – AI impact on operations [7]

identified as important areas to be impacted by AI infusion. Although they have a similar perception of impact, the rationale for each one of them is very different. The capacity optimization case is related to the financing, since this optimization will require less infrastructure investment and, therefore, savings on the CAPEX. As for the service performance analysis case, it is considered a highly impacted area when infusing AI techniques since increasing the service quality implies improving the customer experience. One possible example of a use case in this area is analyzing specific key performance indicators (KPI) about the service performance and proactively detecting and mitigating service degradation.

On the other hand, at the lower end of the identified areas but still with a significant impact (36%), is the network reliability improvement. This is due to the fact that current network deployments, either mobile or fixed, are already very stable.

Autonomous operations evolution path

The transformation towards autonomous operations is already ongoing and will be gradually materialized through specific, self-

contained POCs before reaching production level maturity. Migrating towards autonomous operations does not mean completely dropping the traditional operations support systems (OSS) and business support systems (BSS). Although the limitations to address automation of such systems become clear, an evolutionary strategy towards autonomous operations should be embraced (instead of a revolutionary one). Therefore, it is expected that CSP will go through several maturity levels before they reach the peak of autonomous procedures. Additionally, this change will not be a uniform evolution within the operator, meaning that specific processes might be evolved prior (e.g., customer experience processes) to other processes (e.g., network reliability processes) due to their AI-enhanced business impact. The decision on which processes to impact first will mostly depend on the business impact and technical feasibility.

As a result, to set a clear evolutionary path towards autonomous operations, six maturity levels, illustrated in **Figure 5**, are defined by TM Forum [8].

Hereafter we provide a brief description of each maturity level along with simple examples.

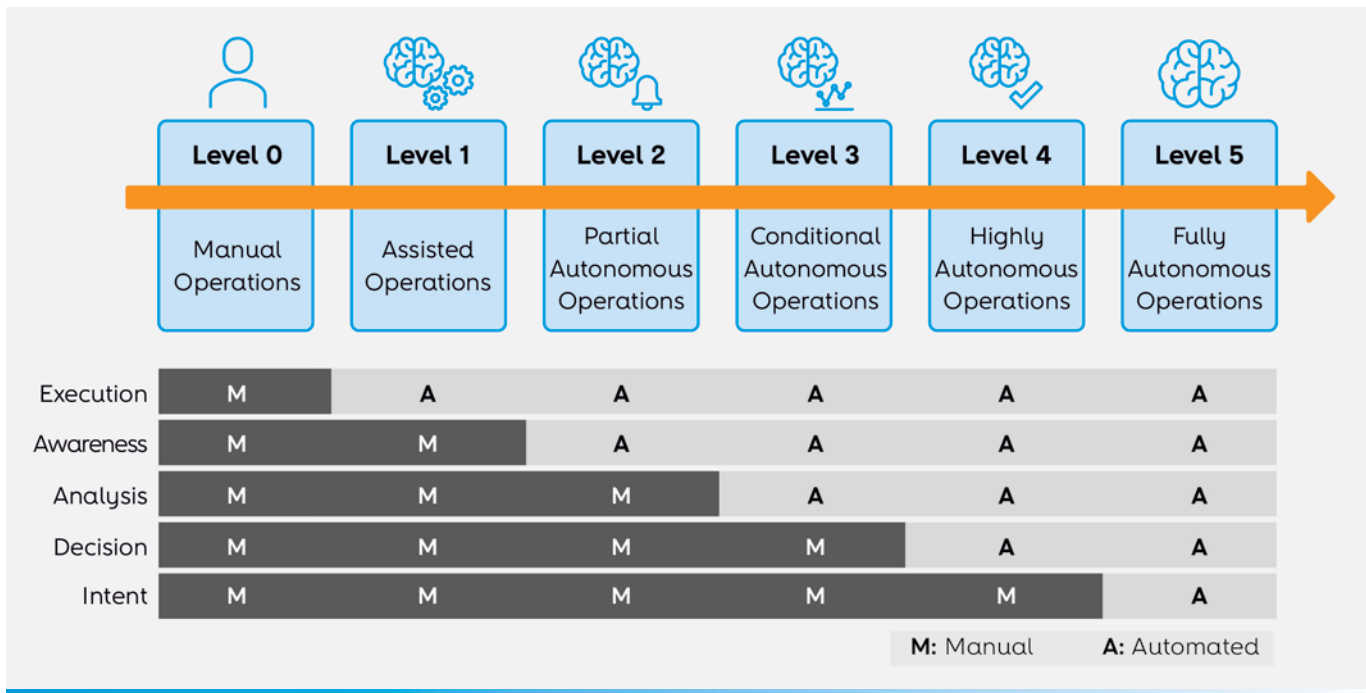


FIGURE 5 – Autonomous operations evolution path [8]

- **Level 0 - manual operations:** The management operations are all assisted by humans, which means there is no automation in the required tasks;
- **Level 1 - assisted operations:** Specific operation rules are pre-configured by a human to execute repetitive and isolated tasks in the system. For example, complex network and service alarm creation based on network events, KPIs based on network events and/or counters, parameters reconfiguration on network equipment, like home devices or mobile network devices;
- **Level 2 - partial autonomous operations:** AI models are introduced to generate insights and raise awareness of the network and service status in specific areas. Based on this information, further analysis, decisions, and mitigation actions can be manually taken by operational teams to close the management loop, for instance, mobile network predictive faults or IPTV set-top boxes (STB) predictive faults;
- **Level 3 - conditional autonomous operations:** advanced AI-based analysis techniques are

integrated to enable the identification of the root causes that are compromising the network and service performance parameters. At this phase, decision-making and actuations to close the loop are still manually implemented. For example, mobile network predictive faults and associated root-cause or IPTV STB predictive faults and associated root-cause;

- **Level 4 - highly autonomous operations:** building on previous levels capabilities (awareness and analysis), the system is augmented with AI-based decision-making procedures, incorporating a policy-driven network management architecture in the following cases: call center specific recommendations to fix customer issues, and mobile network equipment's parameters reconfiguration;
- **Level 5 - fully autonomous operations:** this level is the last step of the autonomous operations evolutionary path. The system is able to implement the entire autonomous lifecycle (infer, analyze, decide, and act) across multiple services and domains without requiring any human intervention.

The autonomous lower level 1 and level 2 described can be applied, or in more advanced CSP are already being applied, enabling the gradual integration of these procedures and therefore starting to better understand their impact in real-life operations. Higher levels should be integrated later for specific use-cases and procedures. Overall, this transformation will take several years to reach a significant maturity level, allowing CSP to improve their processes' efficiency over time.

Network automation is a long-term objective with step-by-step processes, from providing an alternative to repetitive execution actions to observing and monitoring the network environment and network device status, making decisions based on multiple factors and policies, and providing effective perception of end-user experience. The system capability also starts from some service scenarios and covers all service scenarios.

This transformation will take several years to fully develop, so we are following an evolutionary process of gradually introducing automation with AI abilities into different domains to bring immediate value.

Conclusions & takeaways

AI is here to stay and may prove essential to organizations' operational models evolution, such as in telco autonomous networks use-cases. However, although this is widely accepted across the industry, it is also clear that achieving impact and monetizing AI-based solutions is still lagging behind. In summary, as described throughout this article, there are two major barriers to achieving business impact with AI solutions. First, data science and business teams separation, leading to the creation of AI-solutions useless from the business exploitation perspective. Second, the difficulty of closing the gap between insight and

business impact. That means evolving from AI models that produce interesting insights at a POC level to models in which outcomes are integrated into operational processes that, in the end, can create real impact for the business.

There is no recipe to allow industries to overcome the above-described difficulties. Nonetheless, looking into the community evolution in this domain and from the experience that we have collected so far, with our running AI projects, a few strategic actions can be adopted from our perspective. First, it is crucial to guarantee that AI is being done together with the business, meaning that, before starting any data-related procedure, it is important to identify relevant business use-cases and only after start deciding about the required data and models. Another important action is to prioritize a small set of use-cases that are technically simple and fast to close, guaranteeing the return of investment on the data science team and quickly proving the concept. The use-case selection is critical and should set a gradual and evolutionary path towards AI, depending on the operator's internal AI maturity. For example, from Altice Labs experience, predictive maintenance, field-force optimization, and customer care support improvement were identified as the top-three use-cases towards autonomous operations at this moment. The third strategic action is related to data quality. A significant amount of time should be invested in data exploration and analysis to ensure that its quality is adequate to proceed to the modeling phase and generate valuable insights. Most of the time, bad results on the modeling phase are related to problems regarding data – "garbage-in, garbage-out". On the IT side, a dedicated infrastructure for the data science (DS) team should be prepared, starting with the minimum required assets and progressively growing/evolving towards a professional and high-performant IT environment, always aligned with the organization's IT department. Finally, and above all, have senior data-scientists to lead and cultivate the data science team and, in parallel, start promoting internal training sessions to recycle software developers. This training process

is also important to increase the AI knowledge of the organization's business decision-makers.

AI can also significantly contribute to the COVID-19 pandemic that is currently impacting the whole planet. Due to this "new normal", a massive amount of remote work is underway. This has a tremendous impact on service providers, which must be able to accommodate the huge network usage increase and simultaneously

keep the service experience at reasonable levels without increasing monthly fees. Service operations boosted with AI capabilities, also known as autonomous operations, enable a quick and prompt reaction to non-expected traffic patterns due to teleworking. Additionally, potential network and service degradations might be prevented, guaranteeing a positive and effective user experience. 🌐

References

- [1] N. Gates, "Almost 80% of AI and ML Projects Have Stalled, Survey Says," *Robotics Business Review*, 2019. [Online]. Available: <https://www.roboticsbusinessreview.com/ai/almost-80-of-ai-and-ml-projects-have-stalled-survey-says/>
- [2] G. Press, "This Week In AI Stats: Up To 50% Failure Rate In 25% Of Enterprises Deploying AI," *Forbes*, 2019. [Online]. Available: <https://www.forbes.com/sites/gilpress/2019/07/19/this-week-in-ai-stats-up-to-50-failure-rate-in-25-of-enterprises-deploying-ai/#72cd50f372ce>
- [3] Stylumia Intelligence Technology Pvt. Ltd., "Finlands visionary AI initiative," *Medium*, 2019. [Online]. Available: <https://medium.com/stylumia/finlands-visionary-initiative-ai-literacy-93cef375b056>
- [4] A. Díaz, K. Rowshankish, and T. Saleh, "Why data culture matters," *McKinsey Quarterly*, 2018
- [5] D. Waller, "10 Steps to Creating a Data-Driven Culture," *Harvard Business Review*, 2020. [Online]. Available: <https://hbr.org/2020/02/10-steps-to-creating-a-data-driven-culture>
- [6] G. Weiner, "How to build a data culture — and why it matters for nonprofits," *Whole Whale*. [Online]. Available: <https://www.wholewhale.com/tips/data-culture-nonprofits/>
- [7] T. McElligott and D. Bushaus, "Network Automation Using Machine Learning and AI," *TM Forum*, 2020. [Online]. Available: <https://inform.tmforum.org/research-reports/network-automation-using-machine-learning-and-ai/>
- [8] N. Gates, "Whitepaper: Autonomous Networks - Empowering Digital Transformation For The Telecoms Industry," *TM Forum*, 2019. [Online]. Available: <https://www.tmforum.org/resources/standard/autonomous-networks-empowering-digital-transformation-telecoms-industry/>



05

eXtended new Reality

Fausto de Carvalho, Altice Labs

cfausto@alticelabs.com

Leonel Morgado, Universidade Aberta & INESC TEC

leonel.morgado@uab.pt

Ricardo Machado, Altice Labs

ricardo-j-machado@alticelabs.com

This article addresses some aspects of the potential of XR technologies in the context of the accelerated ongoing digital transformation, with public awareness and wider acceptance being prompted by current pandemic, due to the widespread adoption of teleworking, distance learning, and virtual conferences.

The state-of-the-art of XR technologies and immersive environments is briefly addressed from the perspective of their sustained adoption in multiple scenarios, including education and training, well-being and active aging, and business.

Keywords

AR; Augmented cognition; Immersion; Metaverse; MR; NUI; VR; XR

Introduction

Extended reality is a term globally accepted to refer to the various flavors of combined real+virtual immersive environments and associated human-machine interaction through computers and wearables, a superset of the entire range along the reality-virtuality continuum [1], encompassing augmented reality (AR), virtual reality (VR), mixed reality (MR) and their subtle combinations and variations.

In recent decades, early adopters and enthusiasts of the fast-evolving XR technology developed a multiplicity of use cases around education, training, telepresence, serious gaming, and even pure entertainment and enjoyable communication among people around the globe. However, a certain level of complexity has slowed the general adoption of XR tools, even within professional contexts, with effective remote collaborative work falling far short of the maturity of technology. Videoconferencing (telepresence) remains the most notable exception, pushed forward by the general need to reduce travel.

In fact, just a couple of years back, VR environments and gadgets would make a lot of people immediately think about geeky atmospheres where time would be basically wasted in some costly gaming-like experience, ultimately perceived as a dangerous path of unhealthy isolation and escapism into a virtual life.

Suddenly, 2020 happened. And, day after day, due to pandemic concerns, we watch parents dueling for a time slot in the quieter room so that one can participate in video meetings with their co-workers while the other is also online but juggling children's dynamics at the same time: kids go around the house with their laptops, studying, attending classes online, meeting with their teachers, sneaking into social media and multi-user games. And then there are the online gym classes, the video calls with relatives, the video chats with friends, the online concerts,

the online banking, online shopping, online everything: omnipresent technology and a walk on the wild side of digitalization and virtuality.

At some point, we will regain our full freedom to go out to the physical world and live free from imposed screens (albeit with our choice of carry-on screens), so we'll go back to schools, offices, pubs, museums, venues. Most likely, we will be using more and more XR technology everywhere, now that grown-ups in general (not just we geeky grown-ups) are willing to make the most of it, after getting acquainted and experienced on varied flavors of its effectiveness for keeping in touch without being bound to specific locations. This field is reaching a high level of maturity, and we can anticipate platforms and services that will allow us to be highly productive within this accelerating digital transformation context, while improving the balance among the multiple dimensions of happiness and quality of life.

Next, we delve into immersion and its relation to XR. Then we address technical and non-technical aspects that have been pushing this technological area ahead. Before wrapping up with some considerations about current trends and envisioned opportunities, we frame the evolution over the last decade, briefly reviewing some of our XR projects in specific areas: training and e-learning with virtual worlds; serious gaming for well-being and active aging; multimodal interaction and natural user interfaces (NUI); and XR for training, maintenance and other professional activities, including Digital Twins.

Immersion works indeed

When we dive into a book or movie and emotionally relate to its characters and narrative, to the point of feeling them more real (for those moments) than life, we are immersed. When we engage with a challenge at work or with a hobby to the point that night falls or the day breaks

without us realizing it, we are immersed. When technological gadgets buzz and pop around, detecting our motion, reminding us that stuff needs to be done, lighting up the public toilets we enter, we are immersed. When we close our eyes, insert earbuds, and experience spatial sound, we are immersed. And indeed, when we push onto our heads a virtual reality headset, we are immersed.

Immersion is mental absorption. It is “a phenomenon experienced by an individual when (...) in a state of deep mental involvement in which (...) cognitive processes (with or without sensory stimulation) cause a shift in (...) attentional state such that one may experience disassociation from the awareness of the physical world” [2] emerging from three different dimensions: the environment (including technology), the narrative one experiences, and the challenges one interacts with [3].

Immersion is our current state of being in the physical world; it also occurs naturally with good storytellers and engaging situations. When coupled with visual, auditory, and other cues, it is enhanced by embodiment (**Figure 1**), whereas we experience the perception of being within a virtual body, identifying a different self-location, to the point of identifying the virtual body parts as our own, even anticipating pain when they are hit - a perception that is driven and drives the user agency and engagement [5].

Technology has now enabled immersion and embodiment to be promoted, supported, and thus more reliably counted upon for effectiveness. Rather than expect readers and viewers to find themselves immersed in a narrative, immersive technology can empower that narrative with surrounding visuals, audio, and haptics, and transform readers and viewers into users, enabling their engagement and thus their sense of challenge.

Immersive technology thus is the key to effective use of immersion in work, education, and life in general. The affordances of technology lead to the subjective sense of being surrounded, upon



FIGURE 1 – Embodiment [4]

which the narrative and the challenges unfold [6]. And immersion, as we know from even pre-technological efforts [7], leads to effectiveness in engagement and understanding, promoting better and longer-lasting impacts. Therefore, it is expected that widespread use of immersion by leveraging technology can extend this effectiveness to all areas of society.

The single foremost driver of this immersion technology, in present days, is XR: from smartphones and smart glasses that overlay virtual elements in our present world, to more powerful headsets such as Microsoft HoloLens, which can both free the user’s hands for interaction with physical and virtual elements, and provide a quick reaction time in response to head motions, as mentioned in the next section.

Immersive technology has reached maturity

The XR ecosystem has been expanding very quickly, powered by the fast pace of evolution of information and communications technologies, and the market is eagerly embracing the many

technological options, despite some still being experimental. We are reaching a solid maturity level, enabling breakthrough platforms and services in the various flavors of VR, AR, and MR that seemed unattainable not long ago.

AR is already being used massively, often without people realizing it: Instagram and Pokémon GO are two of the most popular mobile apps, incorporating AR features to enhance user experience. Furthermore, this game and others alike (e.g., Ingress, Harry Potter Wizards Unite) are based on a global virtual overlay mapping directly onto real-world points-of-interest (POIs), bounding regular players to a pervasive feeling of persistent immersion, even while offline.

VR popularity has been growing steadily, but it's not yet considered mainstream. It's common to find VR headsets being used in marketing and advertising to suggest advance and modernity, albeit futuristic, which relates to the misleading general idea that this technology is still out of reach. Nevertheless, that may change rapidly, as popular brands with huge fan bases, such as Apple, start to roll out trendy products rumored to be already in production, with the expectable buzz and viral marketing.

When you think of VR headsets, you imagine bulky devices that stick to your face, connected to a big, powerful (and expensive) computer by a long cable. While this is true for some older devices, there are attractive options becoming available: VR headsets without cables, fully standalone, not requiring an external computer or tracking cameras installed in the room. These devices aren't tethered to a single point, therefore giving more freedom to the user, plus they have better screens and higher refresh rates, are lightweight, and generate less heat, so significantly reducing the chance of causing nausea.

It's possible to experience VR with almost zero investment, attaching a smartphone to a Google Cardboard or similar low-cost gadget, frequently available for free at tech events. While it is indeed a way to try out VR and 360-degree immersive

video, it's certainly not a good experience due to the technical limitations: to achieve a more immersive and nausea-free VR experience, one needs six degrees of freedom (6DoF), meaning that the headset must track the translation (x,y,z) and rotation (pitch, yaw, and roll) of your head, and quick display response (almost instantly). This allows users to move freely around a virtual object to explore it from every angle and to come closer to inspect details, avoiding nausea. Additionally, having a way to interact with the virtual world, hands preferably, is important to enhance the sense of system immersion. That can be achieved with either two 6DoF controllers or having hands tracked by the headset itself. All of the above is already commercially available in some headsets for about 300 USD, the equivalent of a mid-range smartphone.

A healthy industry ecosystem is pushing technology forward and promoting innovation. Coming from a large mix of big companies and startups, and just naming a few, we have VR affordable headsets (Oculus Quest 2), and high-end devices (HTC Vive, HP Reverb G2), untethered cloud-powered MR headsets (Microsoft HoloLens 2) and AR/MR glasses almost indistinguishable from normal glasses (Nreal Augmented Reality glasses). Smartphone industry is, in fact, one of the key enablers of recent improvements on XR devices, with their small high-resolution screens and low-power powerful processors (e.g., Qualcomm Snapdragon XR2). And then there is a vast catalog of software and content, based on robust tools (e.g., PTC Vuforia Engine, Apple ARKit, Google ARCore) and driven by the quick technology adoption by the major 3D engines (Unity and Unreal), empowering thousands of enthusiastic developers.

eXtended Reality is (and has been) everywhere

Previous sections made evidence that XR is a multi-flavored technologically complex area, encompassing a medley of economic and human factors that have been frustrating a wider transposition of research and experimentation into market innovation [8]. Nevertheless, we have witnessed remarkable progress in terms of concepts, use cases, and technology in the last decade, from academia, startups, and industry, with big tech companies racing for strong positions in the ecosystem, aiming to conquer the huge emergent multi-billion market with their devices and/or development software platforms.

At Altice Labs, stemming from prior work at Portugal Telecom Inovação, we have relentlessly carried on exploratory projects addressing multiple dimensions and challenges on these subjects, mainly focused on advancing our knowledge and scrutinizing opportunities, but also to raise awareness and to collect precious feedback. We teamed mostly with academic partners to create a series of prototypes and

proofs-of-concept, exposed to varied audiences in multiple contexts and events, of which we present below some highlights.

Our initial exploration of virtual worlds, around platforms such as Second Life and Open Simulator, was the basis for a set of projects (with UTAD, University of Trás-os-Montes e Alto Douro) to enhance the Formare [9] corporate learning management system (LMS) with immersive features blending these technologies with classical e-learning processes [10]. Fast-forwarding ten years, we currently see virtual worlds empowering massive live conferences online with over 3000 participants and high-profile speakers from industry and government, such as iLRN2020 [11] (**Figure 2**).

The gaming industry has a long record of promoting video games, which are also a form of exercise (exergames), for platforms such as Microsoft Xbox, Nintendo Wii, and Switch consoles. In fact, natural user interfaces (NUI) leverage VR applied to e-health, well-being, and active aging, allowing engaging applications for fitness, physiotherapy, and mental rehabilitation. Move4Health project (with Instituto de Telecomunicações de Aveiro, IT Aveiro) created a VR exergame based on real-time markerless motion capture, to assess the use of low-cost



FIGURE 2 – iLRN2020 6th International Conference of the Immersive Learning Research Network

devices (Kinect) for rehabilitation therapies based on gross motor skills. Furthermore, in Online Gym (with UTAD/INESC TEC), we successfully created and tested a prototype allowing multiple persons (elders, one over 80 years old) in different locations to participate via Kinect in shared, synchronized 3D gym classes in Open Simulator [12].

Once we perceived how critical natural interaction is, for several of our use cases with higher potential to thrive in the market, we focused on immersive multimodal interaction in the InMerse project (with UTAD/Universidade Aberta/INESC TEC): a gesture-controlled digital signage prototype led to relevant results as a flexible software architecture [13]. This empowered a game/installation prototype that explored user experience (UX) and multi-user interaction: two players with different devices, roles, and locations, sharing gestures and playing within a 3D scenario set around the fictional epic episode of Adamastor during the Portuguese Age of Discovery [14].

Recent work has taken the challenge of empowering users further by leveraging their rich, intuitive understanding of cultural gestures and rituals to command immersive environments: the Shamanic interface concept [15], which has proven in controlled lab experiments to be extremely effective for users' ability to interact [16].

XR is the latest development in what traditionally was seen as VR or AR. The convergence of head-mounted displays (e.g., Oculus Rift) and camera-empowered devices, such as smart glasses (e.g., Google Glass) or smartphones, led first to MR, the convergence of VR and AR into a single device, and from there to the ambition of freeing the user for interaction and providing seamless blending of the virtual with the physical: XR. This seamlessness was made possible in two ways: by powerful, lightweight devices, such as Microsoft HoloLens, and by a combination of wall-sized projection and motion detection, such as CAVE systems [17]. We employed this in project ARaNI (with UTAD/INESC TEC) in a prototype for joint collaborative interaction over a 3D virtual human body model.

In another ARaNI prototype, we tested a Smart Mirror as a possible AR platform, with a necktie teaching application.

We also explored a novel approach to VR: created after a company repurposing challenge, the Immersive Phone Booth prototype (**Figure 3**) was available in early 2020, allowing 360-degree video immersive visualization.



FIGURE 3 – Immersive phone booth (Altice Labs 2020)

Until now, simpler AR/MR use cases for training, maintenance, field operations, and other professional activities have been higher in the ranking of successful XR deployments, despite so much amazing technology and many ingenious applications shown regularly in events and conferences. Digital Twins, accurate dynamic virtual representations of physical entities, are gaining momentum in Industry 4.0, and we have pursued this domain as well, with some AR/VR proofs of concept, such as an immersive robot arm controller. In fact, this is an area that relates directly to early work around role-playing in virtual worlds: the development of a mechanical maintenance training simulator in OpenSimulator for F-16 aircraft engines [18] developed by UTAD & INESC TEC (see **Figure 4**).



FIGURE 4 – XR in Industry 4.0 context [18]

What are the frontiers of opportunity and challenges?

So, what's next? As ever, any forecast is risky, especially in this area that has been promising so much for so long without actually getting there. Still, the ongoing workplace transformation is pushing a series of technological trends that many analysts seem to agree on [19], and we need no crystal ball to tell us that the significant increase in teleworking will have a strong impact on decision-making at home and beyond.

5G is arriving and it's poised to be a game-changer for XR, paving the way for powerful distributed processing capabilities across the edge, the network, and the cloud, available pervasively to portable connected devices with tangible UIs, with negligible latency. Furthermore, massive deployment of internet of things (IoT) is surrounding us with a plethora of sensors, gathering (big) data and allowing insights and intelligent responsiveness through machine learning and real-time context-aware analytics, enabling the enhancement of the physical world around us by a dynamic, persistent virtual space that can be perceived consistently and shared collectively - a metaverse where Augmented Cognition is, in fact, a novel dimension of immersivity.

Ultimately, we are moving towards immersive environments where technology ceases to be special and becomes pervasive. That is, technology bridges the mental context (needs,

preferences, prior knowledge) with the physical and virtual contexts, becoming seamless [20]. This will create new opportunities for services in a renewed ecosystem that digitally crosses our lives at homes, schools, businesses, and the city itself.

Currently, we can identify hindrances still interfering with the expected progress, for example, ergonomic factors, the cost of devices, and their autonomy. The diversity of stakeholders involved in these broader XR scenarios will require reliable, collaborative frameworks to address issues such as effective management, interoperability, security, and privacy. These are priorities acknowledged by researchers and practitioners alike in a recent survey of the field priorities [21].

There is also the need to tackle problems arising from the massive incorporation of AI-based features, and there are even new challenges just emerging, inherent to the intense immersion itself. Nevertheless, we have been witnessing that for each iteration, each cycle, we firmly advance in the right direction, so we may confidently state that, more and more, work and living will become further atopic: not located at any specific location or set of locations, but rather in a wide metaverse of virtuality (see **Figure 5**). 🌐



FIGURE 5 – The future of work [22]

References

- [1] P. Milgram, H. Takemura, A. Utsumi, and F. Kishino, "Augmented reality: a class of displays on the reality-virtuality continuum," Boston, MA, Dec. 1995, pp. 282–292, doi: 10.1117/12.197321
- [2] S. Agrawal, A. Simon, and S. Bech, "Defining Immersion: Literature Review and Implications for Research on Immersive Audiovisual Experiences," in 147th AES Pro Audio International Convention, New York, 2019, p. 14
- [3] N. C. Nilsson, R. Nordahl, and S. Serafin, "Immersion Revisited: A review of existing definitions of immersion and their relation to different theories of presence," *Hum. Technol.*, vol. 12, no. 2, pp. 108–134, Nov. 2016, doi: 10.17011/ht/urn.201611174652
- [4] M. Pesce, "Razer OSVR Open-Source Virtual Reality for Gaming", 2015. [https://commons.wikimedia.org/wiki/File:Razer_OSVR_Open-Source_Virtual_Reality_for_Gaming_\(16863422875\).jpg](https://commons.wikimedia.org/wiki/File:Razer_OSVR_Open-Source_Virtual_Reality_for_Gaming_(16863422875).jpg)
- [5] K. Kilteni, R. Groten, and M. Slater, "The Sense of Embodiment in Virtual Reality," *Presence Teleoperators Virtual Environ.*, vol. 21, no. 4, pp. 373–387, Nov. 2012, doi: 10.1162/PRES_a_00124
- [6] D. Beck, L. Morgado, and P. O'Shea, "Finding the Gaps about Uses of Immersive Learning Environments: A Survey of Surveys," *J. Univers. Comput. Sci.*, in press
- [7] E. L. Robinson, "Immersion Learning in Social Work Education: A Pedagogical Tool for Enriching Knowledge and Practice Skills among BSW Students," *J. Teach. Soc. Work*, vol. 38, no. 5, pp. 536–550, Oct. 2018, doi: 10.1080/08841233.2018.1516712
- [8] S. H. W. Chuah, "Wearable XR-technology: literature review, conceptual framework and future research directions," *Int. J. Technol. Mark.*, vol. 13, no. 3/4, p. 205, 2019, doi: 10.1504/IJTMKT.2019.104586
- [9] "Formare", Altice Labs, 2020. <https://www.alticelabs.com/site/formare/>
- [10] L. Morgado et al., "Requirements for the use of virtual worlds in corporate training : perspectives from the post-mortem of a corporate e-learning provider approach of Second Life and OpenSimulator," *ILRN 2016 Immersive Learn. Res. Netw. Conf. Workshop Short Pap. Poster Proc. Second Immersive Learn. Res. Netw. Conf.*, pp. 18–29, 2016
- [11] "iLRN 2020", Immersive Learning Research Network, 2020. <https://immersivelrn.org/ilrn2020/>
- [12] L. Morgado et al., "Online-Gym: Multiuser virtual gymnasium using RINIONS and multiple kinect devices," 2014, doi: 10.1109/vs-games.2014.7012164
- [13] L. Morgado et al., "Separating Gesture Detection and Application Control Concerns with a Multimodal Architecture," in 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, 2015, pp. 1548–1553, doi: 10.1109/cit/iucc/dasc/picom.2015.233

- [14] L. Morgado et al., "Exploring educational immersive videogames: an empirical study with a 3D multimodal interaction prototype," *Behav. Inf. Technol.*, pp. 907–918, 2016, doi: 10.1080/0144929x.2016.1232754
- [15] L. Morgado, "Cultural awareness and personal customization of gestural commands using a shamanic interface," *Procedia Comput. Sci.*, vol. 27, pp. 449–459, 2013
- [16] P. Carvalho, "Experiment in Human-Computer Interaction - Evaluation of a Shamanic Interface for Interaction with Cultural Gestures in Virtual Environments," Master dissertation, Faculdade de Engenharia da Universidade do Porto, Porto, Portugal, 2019
- [17] S. Manjrekar, S. Sandilya, D. Bhosale, S. Kanchi, A. Pitkar, and M. Gondhalekar, "CAVE: An Emerging Immersive Technology -- A Review," in 2014 UKSim-AMSS 16th International Conference on Computer Modelling and Simulation, Cambridge, United Kingdom, Mar. 2014, pp. 131–136, doi: 10.1109/UKSim.2014.20
- [18] A. Pinheiro et al., "Development of a mechanical maintenance training simulator in OpenSimulator for F-16 aircraft engines," *Entertain. Comput.*, vol. 5, no. 4, pp. 347–355, Dec. 2014, doi: 10.1016/j.entcom.2014.06.002
- [19] M. Rimol, "6 Trends on the Gartner Hype Cycle for the Digital Workplace, 2020," Smarter with Gartner, Aug. 24, 2020. <https://www.gartner.com/smarterwithgartner/6-trends-on-the-gartner-hype-cycle-for-the-digital-workplace-2020/>
- [20] A. Coelho et al., "Serious Pervasive Games," *Front. Comput. Sci.*, vol. 2, p. 30, Aug. 2020, doi: 10.3389/fcomp.2020.00030
- [21] H. Gaspar, L. Morgado, H. Mamede, T. Oliveira, B. Manjón, and C. Gütl, "Research priorities in immersive learning technology: the perspectives of the iLRN community," *Virtual Real.*, vol. 24, pp. 319–341, 2020, doi: 10.1007/s10055-019-00393-x
- [22] K. Matsuda, Merger. 2018. <http://km.cx/projects/merger>



06

Addressing privacy regulations for a new world

André Vassilevski Cunha, Altice Portugal

andre-v-cunha@telecom.pt

Isilda Costa, Altice Portugal

icosta@telecom.pt

Paula Cravo, Altice Labs

pcravo@alticelabs.com

Privacy regulations around the world are being subject to a stress test due to the COVID-19 pandemic. The massive use of technologies to overcome containment measures raise the debate on how to safeguard the public interest, while protecting fundamental rights, such as privacy and protection of personal data, and whether is even possible to achieve a reasonable balance.

Trust emerges as a fundamental foundation where democratic systems must build their proposals. Technology companies are vital in providing solutions and services focused on answering the more urgent problems, but addressing and analyzing regulation of privacy worldwide and cooperation between countries, in this context of globalization, is essential to assess the available responses to these emergency situations and the ensuing transformed new world.

Keywords

GDPR; Privacy; Personal data; Security

Introduction

2020 will go down in contemporary history as the year where life as we knew it changed radically due to the COVID-19 pandemic. Technology played a fundamental role, allowing people to keep communicating, working, and, even so, having fun in a confined world. Relevant solutions to stop the virus from spreading were built around the fact that mobile phones are nowadays omnipresent. And while technology is global, regulation is not. Therefore, for organizations operating globally, grasping the differences and similarities of privacy regulations across different countries and regions is of the utmost relevance to address these concerns and propose pathways to move forward. Solid and coherent privacy regulations will foster trust in the digital world, as long as technology developments comply with them.

The pandemic scenario that we are facing also brought some challenges to the working environment, especially because of the exponential growth of the teleworking phenomenon. Although teleworking is no novelty, we have never witnessed a period of time where there were so many people working remotely. To minimize the impacts of the pandemic, companies had to put in place, in a short time, telework solutions. However, companies must be careful when choosing teleworking related solutions since they can pose a threat, not only to the security of their valued information but also to the protection of the personal data of their workers.

In this article, we pursue a twofold but complementary analysis: regulatory and technological. In the first section, we provide a comparative guide with examples of privacy regulations across the globe. In the next section, we focus on how telework helped economies during this crisis and how the privacy regulations can help protect the workers while fostering this form of work. Finally, we briefly describe and analyze some technological solutions used in the pandemic context to protect the security and privacy of individuals.

Privacy regulations around the world

Privacy concerns and technological solutions have to be framed within the regulatory context worldwide. Although the European General Data Protection Regulation (GDPR) [1] may be considered the cornerstone of privacy laws, a benchmark in this subject, it is also important to understand how some other countries address these challenges raised by the use of new technologies on the protection of personal data.

To get a broad perspective of the privacy laws' landscape throughout the world, in this section we will focus on the GDPR and three other privacy laws: the California Consumer Privacy Act (CCPA), from the United States (US), the Lei Geral de Proteção de Dados (LGPD), from Brazil, and the Cybersecurity Law of the People's Republic of China (CSL). Regarding the comparisons with the CSL, we will also mention the Personal Information Security Specification (PISS), a set of non-binding recommendations and standards on cybersecurity and data protection issued by the Chinese authorities.

Scope of the regulations

The first aspect that needs to be analyzed in these laws is their scope. All the above-mentioned laws apply to personal data or information on natural persons. However, the CCPA, in contrast with the other laws, only intends to protect the personal data of natural persons when they act as consumers. It is also important to highlight that none of these legislations applies to anonymized data, where the natural person can no longer be identified.

Even though these laws apply to entities that process personal data of residents in their respective jurisdictions, both the GDPR and LGPD apply to organizations that are not established in their territories if the processing of personal data is related to the offering of goods or services to

individuals located in their territories [2]. The CCPA may also apply to organizations established outside of California if they meet the criteria to be considered as *“doing business in California.”*

Definitions

There are three core concepts associated with the processing of personal data: personal data *per se*, and controller and processor concepts.

With some minor differences between them, the above legislations adopt a very similar definition of personal data. In broad terms, they define personal data as *“information related to an identified or identifiable natural person”* (the CSL mentions *“information used to identify a natural person”*). While the various definitions of personal data, set out by these legislations, present some resemblances, the way they approach the notion of special categories of data (*“sensitive data”* according to the LGPD, and *“personal sensitive information”* according to the PISS) is quite different. Both the CSL and the CCPA do not separately define special categories of data. Still, the LGPD and the GDPR have an almost identical definition of this concept, which can be summarized as personal data related to an individual’s religion, philosophical and political beliefs, health, or sexual orientation.

The definitions of controller and processor are essential to fully understand the different roles linked to the processing of personal data. Although the terms may differ (the CCPA mentions *“businesses”* and *“service providers”* and the CSL only describes *“network operator”*), we can find some similarities in the definitions provided by these legislations. They all describe controllers as the natural or legal persons that determine the means and purposes of the processing and define processors as the natural or legal persons who process the personal data on behalf of the controller. Despite not being explicitly defined throughout Chinese legislation, the concept of processor is mentioned in the PISS as *“the connection between a personal information controller and an entrusted party.”*

Data subject rights - right to erasure and right of access

Data subjects are the natural persons to whom the GDPR grants rights protecting information that identifies or makes them identifiable (*“personal data”*). We will focus on:

- **the right to erasure**, which embodies the end of the processing activities linked to the personal data of an individual;
- **the right of access**, which is the first step that needs to be taken by the data subjects to fully understand which of their personal data is being processed by an organization.

All the pieces of legislation that we have mentioned before allow the data subjects to request the deletion of their own personal information. However, the requirements for the deletion of personal information are different in each of these laws. For instance, although the LGPD sets out rules that ensure a similar right to erasure as the GDPR, the CSL does not contain any obligations connected with the right to erasure, such as timeframes or exemptions [3]. Additionally, the CSL’s main ground for the erasure of personal data is if an individual discovers that a network operator has violated the legal provisions in collecting or using an individuals’ personal information. Under the CCPA, although some of the exceptions to the right to erasure are similar to the ones provided by the GDPR, a business is not required to comply with a request for erasure if the personal data is being used to detect security incidents.

Even though the right of access is portrayed as the foundation of all the other data subject rights, differently from the right to erasure, this right is not provided by all the laws addressed in this article. Contrasting with the other three laws, the CSL does not include any reference to the right of access nor any procedures for responding to requests for access. Curiously, the PISS states that the data subjects have the right of access to some of their personal information, leading to a

situation where data subjects don't have the right to access their personal data but, simultaneously, it is recommended for the entities that process personal data to give access to the data subjects' personal data [3].

As referred, all the other three laws that we analyzed establish the right of access. Nevertheless, they all show differences concerning the procedures that organizations should follow in order to fulfill an individual's access request. For example, the LGPD, unlike the GDPR and the CCPA, does not contain a list of reasons to refuse an access request.

Legal basis for processing

Processing personal data cannot be taken lightly. The GDPR only allows the processing of personal data when there is a legal ground for it, listed in article 6. The Brazilian law took a similar approach and established a set of legal foundations under which controllers can decide to process personal data that resemble those set out in the GDPR. In contrast, the CCPA does not list the legal grounds for processing it. Nevertheless, consumers have the right to request businesses not to sell their personal data, and businesses must also obtain consent from consumers if they offer financial incentives built around the personal data provided by the consumer [4].

On the other hand, the Chinese legislator opted to focus on consent as the main justification to process personal data. According to the CSL, personal information can only be processed if consent was previously obtained from the data subject. Even though PISS provides other justifications for the processing of personal information, its core legal basis is still consent.

In our perspective, the existence of a list of grounds under which personal data can be lawfully processed is essential to guarantee that the data subjects' personal information is not misused. Also, the proper establishment of the legal basis for the processing of personal information is vital to protect the data subject,

especially in situations where he is in a weaker position. For example, as we will discuss in the next section, in employer-employee relations, the cases where the employer can process the workers' personal information must be explicitly defined to avoid the violation of workers' rights.

Privacy and teleworking through pandemic times and beyond

Technology plays an important role in the organization and execution of work. Privacy concerns, arising from the increasing role of technology in this area, have to be framed and governed by robust and coherent regulations. Are privacy regulations described in the previous section enough to cope with the challenges that telework faces presently? And what about the future?

Teleworking, where the use of technology is the differentiating factor, has been around for decades. According to Eurostat, since 2008, the percentage of employed persons aged 15 to 64 in the European Union (EU), who usually worked from home, remained pretty much the same at around 5.0% [5]. But one could safely state that 2020 has seen an unprecedented and unexpected rise in the number of teleworkers due to the worldwide response to the COVID-19 pandemic. Many businesses adopted teleworking as a means to overcome restrictions and keep economic activities running.

Recently, EU agency Eurofound reported that over a third (33.7%) of those currently working in the EU worked from home as a result of the pandemic, as shown in **Table 1** [6].

Regardless of the eventual relaxing of pandemic-related measures, it is assumed that in a post-COVID-19 world, teleworking will stay, much often than before, as a common practice. However, the

Location of work during COVID pandemic	% of employees	Weekly hours worked	Note
Home only	33.7	38.9	
Various: home, employer's premises and elsewhere	14.2	41.2	
Employer's premises or other locations outside home only	52.1	40.4	(of which 19.3 hours at home)
All employees	100.0	40.0	
Note: Weekly hours are capped at 100.			

TABLE 1 – Proportion of employees, by location of paid work during COVID-19 pandemic, EU27 [6]

“home office” as a hybrid location that combines private and professional spheres raises security and data privacy concerns due to the blurring of boundaries between the two worlds [7].

Regulatory framework in Europe

In general, in European countries, and as a consequence of the Framework Agreement on Telework [8] signed in July 2002 by European social partners, a teleworker has the same rights and duties as other workers, guaranteed by applicable legislation and collective agreements. Working time, health and safety, training, career opportunities, collective rights, and privacy should be the same as the other workers. Furthermore, the Framework Agreement also addresses the need for employers to respect the privacy of the teleworker, allowing for monitoring systems only if proportionate to the objective.

As a rule, and unless otherwise agreed, the availability, installation, and maintenance of working instruments necessary for telework are the responsibility of the employer. Conversely, in the employment relationship, the employer has the power to direct and control the activity of the worker, legal subordination being a key identifier of these types of relationships.

Many relevant questions stand. Is the employer allowed to implement monitoring tools enabling

remote surveillance of the workers? Is a pandemic crisis reason enough to legitimate the prevalence of the employers' economic interests? Must the right to privacy of the teleworker and its family yield before the interests of the employer to ensure productivity and protect the company's assets from theft, sabotage, and other cyber threats (including the breach of personal data of company's customers)?

Long gone are the days when control of telephone calls or emails and video surveillance were the major threats to the workers' privacy. Applications to assist the employer in controlling the worker are booming right now, and it takes only a minute online to identify those that are trending such as Hubstaff, Time Doctor, StaffCop, EmployeeTrail, Teramind, to name just a few. These applications can gather large amounts of control data: time-tracking hours, keystrokes, mouse movements, computer screenshots, app, URL tracking, sound recordings, etc., besides allowing analytics that can lead to automated making decisions. Those applications can indeed be used in the traditional workplace, but in the “home office”, they amplify the threats to privacy not only of the worker but also their families and persons that they interact with. The International Labor Organization (ILO), in its "Practical Guide on Teleworking during the COVID-19 Pandemic and beyond" [9], discourages the use of such applications due to its intrusive nature, recommending a management approach instead.

The key lies in a difficult balance of interests and, as the EU advisory body Article 29 Working Party puts it, the risks to the privacy of the workers should be addressed *“in a proportionate, non-excessive manner, in whatever way the option is offered and by whatever technology is proposed, particularly if the boundaries between business and private use are fluid”* [10].

The European Charter of Fundamental Rights of the EU states that any limitation on the exercise of the rights and freedoms, such as the right to privacy and the protection of personal data, *“may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others”* [11].

In furtherance of the principles enshrined in the above-mentioned Charter, the GDPR ensures not only a high level of protection of the rights and freedoms of natural persons with regard to the processing of personal data, but also a consistent and homogenous application across the union and even worldwide, insofar as personal data of European citizens are concerned, as already explained in the previous section.

There is no question that employers must comply with the GDPR and abide by all its principles, regardless of technologies used in the work relation (either at the workplace or not), as they are regarded as controllers.

Usually, the performance of the contract is the ground for the lawfulness of processing, but others may also be applicable, such as compliance with legal obligations as per article 6(1)(c) and legitimate interests of the employer as per article 6(1)(f). Consent can be a legal basis, among others, but for most worker’s personal data, *“the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee”* [12].

Pursuant to article 5(1)(c) of the GDPR, employers must ensure that the workers’ personal data should be subject to data minimization (i.e.,

only personal data that is *“adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”* is allowed). Needless to say, the use of remote monitoring tools falls within the scope of this principle.

As respects to data processing in the context of employment, article 88 of the GDPR allows for the member states to provide for specific rules with an obligation to notify the provisions adopted. Not all the countries have made notifications regarding article 88, and in most cases, there are no dramatic changes in labor law [13]. Spain stands out in the European landscape, for in its Ley Orgánica 3/2018 [14] dedicates five provisions to the employment area enforcing the right to privacy and the use of new digital devices in the labor field (article 87); the right to disconnect (article 88) allowing employees in companies of more than 50 people to ignore emails after work hours also, applicable for telework; the right to privacy in the use of audio-visual or geo-location systems in the working area (article 90); and the possibility for collective agreements to reinforce these rights (article 91).

The fact is that the leeway that the member states have in this area may well compromise the harmonization goal of the GDPR conducing to different levels of protection of workers’ privacy rights across the Union.

The future of work

Technology has been shaping the way work is done and also the contractual relationship between employer and worker. This impact tends to grow in a hyper-connected world, namely with increasingly sophisticated artificial intelligence (AI) solutions that allow the collection of large quantities of data, enabling its analysis and subsequent use in the decision-making process of the employer. Article 22 of the GDPR, clearly a forward-looking provision, states that an individual has the right not to be subject to a decision based solely on automated processing

“which produces legal effects concerning him or her or similarly significantly affects him or her.”

This could clearly be the case when using remote surveillance and productivity tools with an impact on the workers' promotion or salary. As regards AI, the European Commission recognizes that along with indisputable benefits also come risks and threats to the rights and safety of individuals *“when facing the information asymmetries of algorithmic decision-making”* [15]. Skepticism over the use of AI, not only in work but in all walks of life, lies mainly in the threats to privacy, personal data, and other fundamental human rights. The debate also revolves around the adequacy and sufficiency of legislation to safeguard those rights against AI tools. Although in Europe, the GDPR is perceived as a robust piece of legislation in what concerns personal data, will it be able to tackle all the challenges AI poses? In the white paper on AI, the European Commission concedes that some specific AI features as opacity *“can make the application and enforcement of this legislation more difficult”* [15]. As a consequence, an assessment of the regulatory framework is ongoing and will result in changes to existing pieces of legislation or the adoption of new ones.

Technology vs. privacy – a pandemic stress test

As mentioned previously, the new reality forced us to revisit our concerns on security and privacy, individual liberties and rights, and public security and safety. Besides the urgent need for teleworking also came the need to control the spread of the pandemic infection, which demanded new technological solutions. This section briefly discusses two technologies that are perceived as vital in addressing the pandemic crisis and some of their privacy issues, exposed to public scrutiny due to the circumstances.

Privacy and subjects' tracing

One of the needs that arise from the pandemic crisis is the relevance of knowing the movements and whereabouts of the population, as recognized by the World Health Organization (WHO) [16]. The information and communication and the technology communities came forward, proposing solutions to automatize the tasks of inquiring where an infected citizen was and with whom was he/she in contact in the previous days. Most of the solutions proposed are based on the fact that mobile phones are omnipresent in a modern world. But these proposals were never free of great controversy and concern for the common citizen and international organizations, like the European Parliament [17].

Smartphone owners carry a location device with them all the time, connected to the internet most of the time. It's possible to infer the localization of a person with an acceptable level of accuracy through several methods, some of which are summarized in **Figure 1**.

Smartphones' extensive capabilities allowed the development of several approaches for personal localization and contact tracing, like the bluetooth-based solution proposed jointly by Apple and Google [18]. However, all proposals present some weaknesses with the potential to violate the subject's privacy rights, most especially those based on the users' geographical location. Indeed, a non-exhaustive analysis conducted by Guardsquare [19] on 17 different mobile contact tracing apps from 17 countries found that a few of them do implement some type of security and privacy protections, as shown in **Figure 2**, but the vast majority are not sufficiently protected against reverse engineering and potential exploitation, being easy for hackers to decompile, attack, and create clones.

COVID-19 tracing apps can be classified as centralized - when they concentrate the information on a server managed by some authority; or decentralized - if they keep information in the user's device. Besides, different approaches use different types of personal data,



Mobile cell triangulation

- Explores the topology of a mobile cellular network and uses radio-triangulation techniques to infer an approximate location of a device;
- No user intervention is needed, only information on the network operator side.



Search engine positioning

- Essential for search engine optimization, to achieve higher (or more numerous) results in search engines for specific keywords;
- Can be disabled via search engine options or add-ons.



IP geolocation

- The mapping of an IP address to the geographic location of the internet from the connected device, such as the country, state, city, zip code, latitude/longitude, ISP, area code, and other information;
- Accuracy varies by country;
- Can be disabled if no data connectivity is active on the device. Otherwise, it can only be masked.



Indoor positioning system (IPS) Wi-Fi positioning system (WPS)

- Uses a network of devices to infer the location of the mobile phone. WPS uses characteristics from nearby Wi-Fi hotspots and other wireless access points. IPS uses different technologies, like RFID or bluetooth beacons;
- Can be switched off by the user on the device.



Mobile device GPS

- Uses satellite networks and provides accurate geo-spatial positioning of the device;
- Only available outdoors;
- The user can switch it on and off on the device.



Social media activity

- Localisation is inferred through the user's activity on social media platforms;
- Provides only city-level accuracy.

FIGURE 1 – Examples of subject localization in smartphones

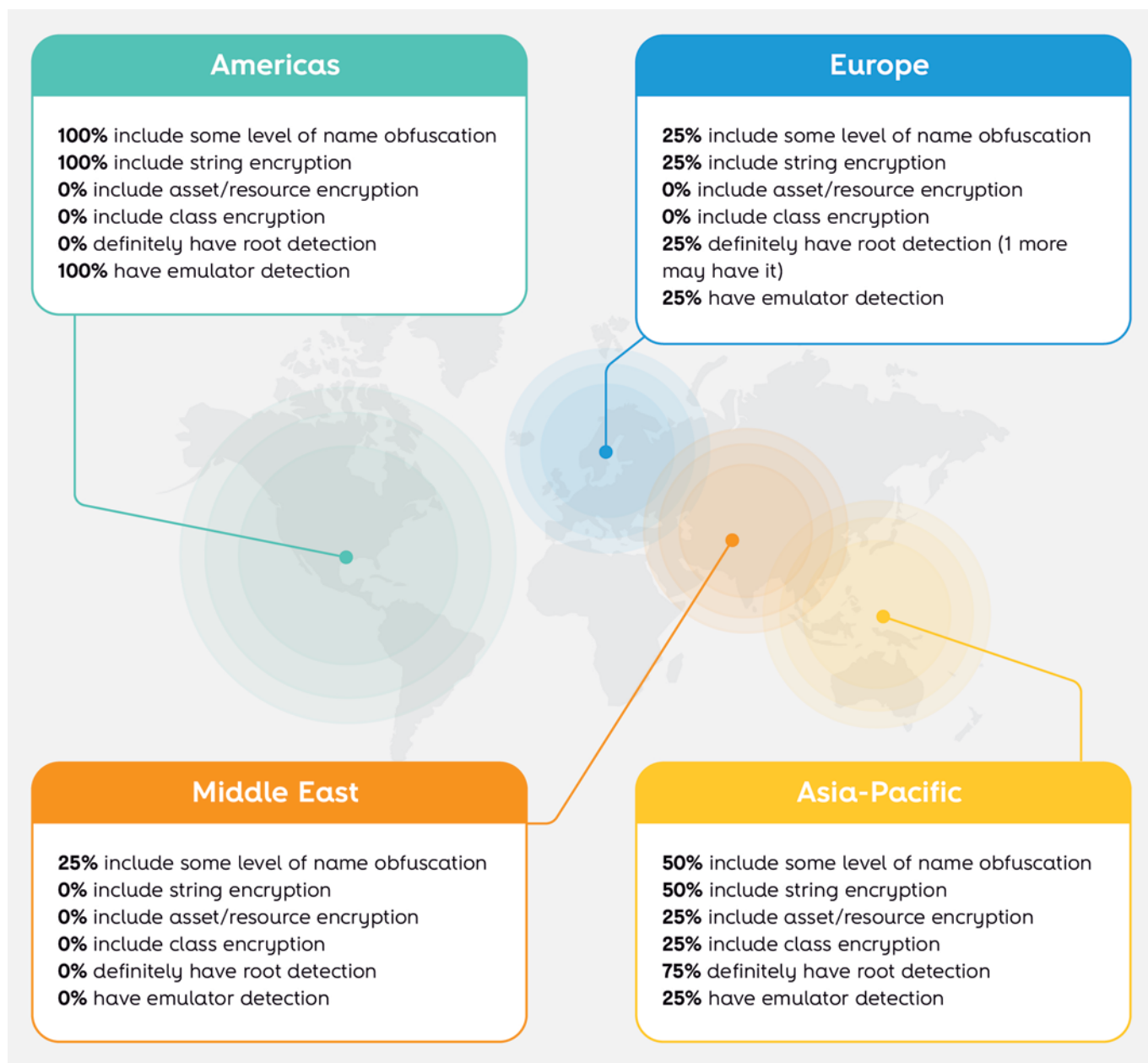


FIGURE 2 – Contact tracing apps - security and privacy hardening techniques [19]

and its processing and storage may be done either locally, on the device, or be centralized on the server. Nevertheless, eventually, some amount of data will be stored on a server. Another aspect that varies in these solutions is the notification mechanisms implemented, which can be anonymized by notifying only those at risk without disclosing information on the infected user and his/her other possible contacts or provide more information to authorities.

In both approaches, there is still the need for an evaluation regarding its respect to the legal basis for processing, as stated on GDPR article 6, and the implementation guidelines for contact tracing apps issued by authorities, like the WHO [20], the US Centers for Disease Control and Prevention (CDC) [21], the European Centre for Disease Prevention and Control (ECDC) [22] or the European Data Protection Board (EDPB) [23]. As stated by Guardsquare's researchers, "when

security flaws are publicized, the whole app is suddenly distrusted and its utility wanes as users drop off.” And they added: “trust is key to success with contact tracing apps, but app makers unfortunately do not seem to be taking the risks seriously enough yet.” [19]

At the time of this article’s writing, 120 contact tracing apps were available in 71 countries [24], but these numbers will undoubtedly change over time. Technology can unquestionably help address world health concerns, like the COVID-19 disease spreading, but even during a pandemic, the “privacy-by-design” ethos should not be sacrificed.

Using AI technology to control the pandemic

State-of-the-art technologies, like AI, can provide a deeper understanding of the infection and accelerate the discovery of a treatment for the disease. This is true for any disease, but the process came to the limelight due to the atypical 2020 circumstances. In fact, the Council of Europe recognized several aspects where researchers, scientists, authorities, and the general public may benefit from AI-supported tools [25]:

- to assist the search for a cure by using biotechnology to predict the virus structure;
- as a driving force for knowledge sharing by screening the vast amount of research papers published on the pandemic;
- as a tool for observing and predicting the evolution of the pandemic, providing a useful source of information for policymakers, the media, and the public to observe emerging trends related to COVID-19 in their countries and around the world;
- to aid healthcare personnel with AI-based coronavirus diagnostic software;
- as a means for population control, for example, by issuing containment orders for populations at risk, verification of compliance

with the measures by mobile phone and geo-location, random checks, etc.;

- to combat misinformation and disinformation about the pandemic.

The means to attain such efficiency are often in direct confrontation with individual privacy and liberties, and solutions are forced to comply with different laws and regulations, conducting to diverse approaches to the problem. However, even in exceptional circumstances, these laws and regulations relating to data protection still apply, and subjects’ rights must be assured. Relating to AI systems, the goal should always be to maximize the benefits while preventing and minimizing their risks. With this aim, the High-Level Expert Group on Artificial Intelligence (AI HLEG), an independent expert group set up by the European Commission, published in 2019 the Ethics Guidelines for Trustworthy Artificial Intelligence [26]. This document contains an assessment list to help evaluate whether any specific AI system meets the requirements for trustworthiness. The assessment list “*raises awareness of the potential impact of AI on society, the environment, consumers, workers and citizens (...) helps foster responsible and sustainable AI innovation in Europe.*” [27]. Trustworthiness is key for European individuals to take full advantage of the benefits of an AI system, as the AI HLEG recognizes.

Conclusion

The increasing impact caused by new technologies on the privacy of individuals is leading to a global yet diverse and independent regulatory response. Some jurisdictions, such as China or California, opted for a sectorial line of action to tackle these challenges. In contrast, others, such as the EU and Brazil, chose a generic legislative approach. As would be expected, we still did not reach (and probably never will) an appropriate level of harmonization across major privacy laws. The biggest issue for companies and specifically for those in technological fields is

how to deal with different privacy laws when their products and services are global. There is not a perfect answer to this question but complying with the GDPR is a starting point.

During the first peak of the pandemic, when suddenly the world had to confine, many turned to technology as a panacea. They faced this unique moment as an opportunity to adopt new ways of living and working through technology. Yet technology is a tool, not a solution, and one must be cautious. By itself, a tool doesn't have to comply with the human definition of ethics or morals - it is agnostic to those concepts. But the use of a tool should comply with the law, regulations, and, if nothing else, the ethics of the user.

As we discussed in this article, laws and regulations are not global, and each nation adopted laws offering different levels of protection for subjects' privacy rights. Also, the

borderline between the right of the employer to achieve effective control of the organization in such difficult times, and the employee rights to his privacy, has many fuzzy areas. Organizations stepped forward issuing ethical advice and guidelines for the implementation of technical solutions to address day-to-day issues that, albeit not new, gained increased importance during the pandemic, like the need for teleworking, for contact tracing apps, or for analyzing the spread of contagious diseases, such as the COVID-19.

Undeniably, privacy laws, regulations and technical guidelines presented in this article are meant to foster individuals' trust, an asset that, above all, shouldn't be compromised: trust in the democratic systems, trust in the security in the digital world, trust in the integrity of fundamental rights. This world crisis showed the global relevance of these frequently ignored issues that should be tackled with global solutions. 

References

- [1] The European Parliament and the Council of the European Union, "General Data Protection Regulation," *The European Parliament and the Council of the European Union*, 2016. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1542977568879&from=EN>
- [2] OneTrust Data Guidance and Baptista Luz Advogados, "Comparing privacy laws: GDPR v. LGPD," no. December, 2019
- [3] OneTrust DataGuidance and Chen & Co. Law Firm, "Comparing privacy laws: GDPR v. CSL and Specification," 2020
- [4] DataGuidance and Future of Privacy Forum, "Comparing privacy laws: GDPR v. CCPA," pp. 1-42, 2018
- [5] Eurostat, "Working from home in the EU," 2018. [Online]. Available: <https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20180620-1>
- [6] D. Ahrendt et al., "COVID-19 unleashed the potential for telework. How are workers coping?," Eurofound, 2020. [Online]. Available: <https://www.eurofound.europa.eu/publications/report/2020/living-working-and-covid-19>

- [7] T. Katsabian, "The Telework Virus: How the COVID-19 Pandemic Has Affected Telework and Exposed Its Implications for Privacy and Equality," *SSRN Electron. J.*, pp. 1–57, 2020
- [8] ETUC, UNICE, UEAPME, and CEEP, "Framework Agreement on Telework," p. , 2002
- [9] ILO, *Teleworking during the COVID-19 pandemic and beyond*. 2020
- [10] Article 29 Working Party, "Opinion 2/2017 on data processing at work - wp249," *European Commission*, 2017. [Online]. Available: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169
- [11] European Parliament, European Council, and European Commission, "Charter of Fundamental Rights of the European Union," *Official Journal of the European Union*, 2012. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN#d1e774-393-1>
- [12] Article 29 Data Protection Working Party, "Wp29 Guidelines on Consent," *Ssrn*, pp. 1–31, 2017
- [13] Bird & Bird, "GDPR Tracker," *Bird & Bird*, 2020. [Online]. Available: <https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/employment>
- [14] España, "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.," *Boletín Of. del Estado*, pp. 119778–119857, 2018
- [15] E. Commission, "White Paper on Artificial Intelligence - A European approach to excellence and trust," *COM(2020) 65 Final*, 2020
- [16] WHO, "Digital tools for COVID-19 contact tracing," *Digit. tools COVID-19 contact tracing*, no. June, p. 4, 2020
- [17] C. Dumbrava, "Tracking mobile devices to fight coronavirus," no. April, p. 12, 2020
- [18] Google, "Privacy-safe contact tracing using Bluetooth Low Energy," *Blog.Google.Com*, 2020
- [19] G. Goodes, "Most Government-Sponsored COVID-19 Contact Tracing Apps Are Insecure and Risk Exposing Users' Privacy and Data," *Guardsquare*, 2020. [Online]. Available: <https://www.guardsquare.com/en/blog/report-proliferation-covid-19-contact-tracing-apps-exposes-significant-security-risks>
- [20] World Health Organization, "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing," no. May, p. 6, 2020
- [21] CDC, "Guidelines for the Implementation and Use of Digital Tools to Augment Traditional Contact Tracing COVID-19 Contact Tracing for Health Departments," *COVID-19 Contact Tracing Heal. Dep.*, pp. 1–7, 2020
- [22] ECDC, "Mobile applications in support of contact tracing for COVID-19 - A guidance for EU EEA Member States," *Eur. Cent. Dis. Prev. Control - Tech. Guid.*, no. June, pp. 1–11, 2020
- [23] European Data Protection Board, "Guidelines 04 / 2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak," no. April, p. 19, 2020

- [24] S. Woodhams, "COVID-19 Digital Rights Tracker," *Top10VPN.com*, 2020. [Online]. Available: <https://www.top10vpn.com/research/investigations/covid-19-digital-rights-tracker/>
- [25] Council of Europe, "AI and control of COVID-19 coronavirus," *Council of Europe*, 2020. [Online]. Available: <https://www.coe.int/en/web/artificial-intelligence/ai-and-control-of-covid-19-coronavirus>
- [26] High-Level Independent Group on Artificial Intelligence (AI HLEG), "Ethics Guidelines for Trustworthy AI," *Eur. Comm.*, pp. 1–39, 2019
- [27] High-Level Independent Group on Artificial Intelligence (AI HLEG) and B. Y. The, "Assessment List for Trustworthy AI," *Eur. Comm.*, pp. 0–33, 2020



07

Data: the good, the bad and the ethical

Prof. John D. Kelleher, Technological University Dublin

john.d.kelleher@TUDublin.ie

Filipe Cabral Pinto, Altice Labs

filipe-c-pinto@alticelabs.com

Luís Cortesão, Altice Labs

luis-m-cortesao@alticelabs.com

It is often the case with new technologies that it is very hard to predict their long-term impacts, and as a result, although it may be beneficial in the short term, it can still cause problems in the longer term. See, for instance, what happened with oil by-products in different areas: the use of plastic as a disposable material did not consider the hundreds of years necessary for its decomposition and its related long-term environmental damage. Data is said to be the new oil because of its intrinsic value. But as in real crude, we should ensure that its use does not create harm in the future. From recent history, we know that any entity can use data in harmful ways, but data also has enormous positive potential when applied to communities' service data.

Keywords

Data; Data ethics; Fake news; AI

Introduction

Most pieces of data are measurements of some type (for example, the height of an individual in centimeters; the number of items a customer purchased; the temperature at a location). The related meta-data concept describes data about data, such as the timestamp when a measurement was taken, and described in this way that data and meta-data may seem objective, primarily useful for generating reports, and innocuous. However, data is subjective, can be used to harm, and is a powerful basis for decision-making to drive action and improve future outcomes. At a high level, the data-driven decision pipeline's critical stages can be understood as: data capture, analysis, insights, and decisions (see **Figure 1**).

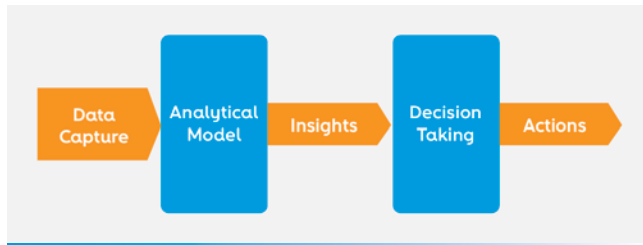


FIGURE 1 – Data-driven decision pipeline

Data's subjectivity arises from various decisions that go into its definition, capture, processing, and interpretation. For example, there were a series of human decisions involved in the definition of the metric systems. Similarly, many human decisions are involved in the design and deployment of sensors throughout our environment: who decides where they should be located, and why did they choose the locations they did? Furthermore, during data processing, many decisions affect the outcomes of any data analysis process, concerning how data is cleaned, merged, the questions used to frame the analysis, or the computational models and techniques used to extract insight from it. Finally, the contentious nature of data interpretation can easily be seen

in the policies adopted in the face of the same data, for example, how society must respond to COVID-19, given its most recent economic and health statistics.

The same data sometimes spawns antagonistic interpretations and reveals information that may lead to different conclusions, according to contexts, beliefs, or experiences. It is easy to observe the opposite perspectives on the same information when analyzed by government members or opposition. The same is true in the sports world: for the same fact, fans of opponent teams may have opposite opinions, whose conclusions aren't always purposeful or malicious.

Although data is intrinsically historical and may seem suitable for reporting what has happened, the emergence of modern data-driven artificial intelligence (AI) systems that can make accurate predictions has unlocked data's power to support decision making and so affect future outcomes. For example, a study of 179 publicly traded firms in 2011 found that firms that adopt data-driven decision-making processes have higher output and productivity than would be expected given their other investments [1].

Somewhat ironically, the power of big data and AI to drive successful decision making is also one of the primary triggers for the growing awareness of the potential harm resulting from data and ever-increasing discussions about data ethics and the need for new data regulations, such as the General Data Protection Regulation (GDPR). In fact, due to the growing prevalence of sensors in modern societies and the tracking of individual behavior in the online setting, these discussions try to shed light on important questions about personal privacy, civil liberties, targeted advertising, and the rise of targeted misinformation.

In the remainder of this article, we will address some of the emerging challenges and opportunities that big data and modern AI pose to individuals and societies.

The good

Data can be and should be used for good. Data is the basis of a set of innovative businesses enabling creative services and operational optimizations.

The evolution of wired and wireless communication systems was vital to support digital transformation. The ubiquitous access to data improved operational efficiency and reduced costs across all sectors of activity. The advent of IoT networks was fundamental to creating the smart cities vision, where data coming from networks of distributed sensors is used to model, in near real-time, and manage the evolving situation of urban space. Similarly, the management of telecommunications networks has also been improved by using distributed sensors and data-driven decision-making. For instance, Communication Service Providers (CSP) uses data-driven predictive maintenance to avoid equipment malfunctions and improve network resource management. Simultaneously, the explosion of data about humans and society that occurred with the shift to online life and the emergence of social media platforms has enabled innovative commercial consumer engagement services supported by big data. Examples of these innovation types include recommendation systems associated with personalized advertising or cross-selling and even churn detection and prevention.

Beyond the business opportunities, access to open datasets about communities and cities, computational resources, and open-source frameworks for data science create conditions for using data to support and empower communities. For example, in recent years, we've seen the emergence of a vibrant "data for good" community. A common theme across these initiatives is the use of data to positively impact the world by fostering the objectives of sustainable development, such as reducing poverty, preserving the environment, or promoting a healthier life.

Naturally, the positive use of data is not limited to these bottom-up grass-roots movements. Governments and international organizations are also keen to leverage the power of data for the public good. Indeed, some of the responses initiated by governments to the COVID-19 pandemic can be understood as using data for good and can be directly linked to the data pipeline described in the introduction. The utilization of personal data in an anonymized way is the basis for new mobile applications aiming to retard virus propagation. Grantz et al. [2] stated that mobile phone data could be used to fight against COVID-19 as a non-pharmaceutical intervention. It can include location-based information, supplied by the CSPs (call detail records) or provided by the mobile GPS; proximity data through bluetooth; or even application data explicitly inserted by users. The collected data may be used in different ways, such as following the risk of importing the virus from a region, detecting mobility patterns, or for contact tracing to advise quarantine to potentially infected people.

The bad

However, governments and large organizations' promise of using data for good can also threaten civil liberties. Two arguments are often used to support the adoption of data-driven infrastructures and technologies throughout society. The first argument is that they can use data to improve systems' efficiency, effectiveness, and competitiveness. The second argument relates to enhancing security; for example, governments often argue that increased surveillance improves security [3].

Regarding the use of data to improve efficiency, effectiveness, and competitiveness, a large body of research indicates that the more personalized advertising is to an individual, the more effective it is [4]. Consequently, companies are encouraged to gather data about their customers to target

and personalize their offers, thus improving their advertising effectiveness. However, although personalization may appear desirable in many ways at a surface level, it inevitably leads to marginalization [5]. For example, targeting a special offer to one customer necessarily marginalizes the customers who do not receive this offer. This form of data-driven discrimination is particularly blatant on websites that use differentiated pricing, where some customers are charged more than others based on their profile [6]. More broadly, data-driven personalization can be understood as a form of negative social profiling.

Beyond marketing and commercial activities, data-driven decision-making and AI are often framed as improving governments' efficiency; for example, smart city technologies are marketed as using data to make public services more efficient and less costly [7]. However, data-driven decision systems work by identifying patterns within data and using the identified patterns to generate output. If the data patterns reflect society's prejudices, then these prejudices will be reinforced by these "smart" systems. This systematic reinforcement of prejudice is particularly problematic when data-driven systems are used for predictive policing or to inform judicial decisions [3].

The emergence of smart city technologies has led to a proliferation of sensors throughout modern societies, powered by modern digital technologies that make it easier to track people through their mobile phones and credit card usage. Furthermore, in online settings, individuals are tracked through the search terms they use, websites they visit, and items they click on to facilitate targeted marketing. Taken together, these different forms of surveillance mean that it has never been easier to track a person's movement and behavior, compromising personal privacy and leading to a self-disciplining effect that curtails personal freedom and has the potential to ultimately undermine democratic processes by diminishing our collective ability to act as political and social agents [8]. However, all these concerns are related to the improper use of real data.

Another set of concerns arises when considering the growing amount of fake data generated not for testing systems purposes but distributed to distort reality. The usage of fake data can be associated with cheating to make money or intentionally harm a person, organization, or country. Disinformation is false information deliberately created and distributed to damage the image of a person or entity. It affects society as it shapes collective minds, even undermining democracy as we know it. The rapid spread via digital platforms, such as Facebook, Google, or Twitter, makes them reach everywhere and persist for eternities, creating alternative truths, sometimes injuring the truth of death. Donald Trump used the term fake news to describe news that hindered his candidacy for the USA's presidency. But fake news has become popular as news that intends to affect the truth to make gains based on lies. The Cambridge Analytica scandal highlighted the risks of the misuse of personal data. The company was accused of using millions of Facebook users' data without their consent to influence the Brexit referendum results and the 2016 presidential election in the USA [9]. The exploitation of psychological profiles combined with profile-based political ads (sometimes exempt the fact-checking) can be used as a powerful weapon to influence people, exposing the weaknesses of democratic processes [10], [11]. In fact, the post-truth appears to be gaining ground in many nations: public opinion is being shaped more by emotional appeals in the form of ads than by objective facts spread by credible sources.

In a growing disinformation world, the spreading of AI deep learning technologies that can generate deep fakes is a worrying development [12]. Deep fake systems can combine images and sound to create fake videos of people that are very difficult to distinguish from real videos, bringing the idea of fake news to a whole new level of danger. It becomes possible to easily undermine the public image of a person or a social group; for example, election results can be distorted by the appearance of a fake video the day before the elections purportedly showing

a candidate doing something illegal, such as receiving bribes. The spread of available tools to create false video content makes the digital world a potential battlefield requiring strong policies and ethics in data to avoid chaos.

And the ethical

In this section are addressed three key pillars of ethical data use (see **Figure 2**): understanding and compliance with data regulations; the creation of a culture of ethical action within an organization; and the engagement with stakeholders and communities potentially affected by data usage and modern AI data-driven technologies throughout the design and development of these technologies.

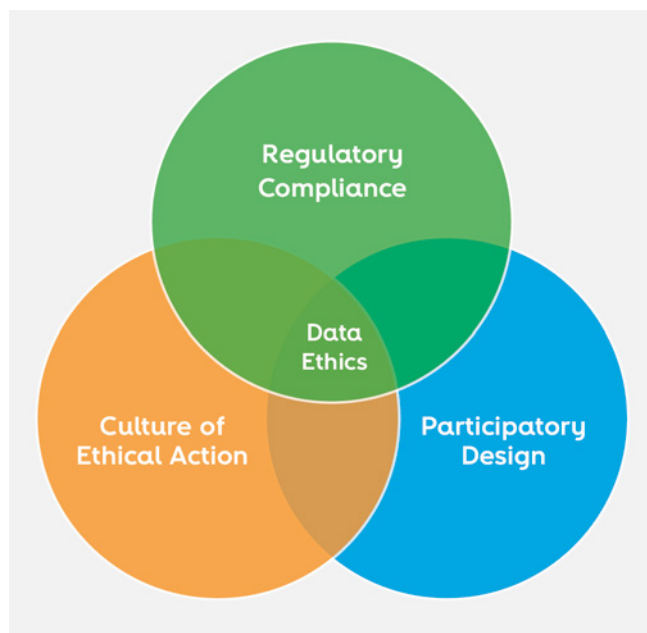


FIGURE 2 – The three key pillars of the ethical use of data

Legal frameworks concerning data usage vary across jurisdictions. However, the majority of legal frameworks contain regulations relating to anti-discrimination and also personal data protection. Most anti-discrimination rules forbid

discrimination based on any of the following protected categories: disability, age, sex, race, ethnicity, nationality, sexual orientation, and religious or political beliefs. Consequently, apart from particular contexts such as medical assessment, data relating to these categories should not be used as the basis for decisions relating to an individual. Complying with this restriction can be more complicated than it might first appear because these protected categories can often be encoded in data through proxy variables. For example, including an individual's address within a dataset may inadvertently make it possible to predict their race or ethnicity.

Furthermore, when datasets are merged, the possibility of these protected types of information becoming identifiable through the combination of features from the combined datasets often becomes feasible (data re-identification). Consequently, care needs to be taken both in the design of datasets, their curation, and the testing of any technologies built using these datasets to ensure that the resulting decisions driven by the technology are not biased by one or more of these categories. It is also important to highlight that this bias can occur at a group level or individual level. For example, at the group level, a system might systematically be biased towards a particular race or ethnicity. However, even if it can be demonstrated that, on average, the decisions made by a system are not biased towards a specific category, it is still problematic if, for a particular individual, the system uses data relating to one of the protected categories to decide for that individual. This is why it is essential to understand how modern AI data-driven systems make decisions, how these decisions are distributed across different communities of people, and what data a system accesses and uses when deciding on an individual. These are the questions at the core of research fields such as explainable AI.

Concerning the use of personal data, probably the most significant recent development has been the GDPR [13]. The GDPR is legally enforceable across all EU member states; however, perhaps the most broadly accepted personal privacy

principles are the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [14]. Indeed, the GDPR can be traced back to these OECD guidelines. In these guidelines, the concept of personal data is defined as data

relating to an identifiable individual, known as the data subject, and the data controller determines the purposes for which and how personal data is processed. There are eight core principles set out in the OECD guidelines, as depicted in **Figure 3**.

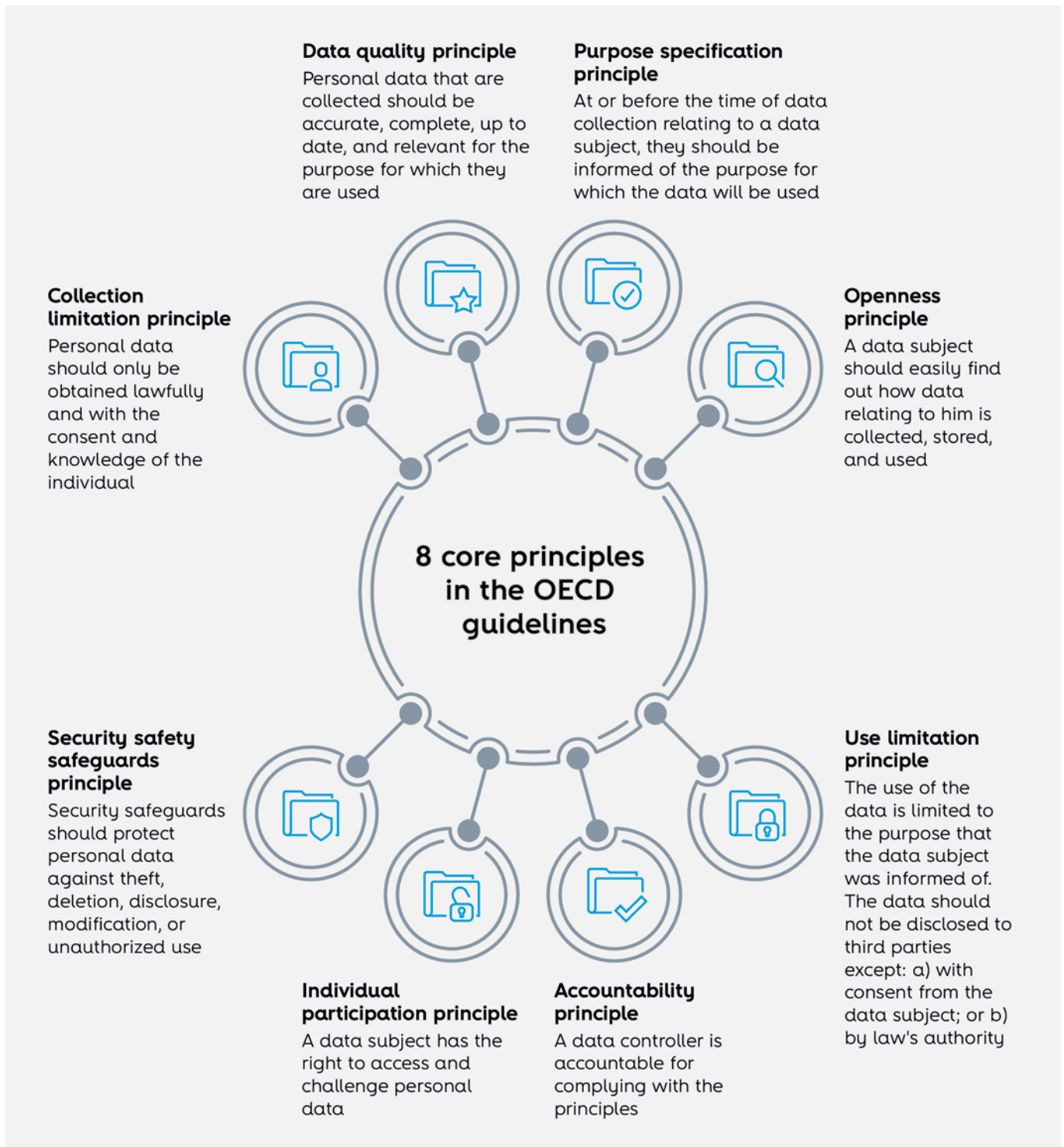


FIGURE 3 – OECD privacy guidelines: basic principles of national application [14]

Although these principles are relatively straightforward in their meaning and intent, it may be challenging to translate them into a culture of ethical action and practice within an organization [7]. Many professional bodies have developed guidelines to help their members in transposing regulatory principles to practice. For example, the IEEE has produced a call to action for businesses using AI entitled Ethically Aligned Design (EAD) [15]. This call to action is relevant to the ethical use of data because data is at the heart of modern AI systems. The EAD highlights the value of necessity foregrounding ethical considerations throughout AI technology and data-driven organizations. In particular, developing an ethics-based culture and implementing ethics-based systems and practices within an organization is the basis for building trust with investors, stakeholders, employees, and customers. The EAD suggests a two-stage process for organizations to develop and sustain a culture of ethical practice. In the first phase, people are introduced to ethical concepts relating to AI design and data usage at scale. This first phase includes working with executives to identify the organization's core values and ethical principles and launching a communication and training campaign. The second phase involves helping, supporting, and incentivizing people to understand and apply these new concepts within their work's local context. This may include identifying and training a core team of strategically positioned employees who can provide local support and evangelize the importance of ethical decision-making. It also involves emphasizing the consideration of ethical implications as a core function of each person's role and incentivizing people to make ethical decisions. The goal here is to move people from awareness of ethics to ethical action.

The widespread use of AI and data-driven systems throughout modern societies means that everyone involved in their design, development, and use should be mindful that technology is never neutral, being aware of any technology's ethical implications. Furthermore, they should consider short-term impacts and long-term

impacts and how technology might affect a future society. Consequently, technology should be designed and developed aligned with the values of the society it affects. This means that human needs and the protection of human rights should be at the core of the design and use of AI technology and data, requiring understanding and empathizing with the community members that will be affected by that technology. The best way to develop this understanding is to engage with stakeholders and the community throughout the technology development lifecycle by adopting, for example, the participatory design (or co-design) concept where the end-users and those potentially affected by technology are invited to work with technology designers and developers during the innovation process.

Conclusions

Data by itself is neither good, nor bad, nor unethical. It is the use that data is put to which is essential. Properly used data can improve business, manage cities and sustainable development, and help control diseases.

In its turn, fake data can be used to distort the truth and undermine democracy, and large scale data ecosystems may threaten civil liberties. The use of data, mainly when it involves personal data, raises ethical issues, which affect all the data lifecycle. Responsible utilization of data must prevail regardless of the context in which it is being used. In addition to the processes related to data collection and storage, more critical issues arise when data is associated with AI mechanisms to extract knowledge and predict an individual's behavior based on the data collected about them without their awareness. Besides strong regulation, organizations must proactively work to develop a culture of ethical action and engage with external communities and stakeholders to ensure that ethical practice is at the heart of technical innovation and data usage.

Data is like pills: when used according to the rules, they can be highly effective, but if used without any control, they can be harmful and can even cause irreversible damage. Regardless of whether it is true or false, data can be applied for a worthy purpose or misrepresenting the truth. In the end, it isn't the data; it is how it is used! 🌐

Acknowledgments

Some of the findings mentioned in this article result from research conducted at Technological University Dublin with the financial support of the ADAPT Research Centre which is funded by the SFI Research Centres Programme and is co-funded under the European Regional Development Fund (ERDF) through Grant #13/RC/2106.

References

- [1] Erik Brynjolfsson, Lorin M. Hitt, and Heekyung Hellen Kim, "Strength in Numbers: How does data driven decision making affect firm performance?", SSRN Electronic Journal, DOI: [10.2139/ssrn.1819486](https://doi.org/10.2139/ssrn.1819486), 2011
- [2] Kyra H. Grantz et al., "The use of mobile phone data to inform analysis of COVID-19 pandemic epidemiology", Nature Communications 11, 4961 (2020). <https://doi.org/10.1038/s41467-020-18190-5>
- [3] John D. Kelleher and Brendan Tierney, "Data Science", MIT Press, 2018
- [4] Shawndra Hill, Foster Provost, and Chris Volinsky, "Network-Based Marketing: Identifying Likely Adopters via Consumer Networks", Statistical Science 21(2) pp. 256-276, 2006
- [5] John D. Kelleher and Aphra Kerr, "Finding common ground for citizen empowerment in the Smart City", Ethics and Politics, 22(2), pp. 33-61, 2020. doi: [10.21427/9fr1-9540](https://doi.org/10.21427/9fr1-9540)
- [6] Tim Walker, "How much ...? The rise of dynamic and personalised pricing", The Guardian, 20 Nov. 2017. [Online]. Available at: <https://www.theguardian.com/global/2017/nov/20/dynamic-personalised-pricing>
- [7] Aphra Kerr, Marguerite Barry, and John d. Kelleher, "Expectations of Artificial Intelligence and the Performativity of Ethics: Implications for Communication Governance", Big Data and Society, 7(1), 2020. doi: [10.1177/2053951720915939](https://doi.org/10.1177/2053951720915939)
- [8] Noel Fitzpatrick and John D. Kelleher, "On the Exactitude of Big Data: la Bêtise and Artificial Intelligence", La Deluezia, 2018. doi: [10.21427/dfw8-m918](https://doi.org/10.21427/dfw8-m918)
- [9] Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", The Guardian, Mar 2018. [Online]. Available at: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- [10] Dipayan Ghosh and Ben Scott, "Facebook's New Controversy Shows How Easily Online Political Ads Can Manipulate You", Time, March 2018. [Online]. Available at: <https://time.com/5197255/facebook-cambridge-analytica-donald-trump-ads-data/>

- [11] Natasha Lomas, "Facebook finally hands over leave campaign Brexit ads", Tech Crunch, July 2018. [Online]. Available at: <https://techcrunch.com/2018/07/26/facebook-finally-hands-over-leave-campaign-brexit-ads/>
- [12] John D. Kelleher, "Deep Learning", MIT Press, 2019
- [13] European Council and Parliament, "General Data Protection Regulations of the European Council and Parliament", Official Journal of the European Union L 119: 1-2016. [Online]. Available at: https://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- [14] Organization for Economic Co-operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", 2013. [Online]. Available at: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm>
- [15] IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, "Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems", March, 2019. [Online]. Available at: <https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead/ead-for-business.pdf>



08

SmartAL is adopting
PETs!

Mafalda Nunes, Altice Labs

mafalda-g-nunes@alticelabs.com

Ricardo Machado, Altice Labs

ricardo-j-machado@alticelabs.com

José Bacelar Almeida, Universidade do Minho

jba@di.uminho.pt

Privacy enhancing technologies are experiencing a renaissance as global awareness, demand, and regulation for privacy increases. Besides helping to achieve compliance with privacy policies or data protection legislation, these technologies also boost the data subjects' trust in the solutions developed to address the current reality we are living in, triggered by the pandemic crisis.

In this article, we will present some privacy enhancing technologies applied to Altice Labs' SmartAL.

Keywords

PET; Security-by-design; Privacy-by-design; SmartAL

Introduction

The term privacy enhancing technologies (PET) has been around for decades and is now experiencing a renaissance as global awareness, demand, and regulation for privacy increases. PET help achieve compliance with privacy policies or data protection legislation, such as the European Union General Data Protection Regulation (GDPR) [1].

The term covers the broader range of technologies and approaches (from a piece of tape masking a webcam to advanced cryptographic techniques) designed to enable, enhance, and preserve data privacy throughout its lifecycle [2]. Data can be considered to have three stages in its lifecycle: at rest, in transit, and in use. The usage of PET is mainly focused on the third stage, in which data assets are meaningfully used or processed, and also in the first stage, where the use of stored data is somehow facilitated by the applied technologies.

Organizations frequently need to execute operations such as sharing, searches, or analytics over data, which creates points of data exposure. PET are designed to help reduce this vulnerability by enabling data to be securely and privately processed. Examples of areas where these technologies can be applied are data analysis, machine learning, e-health, cloud computation, internet of things (IoT), among others. The current COVID-19 pandemic reality, for example, has been exposing privacy and security issues related to the processing of sensitive data, such as location and health information. These issues could be addressed using PET, along with other security mechanisms.

In this article, there will be an analysis of some promising PET, their applicability scenarios, and maturity level. The article will also address a practical application of some of those PET in an assisted living platform (SmartAL), a scenario that will require the handling of sensitive data (health) and a guarantee of privacy and security for all users.

Privacy enhancing technologies

PET allow keeping the data subject's privacy in the data usage and storage stages, which can be associated with data collection, disclosure, storage, or computation. In this section, some promising PET that address one or several of these kinds of usage will be analyzed, including their advantages and disadvantages, maturity level, and some application cases. The PET that will be analyzed are briefly presented in **Figure 1**.

Anonymization and pseudonymization

The European Union Agency for Cybersecurity (ENISA) defines anonymization as the process of permanently modifying personal data in such a way that individuals can no longer be identified, and no information about them can be learned [3]. On the other hand, pseudonymization replaces identifiable or sensitive data with reversible artificial identifiers or pseudonyms [4]. The original values are securely kept but can be retrieved and linked back to the pseudonym if the need arises.

Some of the top reasons why enterprise businesses use anonymization [5] are:

- Protect data from third-party vendors, such as marketers, consultants, and others;
- Minimize the impact of data breaches that are a result of operator error;
- Perform operations where some of the data does not need to be real, such as conducting application tests.

Furthermore, anonymization can be one way to comply with the GDPR demands for secure data storage of personal information.

There are several privacy models that can be used for data anonymization, such as k-anonymization, differential privacy, and their

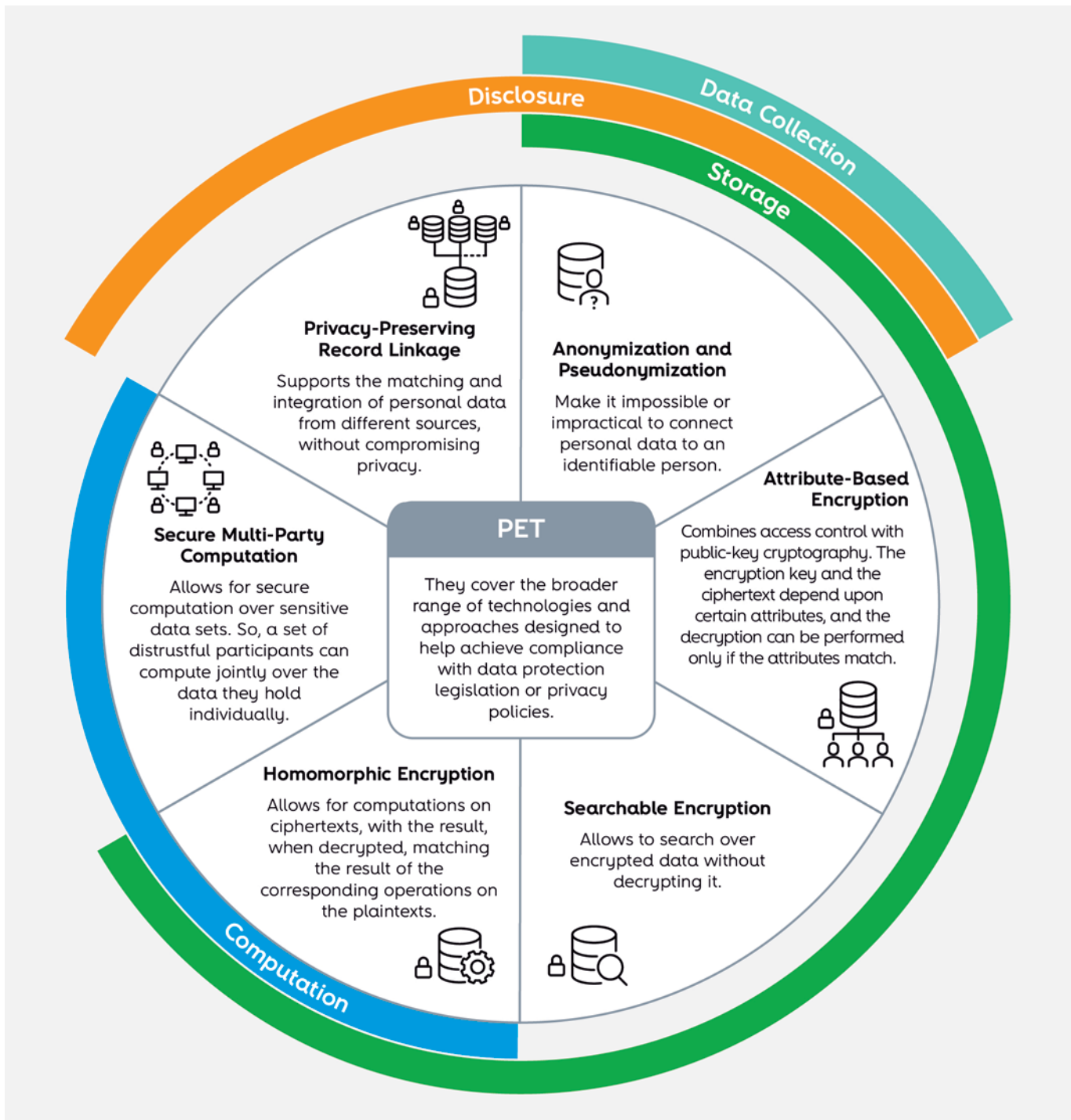


FIGURE 1 – PET covered by this article

variants. k-anonymization is an approach where certain values in a dataset are suppressed or generalized, ensuring that the information from any single individual cannot be distinguished from at least k-1 other individuals in the dataset [6]. The differential privacy model seeks to limit the impact of any individual subject's contribution

on the outcome of the analysis by adding noise to data in a way that still permits valid statistical inferences to be made [3].

The differential privacy model has the advantage of being strongly composable, which means that combining two differentially private data sets still

results in a differentially private data set [3]. But this property is achieved through the addition of noise, which limits the utility of the anonymized results and the type of queries that can be performed.

In contrast, k-anonymity mechanisms focus on preserving data utility for general-purposes. However, k-anonymity is not composable and cannot guarantee privacy if sensitive values in the data set lack diversity and some further information is known to the attacker.

So, k-anonymity preserves better the data utility, while differential privacy provides stronger privacy guarantees.

Both these models are currently used by big companies to ensure data privacy. For example, Google uses k-anonymity alongside cryptographic hashing in its Password Checkup Chrome extension [7], which verifies if the used username and password are included in 4 billion credentials that Google knows to be unsafe, without disclosing the searched username and password. Also, Apple and Google implemented their own versions of distributed differential privacy for collecting statistics from end-users [6].

Privacy-preserving record linkage

Privacy-preserving record linkage (PPRL) solves the problem of matching records from distinct sources that refer to the same individual without compromising privacy [8].

Linking records makes it possible to combine data from different sources to answer research questions that are very difficult to answer using data from just one source [9]. In medical research, for example, data from several sources (e.g., hospitals) could be matched to investigate possible correlations between different diseases of the same patients without revealing the patients' identity. However, the quality of linkage procedures and the reliability of the linked datasets are difficult to determine, which constitutes a major issue in record linkage.

There are already some products available that allow two organizations to carry out private record linkage. However, there is still research on several components of this technique, such as performance and scalability [10]. Multi-party PPRL methods involving more than two data holders are also being analyzed.

Attribute-based encryption

Attribute-based encryption (ABE) combines access control with public-key cryptography in a way that the key used for encryption and the resulting ciphertext both depend upon certain attributes, such as the user profile, access level, or the individual's area of expertise [3]. This way, any user who possesses a certified attribute set matching the ciphertext attributes can decrypt the data with his own private key, without interacting with the data owner [11].

So, ABE has the same advantages as traditional encryption, such as confidentiality, reduced impact of data breaches, and data is secured regardless of how it is stored or transmitted. Besides, ABE also adds flexible access control to these advantages. The price to pay for having such fine-grained access control is the size of the ciphertexts, which grow linearly with the complexity of the access policy, or the number of attributes. It may also fail to perform in the presence of many users.

Despite that, ABE has been increasingly applied in areas where flexible access control of sensitive data is required, such as mobile computing, cloud computing, social networks, and IoT. Some more concrete application scenarios are pay-TV, e-health, cloud storage, among others [12].

Searchable encryption

Searchable encryption (SE) allows users to search over encrypted data without decrypting it [13]. With this technology, a user can authorize a third-party data storage server to retrieve his/her encrypted data without leaking either what is searched for or the data itself. However, most of the existing

SE schemes have a limited query expressiveness, being limited to searching by keywords.

SE's two main flavors are symmetric SE, which uses only one secret key, and public SE, which uses both a private and a public key. The possession of the secret key (or, respectively, the private key) allows not only to decrypt, but also to generate trapdoors for queries that, in turn, can be sent to third parties for running them on the ciphertext. As an example, data can be stored in encrypted form in the cloud and still allow authorized clients to request the execution of queries to the cloud provider without giving it access to the unencrypted data.

Symmetric SE has the advantage of efficiency, but it lacks in functionality, as it can only be used for a single user scenario by default. It can be applied to a scenario with multiple users, but the key distribution and management problem must be dealt with [14]. Public SE's main drawback is inefficiency, whereas the advantage is functionality because it can be more easily applied to scenarios with more than one user. However, this advantage brings other challenges regarding more complex multi-user scenarios, such as user authentication, access control, and revocation. Besides, in those cases, the key management is taken care of by the data owner, and he needs to be online every time a new user registers in the system [13].

Currently, no SE scheme addresses all issues mentioned above. There are already some schemes with more simple practical applications proposed, but there are still numerous research areas regarding this encryption technique. Examples of practical applications that could employ SE are an encrypted email system, cryptographic cloud storage, encrypted audit logs, IoT, and e-health systems.

Homomorphic encryption

Homomorphic encryption (HE) is an encryption scheme that allows for computations on ciphertexts, with the decrypted result matching

the result of the corresponding operations on the plaintexts [15]. This allows for a secure outsourced computation, where a third party can process the encrypted data without any key, and the process itself does not reveal any new information. The user with the key can decrypt the processed data and get exactly the plaintext processing result.

However, this technology has some limitations or disadvantages, such as the need for the data to be represented as polynomials, and the requirement of expert knowledge to design meaningful and useful programs based on HE.

There are several degrees of HE. In partial HE (PHE), only a restricted set of operations can be performed homomorphically, for instance, sums or multiplications. Various mature and efficient PHE schemes exist that have found numerous applications on specific problems, such as counting votes without compromising vote secrecy, in e-voting protocols. However, the restriction on the available operations severely limits its applicability to more ambitious scenarios.

Another possibility is fully HE (FHE), where arbitrary functionalities are allowed, usually expressed as some kind of circuit. Its flexibility dramatically increases HE's applicability, and the theoretical result establishing its possibility [16] is recognized as a breakthrough in recent cryptography research. For example, SE might be seen as a particular case of FHE. Unfortunately, the resulting schemes' complexity makes them prohibitively inefficient, and the research community clearly acknowledges that FHE is still not feasible in practical applications.

In between PHE and FHE, there's somewhat HE (SHE), where the allowed operations are not restricted a priori, but instead (some measure of) the complexity for the intended functionality is limited (e.g., the circuit depth). This is, indeed, an intermediate stage for the construction of FHE schemes and is still an area of active research. Nevertheless, SHE schemes have already found practical applicability in some recent advanced applications [17], in medical, financial, and advertising domains, for example.

So, PHE and SHE can already be practically applied to several real scenarios, while FHE is still the subject of ongoing research. It can also be applied to some scenarios, but with an unacceptable performance for actual use cases.

Secure multi-party computation

Secure multi-party computation (MPC) is a class of cryptographic techniques that allow for secure computation over sensitive data sets. In MPC, a set of participants jointly compute on data they hold individually, without ever revealing that data to the other participants [18]. If some parties, typically a majority, honestly follow the protocol, no party learns anything beyond the computation's final output.

So, MPC allows to execute collaboratively or distributed data mining on encrypted data coming from different parties, without the need for a trusted central authority. However, this technology has some disadvantages, such as the high computation time compared to the same processing with plaintexts, the reduced scalability due to the data size, the need for a different protocol for distinct computations, and the requirement of expert knowledge to implement a performant secure MPC.

During recent years, MPC techniques have experienced dramatic advances in their performance [19]. MPC has been applied in a limited number of products, research and development are ongoing, and other applications are at a proof-of-concept stage. Many examples show the importance of secure MPC constructions in practice, such as privacy-preserving decision making on distributed medical or financial data, privacy-preserving machine learning, auctions, among others.

The SmartAL use case

SmartAL is an Altice Labs' platform that enables the monitoring, in real-time, of chronic or senior patients, patients in convalescence or post-hospital follow-up, as well as disease progression, namely in chronic patients or COVID-19 asymptomatic or suspected cases, where isolation is mandatory. This platform allows the telemonitoring of vital signs, video consultation, and tracking activities related to health, well-being, and safety.

In this ecosystem, there are multiple user profiles, each with its own set of permissions and restrictions (for example, medical professionals can see their patients' vital signs, while clerical staff cannot). Taking into account the sensitivity of the information stored on this platform and the need to share it with other users, one of SmartAL's goals is to increase the level of protection of the user's privacy while keeping an acceptable performance on data access and manipulation. For that, new encryption techniques able to protect users' personal data will be considered. Another goal is to make it impossible for unauthorized entities to decrypt sensitive data, including the platform's server itself.

The aforementioned PET can be used to help to fulfill these goals. ABE can be used for fine-grained access control, HE to perform operations over encrypted data, and SE to search over the encrypted data. With this in mind, a solution based on the scheme presented by Pournaghi et al. [20] is proposed next.

This solution includes several entities, such as the trusted entity key generation center (KGC), that issues the user ABE private keys upon user authentication, and the semi-trusted entities data storage and security storage. The data storage is the SmartAL server, which stores the users' personal and medical data, among which the most sensitive will be encrypted. The security

storage will hold the keys used to encrypt the SmartAL data, ciphered with ABE. This way, only authorized users will have access to an ABE private key, that will allow them to decrypt the keys that give access to the SmartAL data. Regarding the platform users, some will be trusted entities, if they are authenticated and authorized to perform the intended operation. Otherwise, the user will be untrusted. Otherwise, the user will be untrusted. All entities involved in this scheme are presented in **Figure 2**.

The proposed approach consists of the following 3 phases:

- **Setup** – This is an initial phase in which some keys and administrative entities are created. The KGC generates the needed ABE master keys, and a default user with the system administrator profile is created in all servers: SmartAL, KGC, and security storage. This user will then create other users according to his permissions;
- **Write Data** – In this phase, data is inserted, encrypted, and stored. This process is shown in **Figure 3**. Before anyone entering data about a particular patient, an administrative user should establish a relationship between

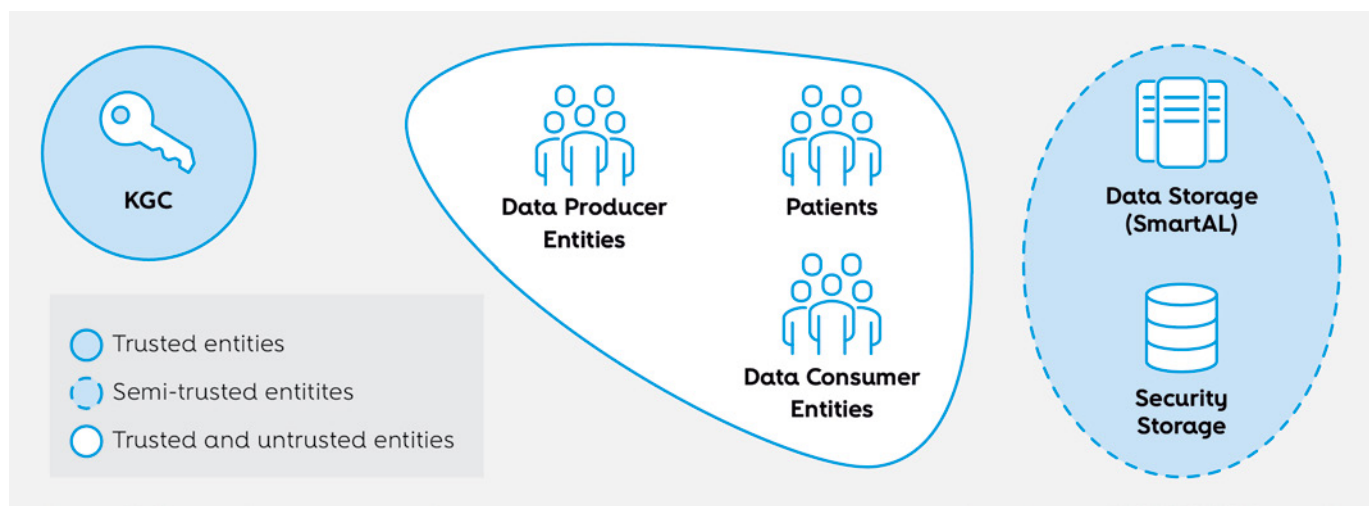


FIGURE 2 – Entities involved in the proposed scheme

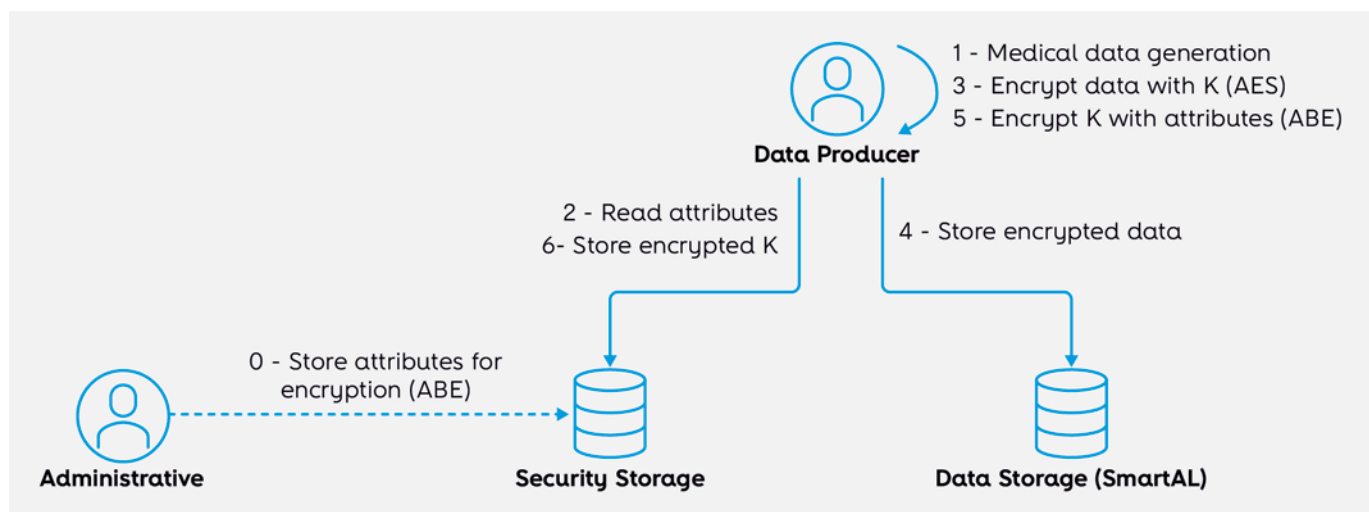


FIGURE 3 – Data storage phase from the proposed solution

the patient and the user entering the data, as well as set the ABE encryption attributes for that patient (step 0). Then, the data producer enters medical data, reads the respective attributes for the patient from the security storage, encrypts data with a key K , and stores the encrypted data on the SmartAL database (steps 1 to 4). Finally, K is encrypted using the attributes for the intended patient (ABE) and stored in the security storage;

- Read data – In this phase, data is read, decrypted, and presented. This process is shown in **Figure 4**. First, the encrypted key K is obtained from the security storage and decrypted using the data consumer ABE private key. Then, encrypted data is obtained from the SmartAL database and decrypted using K .

It should be noted that K can be the key of a simple symmetric cipher if there is no need for data processing on the server-side. The methodology of encrypting keys with ABE and data with a symmetric key is motivated by the greater efficiency of symmetric encryption and decryption operations. So, this methodology may

have its advantages if there is a large amount of data to encrypt and decrypt.

However, if there is an intention for the server to search or perform some operations over the encrypted data, K can be the key of a SE or HE scheme. Examples of this kind of operations are the comparison of encrypted patient measurements with threshold values to alert doctors if the heart rate is too high or the blood pressure drops, for example, or the computation of the encrypted body mass index (BMI) value from the user encrypted weight and height.

A basic version of this scheme was implemented, using only symmetric encryption over the SmartAL medical measurements. There was an expected decrease in this implementation performance compared to a model using only plaintext, mainly due to client-side processing, such as data encryption and decryption. Still, this implementation performance was evaluated on old smartphones, being the oldest one released seven years ago, and the results obtained were considered acceptable, revealing that such a scheme can already be used in practice.

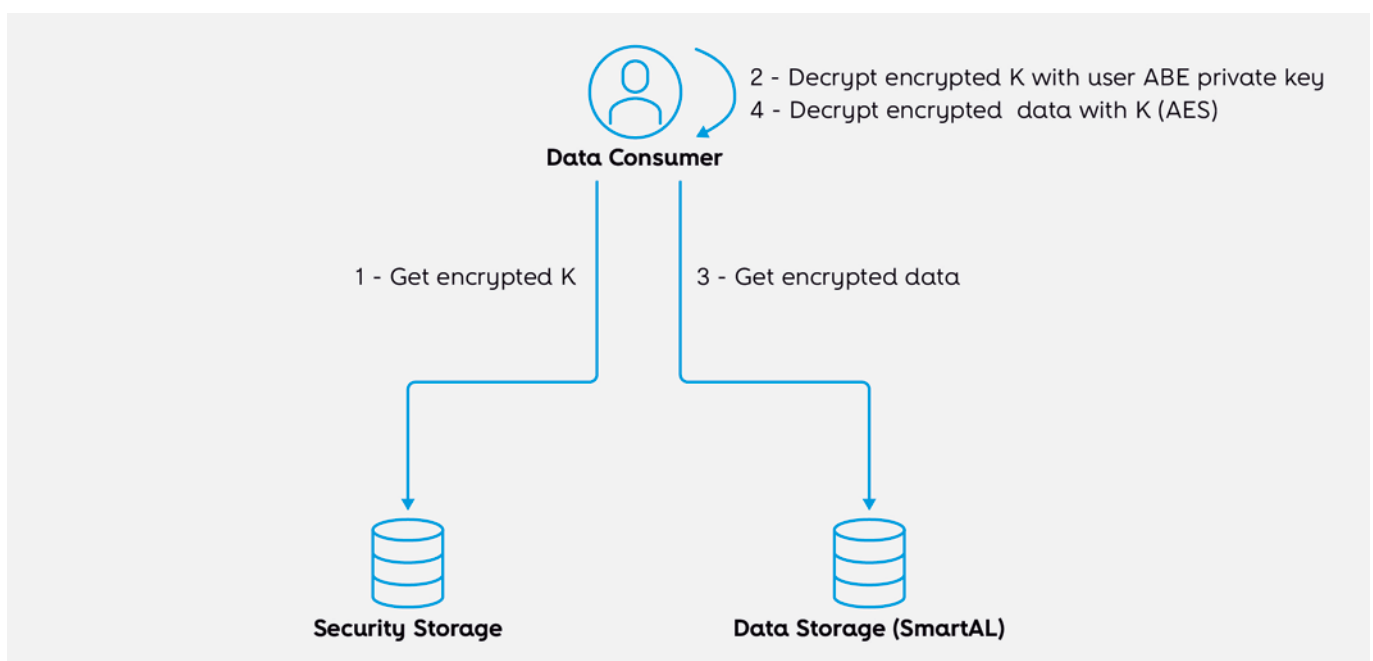


FIGURE 4 – Data reading phase from the proposed solution

Conclusions

The current economic environment still provides little incentive for deploying promising consent technologies, since online industry revenue streams are based on the collection of as much personal data as possible. However, data privacy laws such as the GDPR have gained more relevance and are designed to give users more control over their data while demanding from businesses more protection for their users' personal data.

Besides the economic environment, the current COVID-19 pandemic compelled the use of massive personal data to accelerate researches that better understand the disease evolution with the goal of developing an effective treatment or vaccine. Yet, data privacy and security concerns were, once again, belittled.

Privacy-enhancing technologies are a means of implementing data protection by design on a technical level, thus helping to achieve GDPR compliance. They embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals. These technologies also boost the data subjects' trust in the solutions developed to address the current reality we are living in, triggered by the pandemic crisis.

It should be noted that most existing PET encryption schemes are based on conventional cryptographic hardness assumptions, which are

vulnerable to adversaries equipped with quantum computers in the future.

All PET mentioned in this article have their advantages and disadvantages, and when choosing which ones to use, we need to strike a balance between security and performance. For SmartAL, the cost of the chosen PET in terms of performance, space occupation, and key management were considered acceptable. Given the very sensitive nature of the information that is handled, the increase in privacy and security, while maintaining the functionality, far outweighs the negatives of using these technologies.

From a business point of view, the most obvious reason to invest in PET would be to avoid the heavy fines imposed by GDPR, but that would be a narrow view of the problem. Recent data leaks have increased public perception of security. Through no fault of their own, their personal information can become available on the internet, which, at best, can be obnoxious and, at worst, life-ruining. There is a demand for accountability, and the consequences of ignoring fundamental security guidelines are clear. Privacy is no longer opt-in; it's a requirement.

Information is valuable, and users are starting to think twice before trusting a company with their data. This concern can be mitigated by the adoption of PET, which in turn will increase the company's credibility. By guaranteeing privacy-by-design products and services, a company's offer will certainly stand out from the crowd. 🌐

References

- [1] Intersoft Consulting, "GDPR," [Online]. Available: <https://gdpr-info.eu/>
- [2] E. A. Williams, "CPO Magazine," 25 May 2020. [Online]. Available: <https://www.cpomagazine.com/data-privacy/whats-old-is-new-again-examining-privacy-enhancing-technologies/>
- [3] G. D. Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y.-A. d. Montjoye and A. Bourka, "Privacy by design in big data," 2015
- [4] PrivSec Report, "Data masking: anonymization or pseudonymization?," 28 September 2017. [Online]. Available: <https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/>
- [5] S. Watts, "Data Masking: An Introduction," 22 June 2018. [Online]. Available: <https://www.bmc.com/blogs/data-masking/>
- [6] The Royal Society, "Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis", 2019
- [7] J. Pullman, K. Thomas and E. Bursztein, "Protect your accounts from data breaches with Password Checkup," 5 February 2019. [Online]. Available: <https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html>
- [8] M. Franke, M. Gladbach, Z. Sehili, F. Rohde and E. Rahm, "ScaDS Research on Scalable Privacy-preserving Record Linkage," *Datenbank-Spektrum*, vol. 19, p. 31–40, 2019
- [9] A. Ariel, B. Bakker, M. d. Groot, G. v. Grootheest, J. v. d. Laan, J. Smit and B. Verkerk, "Record Linkage in Health Data: a simulation study," 2014
- [10] Z. Sehili, M. Franke, M. Gladbach, F. Rohde and E. Rahm, "Privacy Preserving Record Linkage (PPRL)," 13 March 2018. [Online]. Available: https://dbs.uni-leipzig.de/research/projects/ppr_big_data
- [11] V.-H. Hoang, E. Lehtihet and Y. Ghamri-Doudane, "Forward-Secure Data Outsourcing Based on Revocable Attribute-Based Encryption," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019
- [12] Q. M. Malluhi, A. Shikfa and V. C. Trinh, "A Ciphertext-Policy Attribute-based Encryption Scheme With Optimized Ciphertext Size And Fast Decryption," in *ASIA CCS '17: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017
- [13] U. Varri, S. Pasupuleti and K. V. Kadambari, "A scoping review of searchable encryption schemes in cloud computing: taxonomy, methods, and recent developments," *The Journal of Supercomputing*, vol. 76, n° 4, 2020
- [14] Y. Lu and J. Li, "Constructing certificateless encryption with keyword search against outside and inside keyword guessing attacks," *China Communications*, vol. 16, n° 7, pp. 156–173, 2019
- [15] X. Ma, C. Liu, S. Cao and B. Zhu, "JPEG Decompression in the Homomorphic Encryption Domain," in *MM '18: Proceedings of the 26th ACM international conference on Multimedia*, 2018

- [16] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, Bethesda, MD, USA, Association for Computing Machinery, 2009, p. 169–178
- [17] M. Naehrig, K. Lauter and V. Vaikuntanathan, "Can Homomorphic Encryption Be Practical?," in *Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop*, Chicago, Illinois, USA, Association for Computing Machinery, 2011, p. 113–124
- [18] N. Volgushev, M. Schwarzkopf, B. Getchell, M. Varia, A. Lapets and A. Bestavros, "Conclave: Secure Multi-Party Computation on Big Data," in *Proceedings of the Fourteenth EuroSys Conference 2019*, Dresden, Germany, Association for Computing Machinery, 2019
- [19] F. Bayatbabolghani and M. Blanton, "Secure Multi-Party Computation," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Toronto, Canada, Association for Computing Machinery, 2018, p. 2157–2159
- [20] S. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, 2020



09

Operators' role in next generation MCX

Francisco Fontes, Altice Labs

fontes@alticelabs.com

Rui Calé, Altice Labs

cale@alticelabs.com

José António Almeida, Altice Labs

jose-s-almeida@alticelabs.com

Carlos Pardelinha, Altice Portugal

carlos-pardelinha@telecom.pt

5G and the edge are presented as important enabling factors in the evolution from classical mission critical communications into mission critical intelligence, pushing for a new generation of mission critical services. Here we introduce the present status and trends in this area, the business models supporting them, and the roles that mobile network operators can play.

Keywords

Mission-Critical; Edge; 5G; PPDR; Business-model

Introduction

Governments and companies need their public protection and disaster relief (PPDR) teams and critical national infrastructure (CNI) to accurately evaluate an incident and its context, ensuring the right means and actions are involved, with high operational efficiency and providing the best timely response. Current narrowband technologies used by emergency services are a trusted way to transmit voice. Still, they cannot meet the requirements for the integration of new communication components, such as video, telemetry, remote monitoring and control, required for real-time scenario analytics. These services must be available even in extreme circumstances, guaranteeing that rescue organizations can effectively collaborate when dispatching and managing heterogeneous intervention teams.

The quest for efficiency, security, and prediction is changing the paradigm of information collection and dissemination by PPDR organizations, which no longer depend only on mission-critical communications but are starting using mission-critical intelligence [1], defining the requirements for the next generation mission-critical communications.

The need for a new approach, based on operators' infrastructures, is generally accepted and already reflected by entities such as the European Commission, which already concluded in a 2014 study that *"commercial mobile broadband networks could be used for mission-critical communications with the right legal, regulatory and contractual framework and only if several requirements are fulfilled."* [2]

In this context, 5G networks are emerging as being capable of supporting those new services, with the required availability and reliability, as well as enabling the functional vectors of next generation mission-critical intelligence, connecting everything everywhere, and providing contextual awareness, intelligent ecosystems, and critical intelligence.

Thus, 5G is the next big step, with efficient implementations and better answering requirements of coverage, availability, and security, at an affordable cost.

Next generation mission-critical communications enable PPDR actors to use the 5G broadband wireless network in use cases that will allow them to create a situational and contextual awareness within the geographical perimeter of the crisis scenarios. Use cases with great relevance are the following:

- **Video-surveillance for disaster relief:** the use of surveillance drones to aid the problem of tracking humans quickly from a distance in areas with difficult or slow access, or unsafe for a human to reach;
- **Remote diagnostics in a connected ambulance:** the use of augmented reality, virtual reality, and robotics in an ambulance to allow clinicians to assess and diagnose a patient remotely, view medical records, vital signs, and ultrasounds;
- **Robotic remote operation:** the use of remote-controlled robots to enable specialized people avoiding the risks associated with performing specific tasks at places of difficult access or with dangerous working conditions;
- **Real-time remote health monitoring:** the transmission of physiological signals, collected from wearable or implantable medical devices, from PPDR actors operating in crisis scenarios.

Technological components: 5G and the edge

In the context of mission-critical services (MCX), 5G, as seen before, is surrounded by expectancy and has the potential to play a relevant role. In a shared environment, edge computing is the perfect 5G companion to exploit its characteristics and guarantee the required reliability levels at reduced costs.

5G

5G is observing a widespread deployment, based on 3GPP Rel-15 (5G Phase 1) specifications and the defined non-standalone (NSA) mode of operation, adding additional bandwidth to existing 4G networks. 5G deployments in standalone (SA) mode (requiring a 5G Core), based in the same Rel-15, started by middle 2020, with a first related announcement made by T-Mobile in August 2020 [3].

In past July, the first set of 5G Phase 2 standards were approved [4], providing all required features to support 5G enhanced mobile broadband (eMBB), massive machine-type communications (MTC), and ultra-reliable and low-latency communications (URLLC) use cases [5]. Only at this stage is 5G accomplishing its main objective of answering B2B communications' requirements, like reliability and low latency, besides improving targeted B2C services (e.g., with more bandwidth and higher moving speeds). In that context, several verticals will be able to exploit a shared 5G infrastructure via tailored slices to their needs, with slicing being explicitly and natively supported as its edge computing. 5G incorporates the native capacity to provide access to services from the core, to the very near edge, possibly from service platforms located at or very close to cell sites.

MCX, where the public protection and disaster recovery (PPDR) area fits, will benefit enormously

from exploiting common 5G features, like general lower latency, improved resilience, and accurate localization information (Rel-16). However, for the specific PPDR vertical benefit, 5G Rel-16 specifications include, and subsequent 3GPP Releases will further extend or optimize, additional features, some contributing to increase 5G own resiliency and coverage. That is the case of:

- **Sidelink (SL) communications in partial or out of coverage**, allowing terminal equipment to communicate directly [6];
- **Multi-radio dual connectivity (DC)**, where terminals communicate simultaneously over different radio bearers, increasing reliability [7];
- **Integrated access and backhaul (IAB)**, where 5G cell sites act both as access and backhaul for other cells, guaranteeing operation without the need for a transport network [8];
- **Isolated operation for public safety (IOPS)**, allowing cell sites to provide a minimum set of services at their area of coverage, in case of complete isolation with the rest of the network [9];
- **5G expansion to include non-terrestrial network (NTN) accesses**, for instance, using satellite communications to extend geographical coverage to previously unreachable locations (e.g., deep valleys) [10].

In addition, 5G new radio (5G-NR) has the capacity to efficiently operate in all ranges of frequencies, with no changes in the radio interface. Thus, it may operate at higher frequencies for higher bandwidths, in an urban context, and at lower frequencies for coverage and penetration, useful in crisis scenarios. Opportunistic operation in unlicensed spectrum may also contribute to increased network availability during emergency situations. Other relevant features include user equipment (UE) power-savings features and enhancements to multimedia broadcast multicast services (MBMS) [11], based on groupcast communications. Finally, the specifications also include specific interfaces (SEAL [12] and CAPIF [13]) for applications and

services to access 5G provided services, like location information. **Figure 1** shows how some of the different mentioned mechanisms fit.

However, some of the mentioned mechanisms are incompatible. Specific PPDR 5G slices need to be configured with the right characteristics. For instance, accurate localization information requires 5G to operate in higher frequencies, while higher coverage and penetration, relevant aspects for PPDR in general, are obtained at lower operating frequencies. Thus, there is a need to evaluate how to compose 5G services and features for a holistic PPDR platform, serving all involved actors across the disaster cycle, from prevention to recovery.

In most countries, all the 5G spectrum is being assigned to operators. The usage of 5G by public

entities for such specific public protection services requires the best service to be guaranteed, according to the requirements. Thus, one possible solution may use shared spectrum and implement a, yet to be standardized, specific PPDR vertical slice, as is already the case for vehicle-to-everything (V2X), in all operators, and a common core, independent of those. Having a mobile virtual network operator (MVNO) for PPDR is another possibility.

Another important aspect is the addition of artificial intelligence/machine learning (AI/ML) to manage 5G complexity and guarantee the best usage of 5G allocated resources. In disaster scenarios, this can help in the automated allocation of the right communication means to the involved actors.

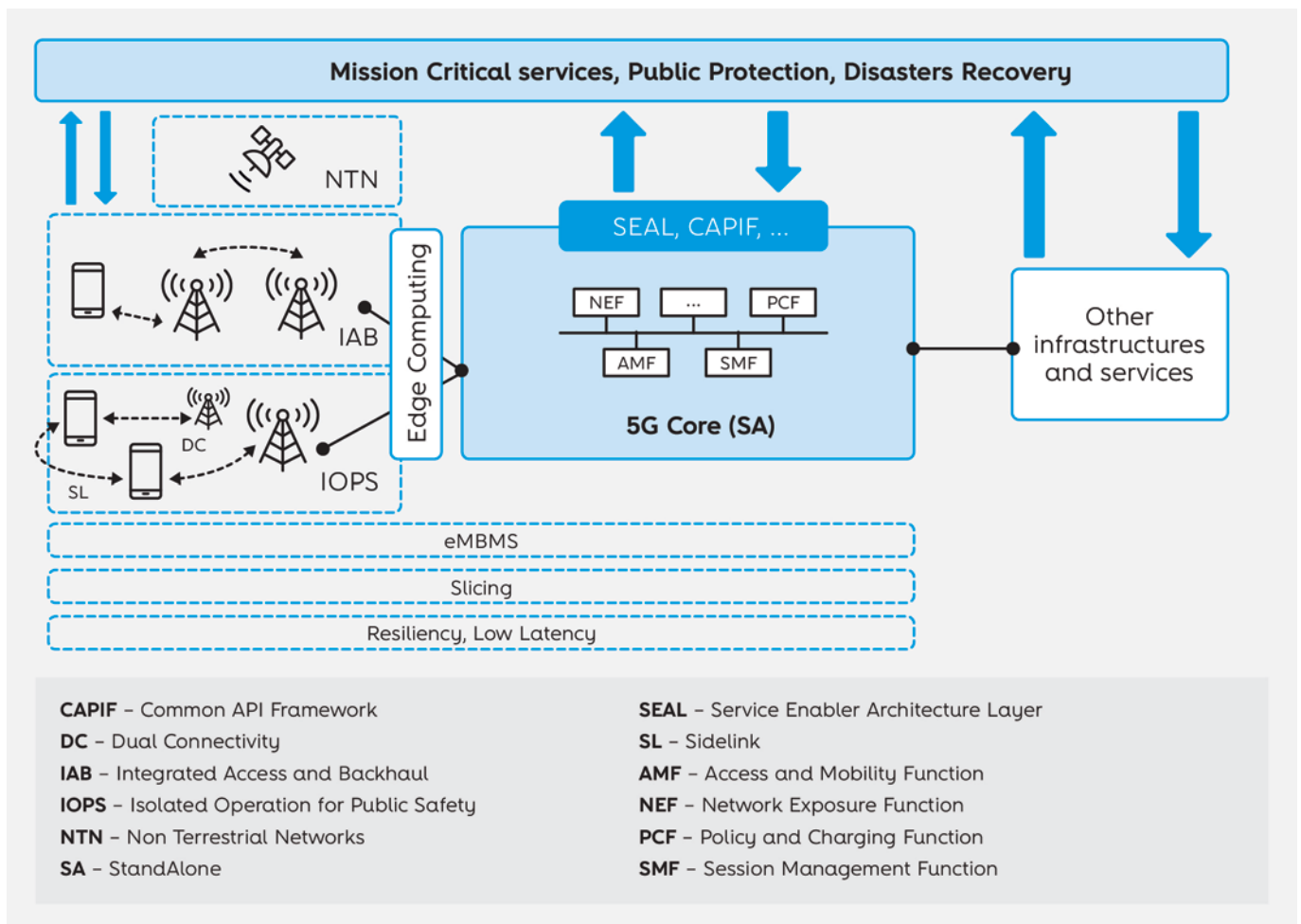


FIGURE 1 – Different 5G features exploitable by MCX

Network edge

Under catastrophic situations, such as earthquakes, fires, or heavy storms, communications infrastructure will most likely be compromised. In such cases, it is common to have long-distance communications breakdown, with services only available locally, at the edge of the network. Albeit limited, this is still of extreme importance to local PPDR activities. The mission-critical isolated operation for public safety (MCIOPS), under specification in 3GPP for Rel.17 [9], defines the communications in such scenarios.

Besides the need to provide basic mission-critical communications, the network edge has growing importance for first responders before, during, and after emergency situations. An ever-increasing plethora of devices, like cameras, drones, and all kinds of sensors and actuators, produce huge amounts of data that need to be readily processed, analyzed, and acted upon at very short notice or even under real-time constraints, like providing haptic feedback or augmented reality. Most of these solutions rely on a mix of high bandwidth, low latency, and heavy computing that can only be found together at the network edge, in central offices and remote units, e.g., street cabinets.

Meanwhile, the networks' trend towards softwarization is transforming the network edge, once a complex ecosystem of different network appliances and connections, into something more like a data center, with standard network and computing resources [14]. As seen before, 5G communications provide a flexible and native access to these resources, featuring the need for low latency, high bandwidth, and wider connectivity options. All this is supporting the rise of the edge cloud: an extension of the cloud concepts and services to the edge of the network.

The edge cloud is today a promising work area for consumer, business, and industrial applications. Yet, its potential for domains like PPDR is evident, and many of the special needs that we can associate with public protection and

disaster recovery, namely the mission-critical aspects, are currently being addressed by standards and industry fora.

In the last few years, standards organizations and industry fora have been following this reality. In particular, ETSI multi-access edge computing (MEC) defines an open architecture for *"applications from vendors, service providers, and third-parties across multi-vendor multi-access edge computing platforms"* [15], which set up a reference for the usage of these important edge resources.

In the scope of 5G, for Rel.17, 3GPP is carrying out the studies to include standards specification for edge computing across various service/systems aspects (SA): In particular, the SA6 initiative defines an architecture that enables applications to be hosted on the edge of the 3GPP network, EDGEAPP [16], that frames the aforementioned studies. Another relevant mission-critical aspect of the edge is the IOPS [9], already mentioned.

Network operational models

A next generation mission-critical network, supported on a 5G network, requires the definition of a network operational model to be implemented at a sustainable cost. The adoption of such operational models in each country must precede an evaluation of the models that accomplish the requirements and allow for a business strategy with economic sustainability. This analysis needs to consider different perspectives like (i) spectrum management, (ii) governance model, (iii) technological model, and (iv) cost model.

The spectrum management is performed by regulators, planning spectrum assignments in dedicated or shared mode, to ensure the right balance usage amongst the various communication applications, and increasing spectrum usage efficiency, according to service requirements.

The governance model is used by national authorities to ensure that all functional requirements are accomplished with the levels of quality and safety required by this type of communications, and also to take into account economic, financial, and organizational aspects. The governance model is based on network ownership and control, and three models can be applied:

- **User owned – user operated (UO-UO):** building, ownership, and operation by the user itself;
- **User owned – commercial operation (UO-CO):** building and ownership by the user. Operation by a commercial provider of outsourced management network services;
- **Commercial owned – commercial operation (CO-CO):** user subscribes to services provided by a commercial network operator.

The technological model is used by national authorities and network operators to determine networks and spectrum sharing with public customers' services. There are three technological models applicable:

- **Dedicated network infrastructure:** a dedicated mobile broadband network using dedicated spectrum;
- **Commercial network(s) infrastructure:** PPDR organizations buy MCX services from a commercial mobile network operator, possibly using shared spectrum;
- **Hybrid solutions:** based on dedicated and commercial network infrastructures, it is a shared infrastructure, which can use, or not, dedicated spectrum. In this case, there are three implementation types: i) a geographical split between dedicated and commercial network infrastructure; ii) an MVNO model where organizations share the radio access network (RAN) with the public customers, and; iii) an MVNO model with partly dedicated/partially shared RAN network.

The cost model is used by decision-makers to estimate the total cost of ownership (TCO) of

a mobile cellular radio network over the long term, which includes both the initial costs to build (largely CAPEX) plus the operational costs (OPEX), and can be summarized in the following elements: the cost of the RAN, standing for approximately up to 70% of the total cost, plus the cost of the access network, representing the second-largest share of the total cost, plus the cost of OSS and BSS.

Some studies [2] [17] show a trend where next generation mission-critical networks converge to the following scenarios, relatively to the operational models that can be adopted:

- **Standalone:** an operational model with dedicated network infrastructure, with UO-UO or UO-CO governance models and always using dedicated spectrum;
- **Hosted:** an operational model with commercial network(s) infrastructure, with CO-CO governance model and always using shared spectrum;
- **Sharing:** an operational model with hybrid solutions, with CO-CO governance models and using dedicated and shared spectrum.

Regardless of the scenario adopted for the operational model, three studies ([2], [17], and [18]) make it evident that if the network is not shared among several services, the TCO to provide a single service like PPDR will always be very high. The study from Analysis Mason [18] shows that the dedicated network scenario's adoption has a relative TCO much higher than that of scenarios where commercial networks are used, even with multiple backup commercial networks. **Figure 2** shows this relation. The high-ambition part also depicted includes investment in increased robustness and security compared to traditional commercial networks.

When financial funding may be an issue, the best approach would be to dilute TCO among several services, using one of the following strategies:

- **Specialization strategy:** use of the standalone scenario for sharing the network with other PPDR and CNI customers. CNI customers can

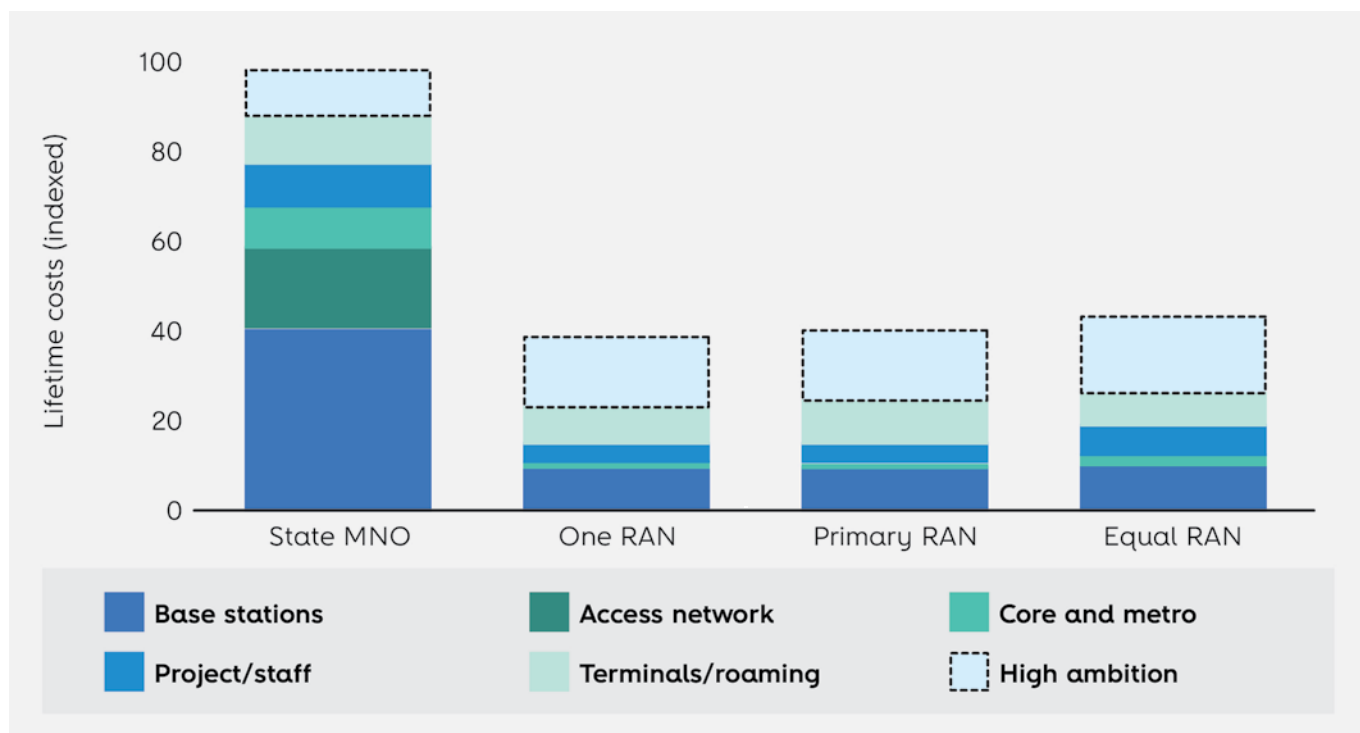


FIGURE 2 – Costs breakdown for next generation emergency networks using commercial mobile networks [18]

be organizations from the utilities sector and/or intelligent transport systems (ITS) sector;

- **Share strategy:** use of hosted or hybrid scenarios for network sharing with public customer's services.

With the specialization strategy, it would be possible to create a specialized and dedicated network for next generation mission-critical communications services at a more affordable cost per customer.

The share strategy, more cost-effective, would allow leveraging 5G networks use cases with the same type of requirements, like autonomous cars, tactile Internet, delivery drones, etc.

However, the best operational model for next generation mission-critical communications networks will depend strongly on specific requirements and the mobile market situation in each specific country. Given the large cost differences identified above, governments and mobile network operators (MNO) need to evaluate and define a strategy to develop a robust and sustainable solution that will serve its ultimate purpose.

MNOs' role for MCX

The adoption of current commercial mobile networks to provide MCX services will lead to a lower cost per transported bit or connected user when compared with the usage of dedicated LTE networks, at a similar frequency band, for the same purpose. However, for that to be possible, MNOs need to deliver extremely high reliable, available, resilient, and secure communications, even in very adverse situations and in locations with less economic return (e.g., less population and industry). Mobile networks supporting MCX services have to guarantee end-to-end availability above 99,999% ("five nines"), from RAN to application servers. Thus, MNOs' geographic coverage and indoor signal penetration at agreed locations must be extended as needed for mission-critical services support. Furthermore, all this network hardening and extended coverage, along with the addition of essential mission-critical functions and resilience, must be accomplished at a reasonable cost. These evolutions may also be

considered business opportunities, leading MNOs to rethink their position relative to the MCX services ecosystem and other use cases that present similar requirements.

The 4G/LTE technology allows several possible alternatives to deploy a public safety LTE network, each with advantages and disadvantages, from a hosted solution to a standalone deployment, passing through various degrees of sharing with commercial networks, as mentioned before.

In the hosted solution, public safety (or MCX) agencies purchase operator services required to meet their mission-critical communications needs, minimizing the need for equipment installation and maintenance. This scenario will be supported by 5G technology, especially when 5G SA networks with slicing features become widely deployed, allowing the implementation of a specific MCX virtual network (or slice) over such commercial networks.

On the other hand, the standalone solution requires the deployment of a full network covering the service area the MCX agency is accountable for. While a dedicated deployment is attractive in terms of MCX agencies being in control of the resources and subscribers database, it comes with operational issues and higher costs to implement and maintain.

In the middle, there are various levels of models of sharing infrastructures with commercial networks: from a full connectivity solution being provided by the commercial network operator and the MCX agency connecting an application server (OTT solution) to only sharing the RAN but having a dedicated core network and service platform. The most significant advantage of these scenarios for MCX agencies is to use from the beginning the wide coverage area already provided by the RAN commercial networks, even though it needs service level agreements to ensure access to commercial network resources in case of emergency and, of course, software package upgrades are needed in the commercial network in order to guarantee mission-critical user experience.

Final remarks

This article addresses possible operators' roles regarding next generation mission-critical communications in the context of 5G and edge computing. It describes 5G main characteristics being incorporated for that purpose. This will be fully reflected in 3GPP Rel-17 specifications, expected in December 2022, making the technology well-positioned for PPDR adoption.

Edge cloud services, leveraging on 5G, pave the way to new, innovative, PPDR services and enable distributed and more resilient services platforms. Without going into much detail, network edge characteristics to support these services, in a resilient way, were presented.

5G is being tailored to be easily deployed by entities other than operators, opening the door for dedicated deployments. However, for PPDR purposes, a careful analysis, considering the presented models, shall take place in order to obtain a suitable critical national infrastructure. Different models to be taken into consideration by decision-makers were described.

In addition to the technological aspect, there are other aspects to be considered for the adoption of 5G by mission-critical communications, such as the operation of PPDR services in a collaborative way even in country border-crossing scenarios. However, until today no concrete guidelines or regulations are available for these.

Altice Portugal already has an extended geographic LTE coverage and is totally committed to continuing to implement standards-compliant network solutions. 5G will be no exception, which will enable the creation of new independent 5G logical networks, tailored to fulfill the diverse requirements of particular applications, like MCX, over the same future Altice Portugal 5G physical infrastructure. 

References

- [1] B. Bhatia, "Status and Trends of Public Protection and Disaster Relief (PPDR) Communications," in *ITU Regional Seminar for CIS and Europe "Development of modern radiocommunication ecosystems"*, 6 to 8 June 2018. ST. PETERSBURG, 2018
- [2] Directorate-General for Communications Networks, Content and Technology (European Commission), SCF Associates Ltd, "Is commercial cellular suitable for mission critical broadband?," 2014. [Online]. Available: <https://op.europa.eu/en/publication-detail/-/publication/246bc6ec-6251-40cb-aab6-748ae316e56d/language-en>
- [3] T-Mobile Network News website, "T-Mobile Launches World's First Nationwide Standalone 5G Network", Aug/20, <https://www.t-mobile.com/news/network/standalone-5g-launch>
- [4] 3GPP, TR 21.916, "Summary of Rel-16 Work Items"
- [5] ITU-R, M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond"
- [6] 3GPP, TR 23.752, "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)"
- [7] 3GPP, TS 37.340, "NR; Multi-connectivity; Overall description; Stage-2"
- [8] 3GPP, TS 38.401, "NG-RAN Architecture description"
- [9] 3GPP, TS 23.180, "Mission critical services support in the Isolated Operation for Public Safety (IOPS) mode of operation"
- [10] 3GPP, TR 38.811, "Study on New Radio (NR) to support non-terrestrial networks"
- [11] 3GPP, TR 23.757, "Study on architectural enhancements for 5G multicast-broadcast services"
- [12] 3GPP, TS 23.434, "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows"
- [13] 3GPP, TS 23.222, "Common API Framework for 3GPP Northbound APIs"
- [14] Broadband Forum, TR-384, "Cloud Central Office Reference Architectural Framework", 2018
- [15] ETSI, "Multi-access Edge Computing (MEC)," ETSI, 2020. [Online]. Available: <https://www.etsi.org/technologies/multi-access-edge-computing>
- [16] 3GPP, TS 23.558 - V0.4.0, "Architecture for enabling Edge Applications",
- [17] "PPDR-TC White Paper - The Strategic Roadmap for Next Generation (Broadband) PPDR Communication Systems", PPDR-TC, 2016
- [18] Harald Wium and Lie Amund Kvalbein, "Four different models for next generation emergency networks using commercial mobile technologies", Analysis Mason, 2018. [Online]. Available: <https://www.analysis.com/about-us/news/newsletter/next-generation-emergency-networks-jul18/>



10

Redesigning the network edge for a new era

André Domingos Brízido, Altice Labs

andre-d-brizado@alticelabs.com

Gonçalo Nuno Gaspar, Altice Labs

goncalo-n-gaspar@alticelabs.com

Miguel Santos, Altice Labs

miguel-c-santos@alticelabs.com

Rui Calé, Altice Labs

cale@alticelabs.com

Vitor Mirones, Altice Labs

mirones@alticelabs.com

A set of new concepts and technologies have emerged in recent years that helped the push for digitalization and automation of networks and enabled Service Providers to a faster transition to that next generation digital paradigm. The definition of a common and aligned architecture for the network edge will allow us to steer our portfolio towards solutions that match not only many challenges presented to us today, but also those raised by new, unexpected realities brought up by an increasingly unstable world.

Keywords

Cloud central office; CO Infrastructure; PON access;
Mobile access; Edge; MEC; 5G small cell

Introduction

Society, as we are experiencing it today, is the result of the major impacts produced by a new worldwide COVID-19 pandemic. The health crisis led to big changes in the way we relate to each other at both personal and professional levels, where the once common close proximity between people was replaced by social distancing and remote interactions. This new way of life also promoted a huge move of work locations since a significant number of people switched their workplace in a couple of days and started to work from home. As a result, there was a big shift in the point of access distribution in the telecom operators' network, together with a steep increase in the overall data traffic. It is expected that these types of changes may happen more often. Hence, the operators need to have an agile network infrastructure that can quickly be adjusted to cope with these needs and the ever-increasing demand for new services while assuring the reliability and resilience required so that businesses can perform and prosper in this "new normal", much more dependent on digital.

With the emergence of more digital services, there was also the need for higher broadband demands, both in latency and throughput. These requirements led to the study of a new geographical distribution of the services, moving them closer to the user and thus paving the way for the re-architecture of the central office (smaller data-centers that are closer to the user and the termination of the access network). As an important player in this ecosystem, Altice Labs has been targeting these moves and since last year has been working on the definition of its approach to what it foresees as the new cloud central office (CCO). The work introduced in the 2018 edition of InnovAction [1] has evolved, resulting in a more complete architectural view, presented in this article.

These changes are also on the radar of the telecommunications community and Broadband Forum (BBF), a leading standards development

organization (SDO) for the fixed broadband. In the last couple of years, BBF started working to address the new CCO and is currently specifying an architecture that gives support to the more agile and automated network infrastructure and services. In this central office, a new degree of flexibility will allow the mapping of services to the corresponding resources using as a basis a set of YANG-based common management models that will enable better and faster deployment of automated processes to manage these next-generation networks.

A set of new concepts and technologies have emerged in recent years that helped the push for digitalization of the networks and enabled service providers to a faster transition to that next generation digital service provider paradigm where network agility and automation are essential, namely: network virtualization, software-defined networks (SDN), and network functions disaggregation.

This article will explore the work Altice Labs is doing towards the automation of the service provider network, with a special focus on the CCO, where a significant part of the network infrastructure resides. It starts by providing an overview of the new CCO architecture as foreseen by Altice Labs. Next, the main processes that allow an automation of the CCO are explained, followed by some use-cases that illustrate the previously described processes. Finally, a summary of the main findings is presented in the conclusions section.

Cloud central office architecture

As mentioned before, the central office is experiencing a significant change in its architecture. More than speaking about evolution, we should more appropriately be speaking about a true revolution because most of the fundamentals of the new CCO sever the ties to the old legacy approach and create a completely

renovated environment where the old monolithic and rigid functions are replaced by a dynamic, integrated and automated virtualized functions ecosystem.

Altice Labs' vision for the new CCO, presented in this section, is based on the work being conducted by the BBF regarding the CCO architecture.

BBF reference architecture

The BBF, as previously referred, is the reference SDO for the fixed access domain. In 2018 it published the TR-384 - Cloud Central Office

Reference Architectural Framework [2] with the purpose of defining the architecture for the next generation central offices, leveraging the agility of SDN, network function virtualization (NFV), and cloud technologies. This architecture has already been described in the abovementioned 2018 InnovAction article [1].

Since the publication of TR-384, the CCO architecture is being revised in WT-411 - Definition of interfaces between CloudCO Functional Modules, yet to be published. **Figure 1** summarizes the CCO architecture.

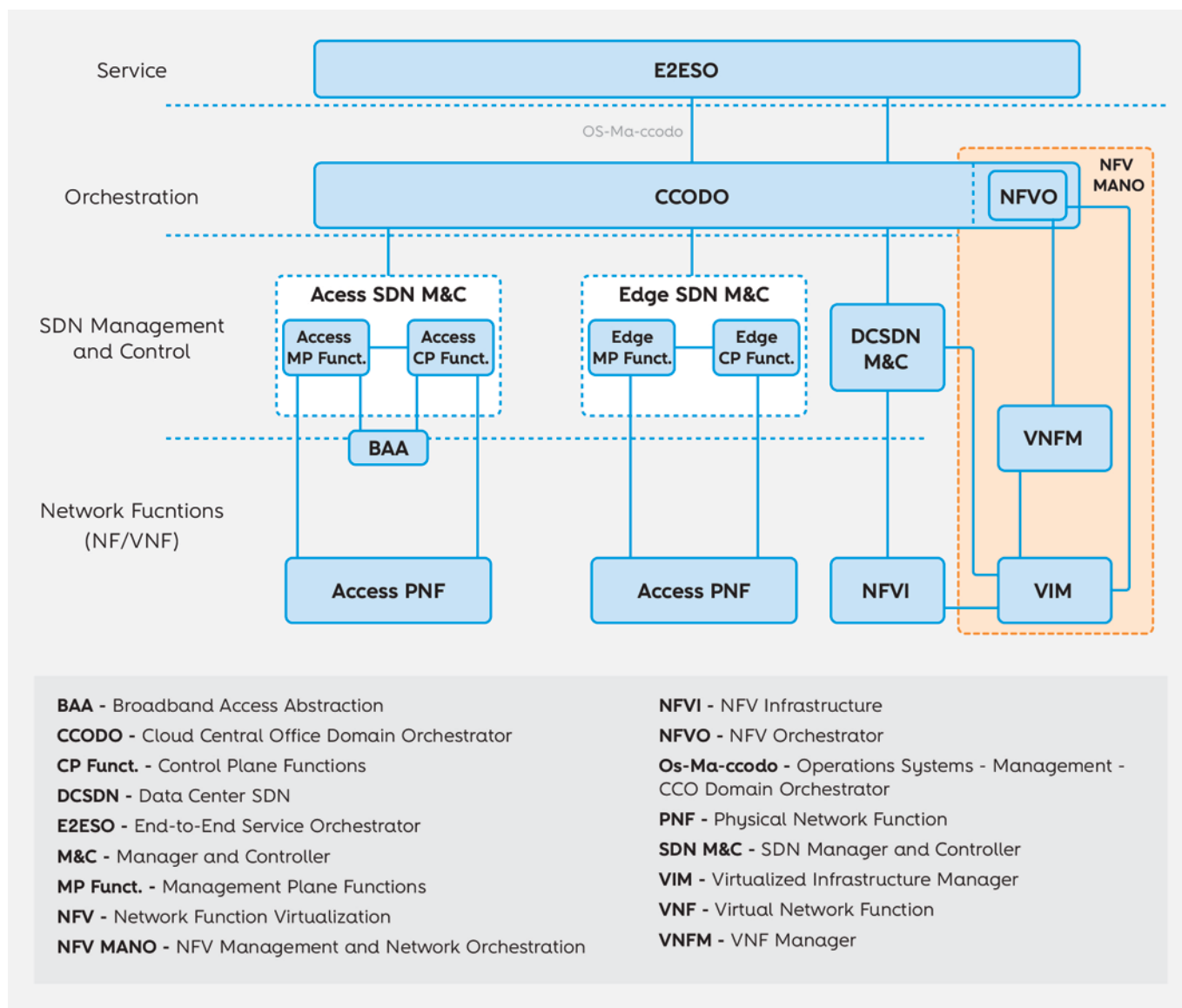


FIGURE 1 – BBF reference CCO architecture

There is a clear separation of the access segment, the edge segment, and the NFV infrastructure (NFVI). Each segment has an SDN Manager & Controller (SDN M&C) not only responsible for delivering traditional fault, configuration, accounting, performance, and security (FCAPS) functionality (the MP Funct. block in **Figure 1**) but also for providing disaggregated control plane functionalities (the CP Funct. block in **Figure 1**).

The CCO domain orchestrator (CCODO) role is to orchestrate all the network segments and provide a high-level view of the CCO network. The latest is provided through a northbound (NB) API that abstracts the CCO network without the need to expose the internal CCO architecture components, allowing the use of a network-as-a-service (NaaS) paradigm. To complement this work, a set of TM Forum API have been identified by the BBF to be used on the operations systems-management-CCO domain orchestrator (Os-Ma-ccodo) reference point, including the service inventory, service catalog, and service fulfillment API. The NB API exposed by the CCODO makes use of a dynamic data model that is provided to different actors: the service consumer, the service developer, and the service provider.

The end-to-end service orchestrator (E2ESO) provides the E2E view of the operator network and coordinates multiple CCODO as well as the wide-area SDN controller and orchestrator that connects the different CCO domains.

The access segment has no user plane Virtual Network Function (VNF) because it concerns the access nodes (e.g., optical line terminations - OLT, distribution point units - DPU), which connect the end customer to the operator network. In the access segment there is also the broadband access abstraction (BAA) layer, which provides a standardized NB API for all access nodes, including legacy nodes.

The edge segment is the place of the broadband network gateway (BNG). TR-459 [3] defines an architecture and requirements of a disaggregated BNG (DBNG) leveraging control and user plane separation (CUPS) and virtualization principles. A

DBNG can have a single control plane instance controlling multiple data plane instances. The control plane and data plane instances can be either virtual or physical and can be scaled independently.

Currently, one of the main goals of the SDN/NFV work area of the BBF is to define all the interfaces between the CCO components. Many of these interfaces rely on NETCONF/RESTCONF [4][5] and YANG for modeling, so in the last few years, a great amount of work has been done by the BBF in publishing standardized YANG data models [6].

Another goal of the SDN/NFV work area is to identify and disaggregate the functionalities of the access nodes so that they can be implemented outside of the access node and increase flexibility. The BAA layer is a good candidate to absorb these functionalities.

An example of such a disaggregated function is the virtual ONT management control interface (vOMCI). . A reference implementation of the vOMCI specification is currently in progress in the open broadband - broadband access abstraction (OB-BAA) open-source project. The OB-BAA project is the Broadband Forum's reference implementation of the BAA layer, and Altice Labs is actively contributing to it.

Altice Labs' reference architecture

Altice Labs has been closely monitoring the work of the BBF and defined its own and aligned view of the, and, more generally, to the edge of the operator's network, setting up the scenario for the evolution of its own portfolio. In this view, various access networks converge and benefit from co-location and from the softwarization of their functions to enable truly convergent approaches [7]. Edge network functions, like the BNG for fixed networks or the user plane function (UPF) for 5G, also relate and coexist, share services, and

reorganize into convergence supporting functions, like the access gateway function (AGF) or the fixed-mobile interworking function (FMIF). Edge computing is also supported to enable other functions, eventually from other providers or clients themselves, to be supported on the networks' edge.

Figure 2 shows a very high-level view of the reference architecture defined by Altice Labs. Aligned with the BBF approach, it features several technical domains or segments: access segment, corresponding to the termination of the various access networks, edge segment for network edge functions, multi-access edge computing (MEC) segment for edge cloud, and data a

center infrastructural segment comprising NFVI, management and network orchestration (MANO), and data center SDN Manager & Controller (M&C). For each of these segments, there is an M&C plane specific to the segment to expose to the CCODO the interfaces that will allow it to manage and coordinate all the processes across the CCO. Above the CCODO, an E2ESO will coordinate the activities necessary to provide and maintain services across the various networks and platforms.

The major principles that drive this architecture are evident in **Figure 2** representation. Horizontally, there is a clear and fundamental separation between the user plane and the control plane to

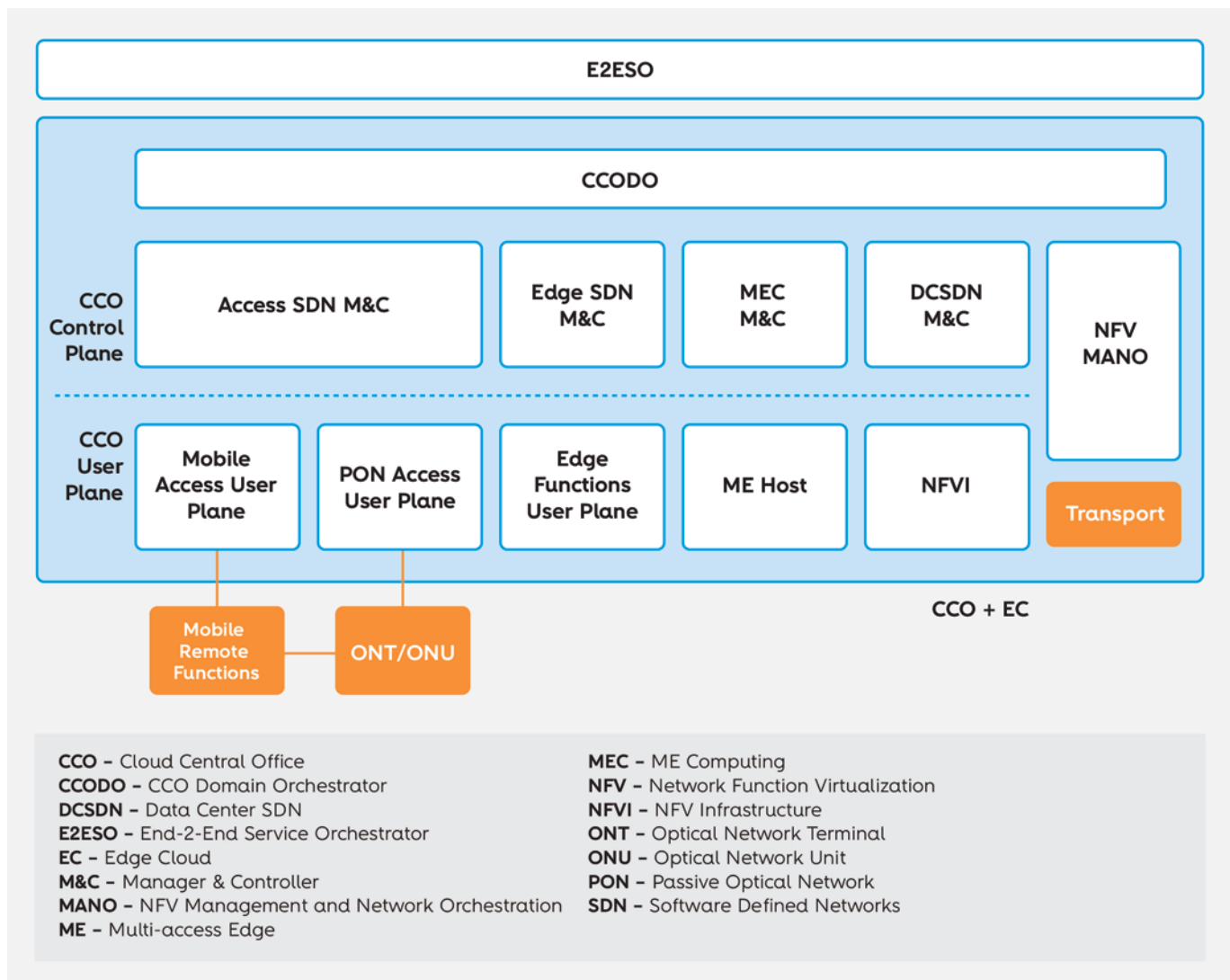


FIGURE 2 – Altice Labs' network edge reference architecture - high-level view

guarantee the CUPS advantages [8]. Vertically, there are apparent silos in the approach. These correspond to internal technical domains under common orchestration and whose control mechanisms can be shared across domains, enforcing the SDN principle of centralized control.

PON access

Altice Labs' architecture for the passive optical network (PON) access network is depicted in **Figure 3**.

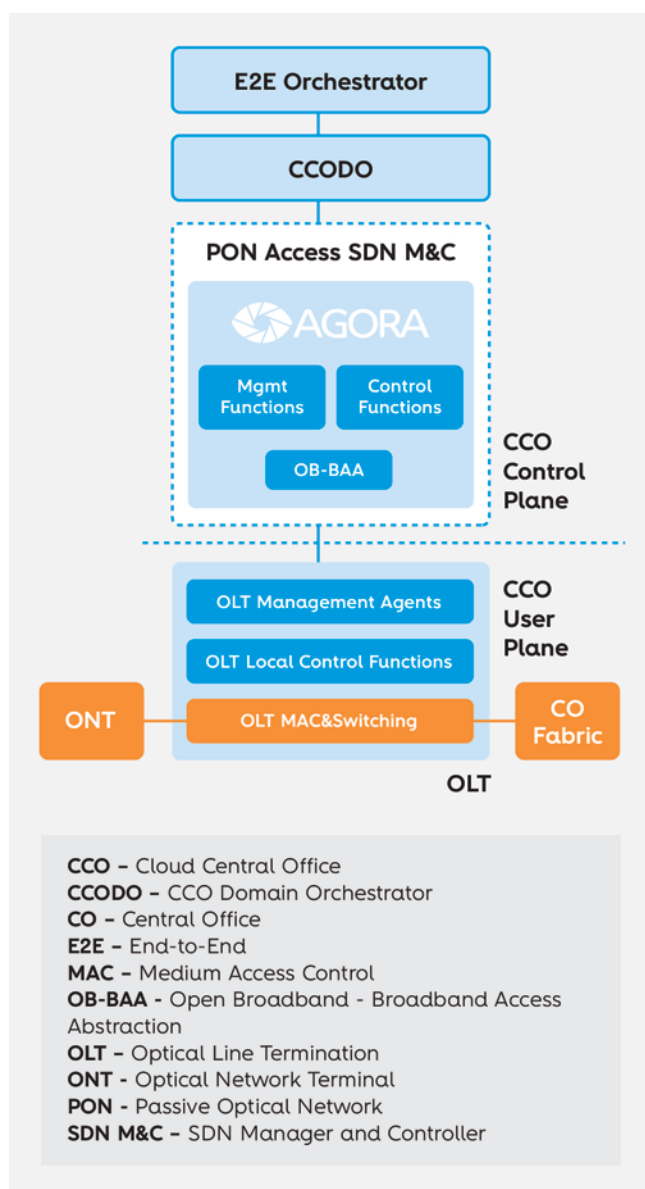


FIGURE 3 – Altice Labs' architecture for the PON access network

As mentioned previously, this architecture is aligned with BBF's CCO architecture. It includes the evolution of Altice Labs' AGORA management solution [9] into an access SDN manager and controller with the possibility of running control plane functions separated from the devices.

One important aspect for operators is the availability of a smooth migration path given the large number of OLT already deployed in their current networks. In Altice Labs' architecture, some management and control plane functions can still remain within the devices, while new added value disaggregated functions can be progressively deployed in the NFVI and therefore increasing the network agility. One example of such functions is virtual ONU management control interface (vOMCI), which allows deploying new types of ONT without having to upgrade the entire OLT software. The OB-BAA component has an important role in providing such disaggregated functions as well as providing an adaptation function to third party and legacy access nodes.

Other important aspects for operators are network programmability and automation, which are enabled by using open interfaces based on the NETCONF or RESTCONF protocol and standardized YANG data models.

Mobile access

Figure 4 illustrates the structure of mobile access within the CCO architecture. It represents the various hauling options (front-haul, mid-haul, and back-haul). In Altice Labs' reference architecture, these options are covered by a PON. Among the various function splitting possibilities considered for the access, the option chosen for implementation by Altice Labs is named "front-haul x", using PON for transport between DU-L and DU-H (third option in **Figure 4**).

Function placement in the CCO will depend on the splitting option, but, in general, the management of these functions is the responsibility of the mobile access manager (MA-M).

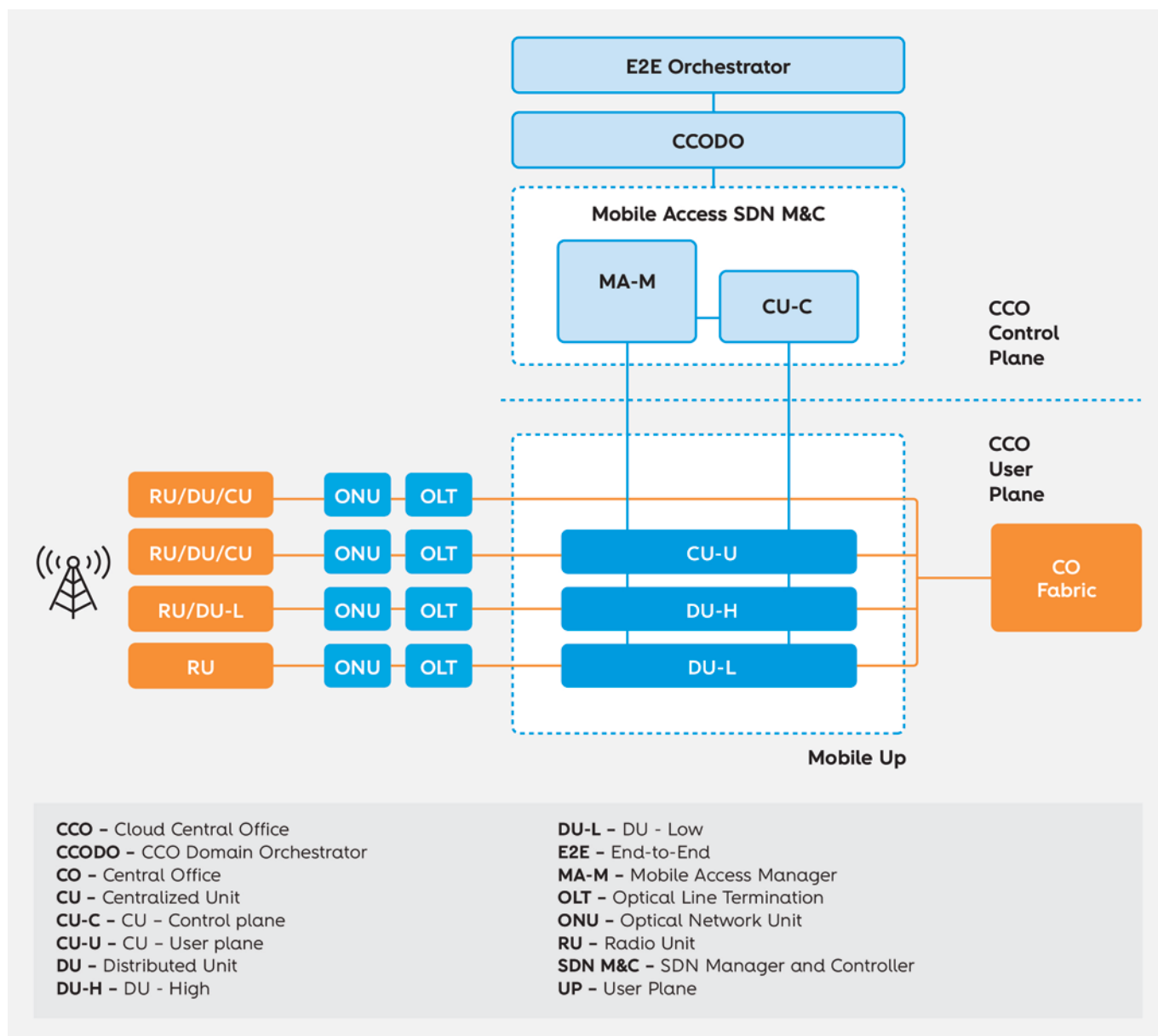


FIGURE 4 – Mobile access segment

The Radio unit (RU) and distributed unit (DU) are, basically, real-time user plane functions, but the centralized unit (CU), less constrained by time, has a separated control plane implementation (CU-C).

Edge

Another CCO segment of major interest for Altice Labs is the edge, depicted in **Figure 5**. In this segment of the architecture, we can find the

various service gateways that can be employed in the context of the fixed and converged network, namely the BNG, AGF, and FMIF. According to Altice Labs' vision, in a full wireless and wireline convergence, we should also consider in this segment the 5G user plane function (UPF). The edge provides the interconnection of the access network with the transport and services networks, and also the control of the data sessions that cross its user plane ("edge" is a somewhat overloaded term. In this article, it refers to the network edge, as defined above).

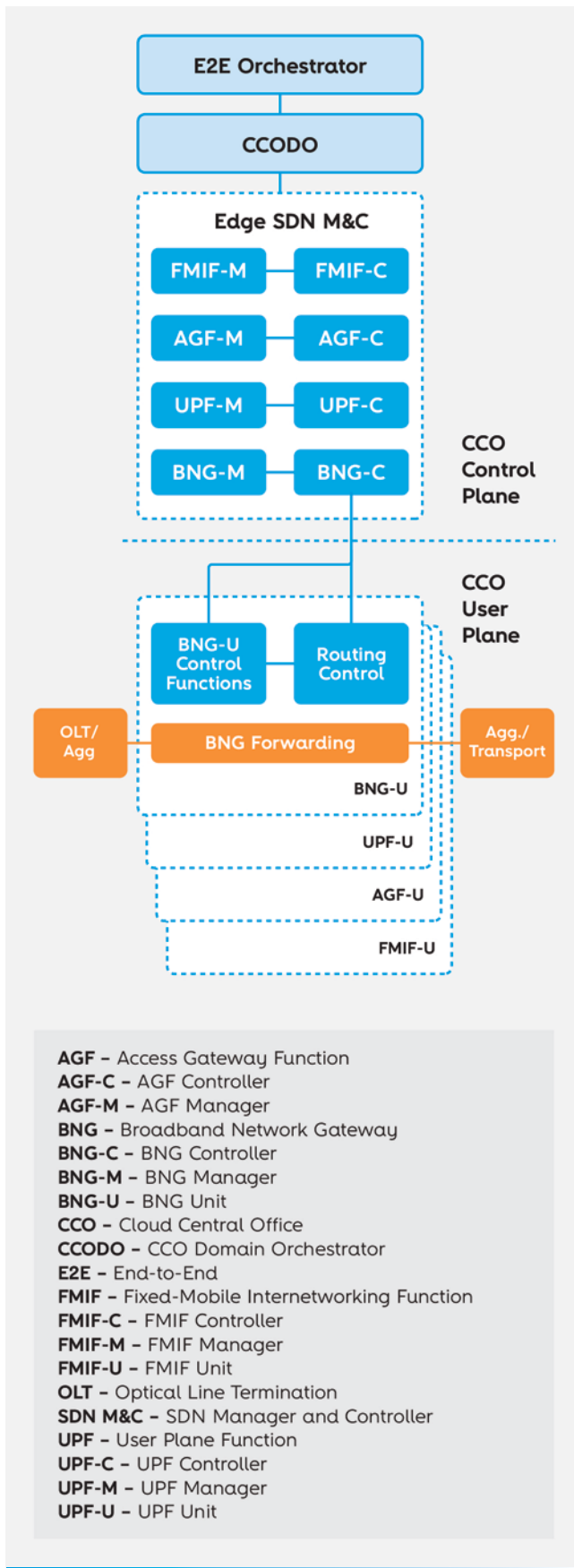


FIGURE 5 – Edge segment

Following the chief principles that guide the CCO, the functions that are part of the edge must be fully virtualized and implement a control and user plane separation where the different user planes are managed by their respective control plane.

The functions in this segment are to be part of a larger integrated solution, first in the CCO domain and afterward in the E2E service delivery. So, the CCODO must be integrated with the control plane of the edge segment to manage the lifecycle of the different functions in an integrated way, thus providing the needed automation of these cloud network functions.

To allow the automated management by the CCODO, the control plane that manages these functions exposes a set of API that enable the creation, configuration, monitoring, scaling, update, and removal of each function.

MEC

Multi-access edge computing (MEC), defined by ETSI MEC ISG [10], is a layered, hierarchical architecture that represents the extension of the central/public clouds to the network edge, closer to end-users. It provides a heterogeneous application ecosystem, created to be explored via partnerships and an ever-growing applications market.

MEC provides a set of API to support the development of edge applications and is integrated with CCODO (e.g., for traffic steering, prioritization, and function lifecycle management). Besides this integration, MEC will have its own orchestration, managing the delivery of services/applications to the network edge.

Altice Labs' reference architecture uses the MEC architecture [11] as its reference. **Figure 6** illustrates at a very high level how this alignment is guaranteed.

In a virtualized user plane, mobile edge platforms (MEP) run on mobile edge hosts, most likely collocated with the CCO, at the access, or even in customer premises. A mobile edge platform

manager & controller (MEP/MEPM) will take care of managing these applications. The eventual MEC orchestration, bearing the orchestration aspects specific to the edge cloud, is not represented in **Figure 6**.

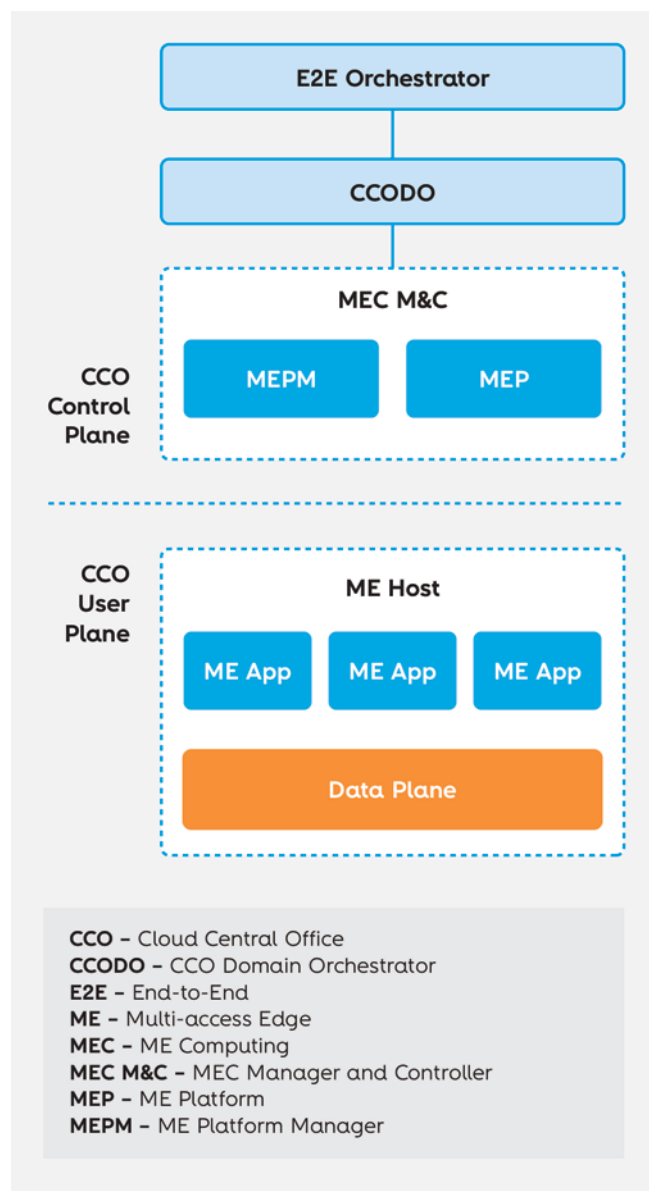


FIGURE 6 – MEC segment

CO infrastructure

To virtualize network functions, the CCO has to offer all the necessary mechanisms to run those functions on a set of switches, servers and some specific hardware that make the NFVI.

In this view, those mechanisms have two major components: NFV MANO, which controls the lifecycle of all VNF, according to the standard defined by ETSI NFV ISG [12], and the data center SDN M&C (DCSDN M&C), that takes care of all network aggregation and routing control that occurs at the CCO and is not directly related to the lifecycle of network functions and network services. These two components are orchestrated by the CCODO via their standard interfaces. The CCODO orchestrates the NFV MANO sub-system via interfaces standardized by ETSI [13] and the DCSDN M&C component via interfaces under standardization by the BBF SDN/NFV WorkGroup [14]. **Figure 7** illustrates this part of the architecture.

In this approach, one aspect remains unclear: The ETSI NFV Industry Standards Group went to considerable lengths to fully standardize an architecture for the virtualization of Network Functions, where it is implicit that these functions process user data packets (user plane), and hence needs a particular set of capabilities for combining/chaining them into network services. This leads to a complex architecture that includes a set of constraints that limits its flexibility. Here we take an approach where it is assumed that UP and CP are separated *a priori*, and thus it is fair to question whether a “pure” standard NFV environment is the most adequate for the CO infrastructure. Actually, the lifecycle of the functions described for the SDN M&C areas in the sections above can (and probably will) be managed using simpler, more IT-centered solutions, that do not need to deal with the complexities and restrictions of the UP virtualization. These mechanisms will take their place in the DCSDN M&C (see **Figure 7**) and will be subject to CCODO orchestration, using the interfaces that they make available.

Orchestration

The orchestration is separated into two different layers, the E2E layer and domain-specific layers, so that the inherent complexity of each domain or sub-domain can be abstracted. This contributes to the overall capacity of the E2E orchestrator to

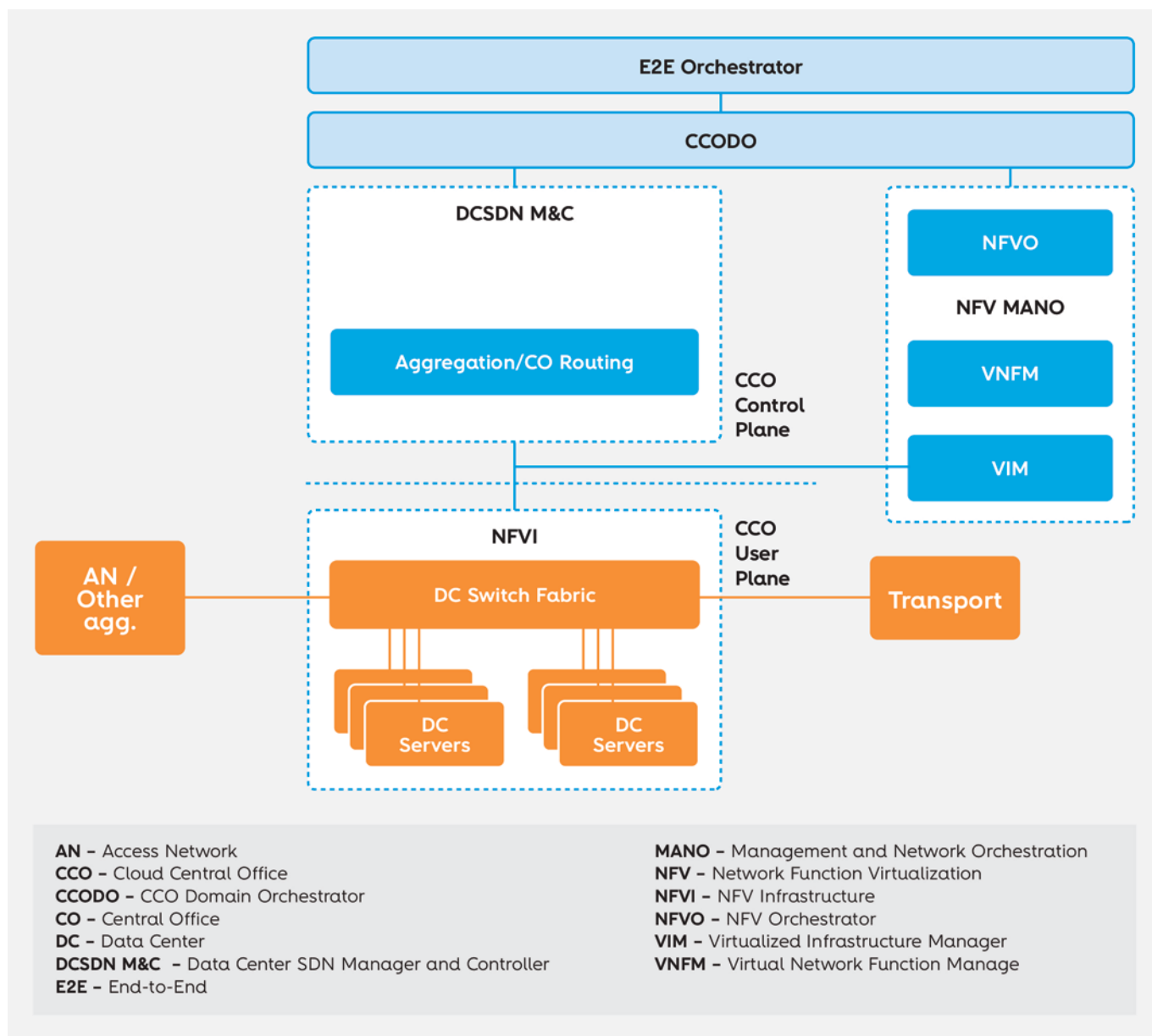


FIGURE 7 – Infrastructure segment

coordinate the different domains, CCO or other, in a simpler way. **Figure 8** depicts this layering.

The CCODO NB API will be composed of a set of TM Forum API that will allow access to the services and resources provided by the CCO domain. The services will be modeled as technical services [15] and the resources as physical, logical, or as resource functions in the case of virtual resources.

Through this set of API, a service design application will be able to model the set of services it needs for a specific CCO domain and

onboard them. The modeled services can then be managed by a service provider, and, after instantiated, consumed and configured to the customers' needs. This is one of the key aspects because the entities available in the CCO domain are tailored to each of the needs of every role, allowing it to be adapted to the network evolution or the network/service provider requirements.

The NFVO standard interface functionality will be provided by the CCODO NB API, and the CCODO will be responsible for all the interactions with the NFVO.

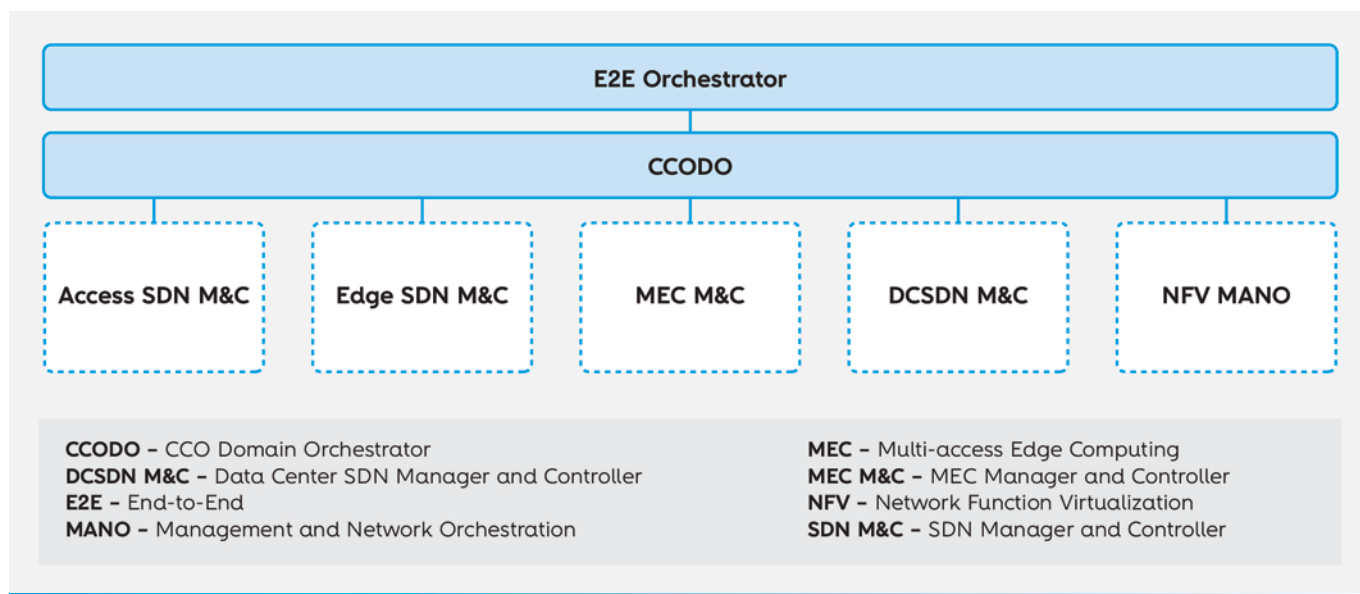


FIGURE 8 – Orchestration

Having only one orchestrator for the CCO domain is advantageous as it avoids the need for coordination over shared resources.

Use cases

In the present COVID-19 scenario, along with the physical relocation of people from their workplaces, offices, or schools to their homes comes the need to provide them with a reliable and secure connection so that they can perform their activities remotely. This implies an adaptation on both mobile and fixed network access for this new traffic demand to be handled properly.

Next, we present a small set of use cases that highlight the capacity of the CCO management to adapt to this new reality.

New 5G RAN small cell

In a 5G network scenario, a need for a new cell is detected, following a high network demand. To provide that, a request is issued to the E2E orchestrator to deploy a new 5G radio access network (RAN) small cell. After the new RU is installed, the E2E orchestrator is notified. It

updates its internal inventory and issues requests to the CCODO so that the 5G RAN is configured accordingly, and a new ONT is provisioned for front-haul-x. The CCODO instantiates a new DU VNF, configures it in an existing CU, and provisions the ONT.

After the 5G RAN is configured, the E2E orchestrator configures the 5G core so that this new cell becomes available. This way, the high demand can be split into more than one cell.

New OLT

A new PON is needed at a central office where all the OLT are at full capacity, so a new OLT is necessary. After the physical equipment is deployed manually by a field technician, the OLT obtains connectivity configuration through DHCP and contacts its access SDN M&C. This triggers the provisioning process in the access SDN M&C, which applies the initial configuration. Then, the E2E orchestrator is notified, and it requests the CCODO to instantiate the new OLT on the CCO. The OLT is registered in the internal inventory, and the required VNF are instantiated, if needed, and configured, both the ones internal to the virtual OLT (vOLT) and the virtual BNG (vBNG) that handles the L3 protocols.

These functions, and the network service they provided, are validated automatically by the orchestrator after a successful deployment.


New MEC application

The network operator creates a new service (e.g., e-health), which requires an application to have a permanent connection to a set of user equipment (UE) and low latency to guarantee minimum delay in the analysis of the data sent by the UE. After this service is designed and onboarded by the E2E orchestrator, it will be available for deployment on the MEC M&C using the CCODO interface. When a subscriber acquires the service, the E2E orchestrator provisioning interface is triggered. It contacts the CCODO to ensure that the new MEC application is deployed in the MEC host closest to the subscriber.

This allows data to be sharply monitored while offloading central servers and core communications.

Conclusions

The content in this article results from a joint work involving multiple Altice Labs' business areas in defining a common architectural view for the edge of the network. The proposed architecture is leveraged by the progress of network technologies and approaches like NFV, SDN, and function disaggregation, in the scope of 5G, fixed broadband (and convergence thereof), and the support to edge cloud. This progress will allow the designing of an ecosystem capable of supporting not only an operators' network functions and communications services but also the verticals that make use of it, and their services and applications, hence brought closer to the end-user.

The definition of a common and aligned architecture for the network edge will allow Altice Labs to steer its portfolio towards solutions that match not only many challenges presented to us today, but also those raised by new, unexpected realities brought up by an increasingly unstable world. 

References

- [1] R. Calé, A. Brízido, and M. Santos, "The digital transformation of the central office," *InnovAction* #3, vol. 1, no. 3, pp. 158–171, 2018.
- [2] Broadband Forum, "TR-384 - Cloud Central Office (CloudCO) Reference Architectural Framework," 2018. [Online]. Available: <https://www.broadband-forum.org/technical/download/TR-384.pdf>.
- [3] Broadband Forum, "TR-459 - Control and User Plane Separation for a disaggregated BNG," no. June, pp. 1–102, 2020.
- [4] IETF, "Network Configuration Protocol (NETCONF)," IETF, 2011. [Online]. Available: <https://tools.ietf.org/html/rfc6241>.
- [5] IETF, "RESTCONF Protocol," *IETF*, 2017. [Online]. Available: <https://tools.ietf.org/html/rfc8040>.
- [6] Broadband Forum, "Broadband Forum YANG Modules," *GitHub*, 2020. [Online]. Available: <https://github.com/BroadbandForum/yang>.

- [7] Broadband Forum, "TR-470 - 5G Wireless Wireline Convergence Architecture," no. August, pp. 1-77, 2020.
- [8] 3GPP, "TS 23.214 - Architecture enhancements for control and user plane separation of EPC nodes," 3GPP, 2020. [Online]. Available: <https://itectec.com/archive/3gpp-specification-ts-23-214/>.
- [9] Altice Labs, "AGORA Network Management System," 2020. [Online]. Available: <https://www.alticelabs.com/site/gpon-solutions/network-management-system/>.
- [10] ETSI, "INDUSTRY SPECIFICATION GROUP (ISG) ON MULTI-ACCESS EDGE COMPUTING (MEC)." [Online]. Available: <https://www.etsi.org/committee/mec>.
- [11] ETSI, "GS MEC 003 - V2.1.1 - Multi-access Edge Computing (MEC); Framework and Reference Architecture," vol. 1, pp. 1-21, 2019.
- [12] ETSI, "INDUSTRY SPECIFICATION GROUP (ISG) NETWORK FUNCTIONS VIRTUALISATION (NFV)." [Online]. Available: <https://www.etsi.org/committee/nfv>.
- [13] ETSI, "GS NFV-IFA 013 V2.1.1 - Network Functions Virtualisation (NFV); Os-Ma-Nfvo reference point -," vol. 1, pp. 1-127, 2016.
- [14] Broadband Forum, "TR-413 - SDN Management and Control Interfaces for CloudCO," no. December, pp. 1-33, 2018.
- [15] J. Reilly, "Unravelling the enigma of resource-facing service," *TM Forum*, 2015. [Online]. Available: <https://inform.tmforum.org/features-and-analysis/2015/12/unravelling-the-enigma-of-resource-facing-service/>.



11

Towards autonomous private 5G networks

Catarina Mónica, Altice Labs

catarina-s-monica@alticelabs.com

Dulce Teles, Altice Labs

dulce@alticelabs.com

Paulo Ferro, Altice Labs

paulo-j-ferro@alticelabs.com

Pedro Antero Carvalhido, Altice Labs

pedro-a-carvalhido@alticelabs.com

In the era of 5G and IoT, operators need to evolve to a model in which the network, and its capacity, is centrally programmable. This pandemic 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. Thus, operators will need to redefine and reshape network operations' solutions.

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.

Keywords

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

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.

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].

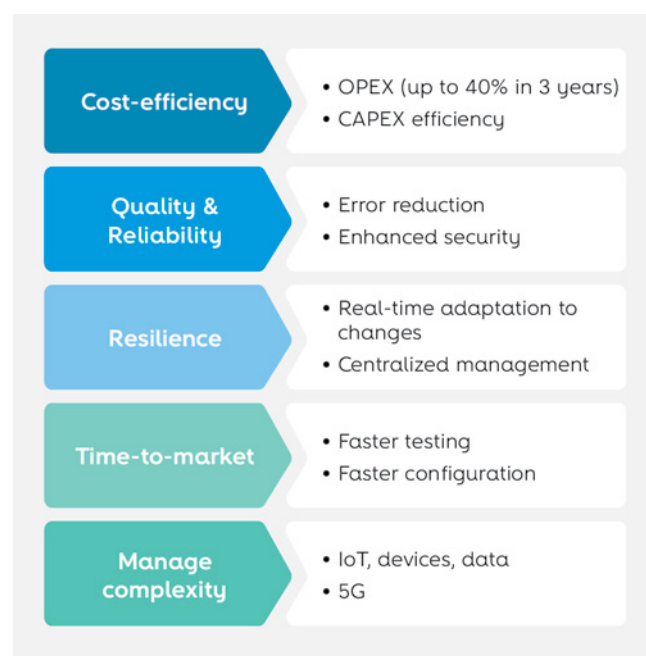


FIGURE 1 – Automation benefits according to MIT research

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.

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.

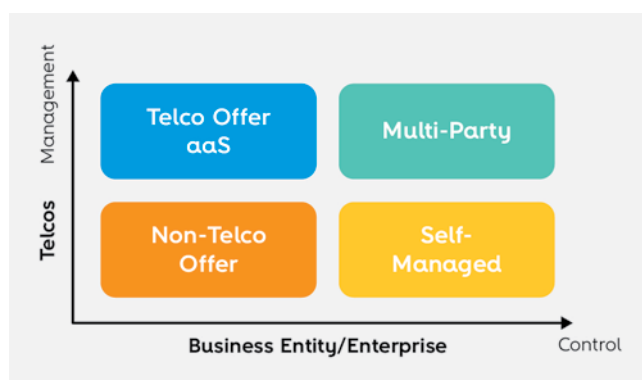


FIGURE 2 – Private 5G mobile business management models

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**.

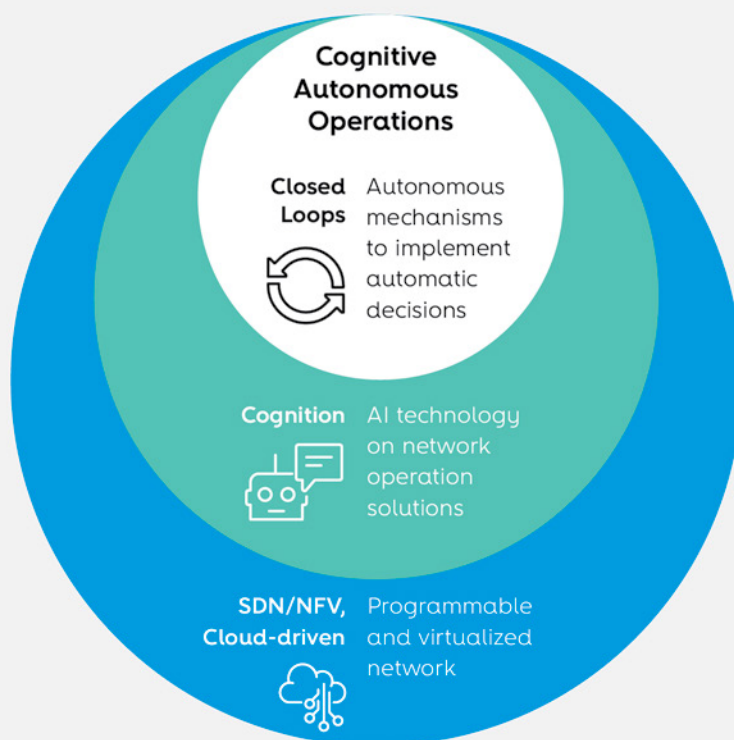


FIGURE 3 – Cognitive autonomous operations – high-level logical view

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 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.

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

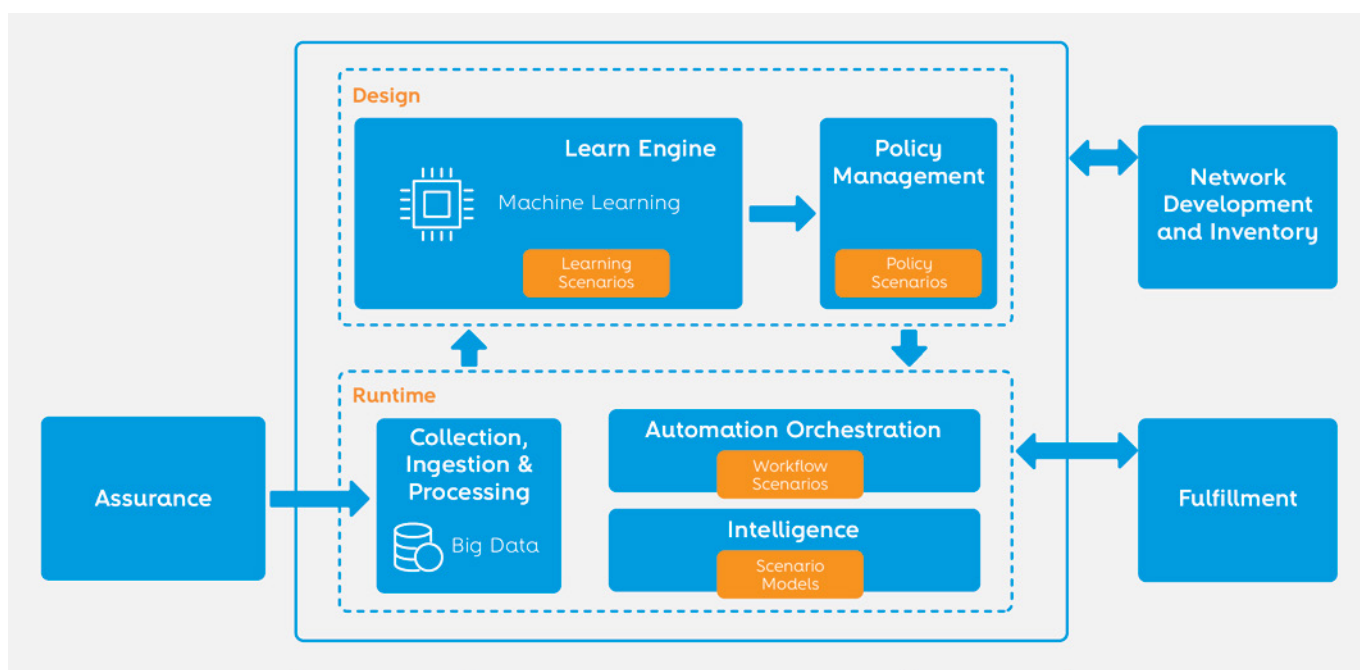


FIGURE 4 – The autonomous operation architecture

(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**.

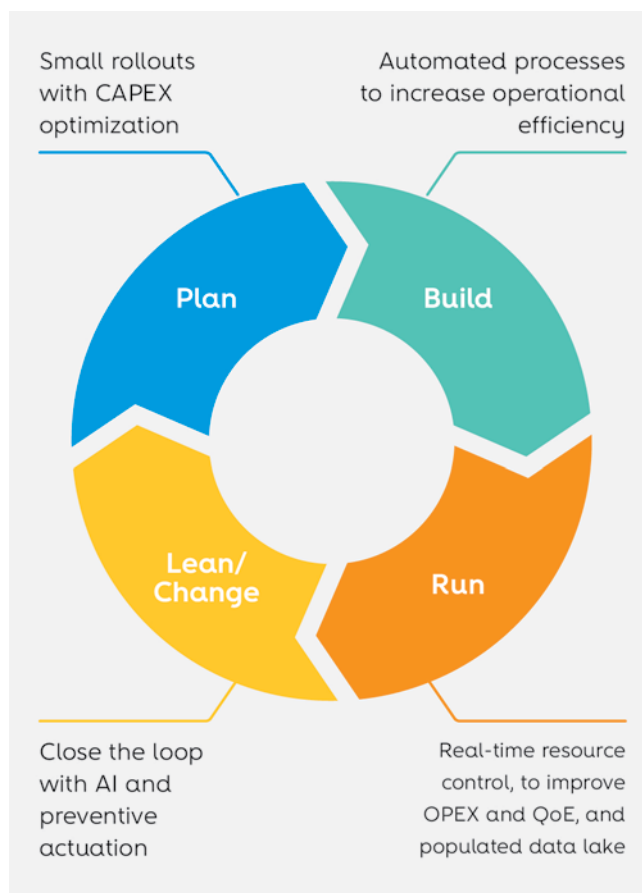


FIGURE 5 – An iterative approach to achieve network autonomy

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.

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>



12

5G radio units towards
virtualized RAN

Samuel Rocha Madail, Altice Labs

samuel-r-madail@alticelabs.com

Joaquim Miguel Silva, Altice Labs

joaquim-miguel-silva@alticelabs.com

Victor Marques, Altice Labs

victor-m-marques@alticelabs.com

Hugo Filipe da Silva Reboredo, Altice Labs

hugo-f-reboredo@alticelabs.com

José Salgado, Altice Labs

jsalgado@alticelabs.com

**Arnaldo Oliveira, Instituto das Telecomunicações,
Aveiro**

arnaldo.oliveira@ua.pt

Keywords

Open RAN; Function disaggregation; Interface standardization;
Open interfaces; 5Growth

Introduction

The next decade is expected to be profoundly impacted by 5G. By the end of 2020, more than one-fifth of the world's countries will have launched 5G services – particularly, in Europe, the expected 5G penetration should reach 30% by 2025 [1]. Mobile communications are foreseen as the enablers for a new industrial revolution. Thus, as the global pacesetter for convergence of all connected technologies bringing this technology transformation to fruition economically and efficiently.

It has become clear that 5G technology deployment must use a combination of the low and high-frequency spectrum, requiring a much higher degree of cell densification (primarily achieved via small cells and distributed antenna systems deployment) to guarantee the desired quality of service (QoS). Furthermore, the COVID-19 pandemic brought numerous challenges and uncertainties to the telecom industry, including geopolitical stress escalation and additional 5G deployment challenges. This pandemic leads to an unprecedented disruption, transitioning millions of workers to home-based offices and students to online classrooms while increasing the demand for video, collaboration, and entertainment services. Furthermore, trade war, exacerbated by COVID-19, is restricting the number of vendors available to deploy 5G and creating additional pressure and uncertainty in operators, increasing the lock-in feeling and hindering innovation.

To better deal with these challenges, an open radio ecosystem is required in order to promote transition between proprietary “end-to-end” solutions to an open market of “best-of-breed” system designs offered by numerous vendors, and giving flexibility in network deployment, upgrade, and swap. This would allow to reduce solution cost and contribute, for example, to provide broadband access in remote zones, otherwise non-existent, while providing social inclusion, well-being, and technological integration, particularly important in confinement times.

With such challenges in mind, the design evolution from LTE to 5G new radio (NR), where the original baseband unit (BBU) functions are distributed between three different elements – a centralized unit (CU), a distributed unit (DU), and a radio unit (RU) – will enable the adoption of the necessary technological enablers such as open and standardized interfaces, network functions virtualization and software-based implementations. This approach will facilitate the cloudification of radio access networks (cRAN), allowing resource centralization while better promoting radio access networks virtualization (vRAN), enabling the use of commercial off-the-shelf (COTS) hardware, and also pave the way for decreased fronthaul line rates while meeting latency demands.

Concept of open RAN

The radio access network (RAN), as defined by 3GPP, is already open when it comes to the air interface and the interfaces toward the core network, which are well standardized, enabling devices and nodes from different vendors to interoperate. However, RAN within itself is closed, and markets today are dominated by a small number of incumbent vendors. In a bid to generate more competition and increased vendor diversity, some mobile network operators (MNO) support the concept of an open RAN, to create a more competitive market with more rapid innovation cycles in which proprietary RAN technologies are replaced by open standard alternatives, and disaggregating the base station architecture and its functional components.

Open RAN can be understood as “*the ability to integrate, deploy, and operate RANs using components, subsystems, and software sourced from multiple suppliers, connected over open interfaces*” [2]. O-RAN Alliance refers that “*future RANs will be built on a foundation of standardized interfaces, virtualized network*

elements, white-box hardware that fully embrace the core principles of intelligence and openness” [3]. In the next sections, these three key initiatives will be better explored and explained.

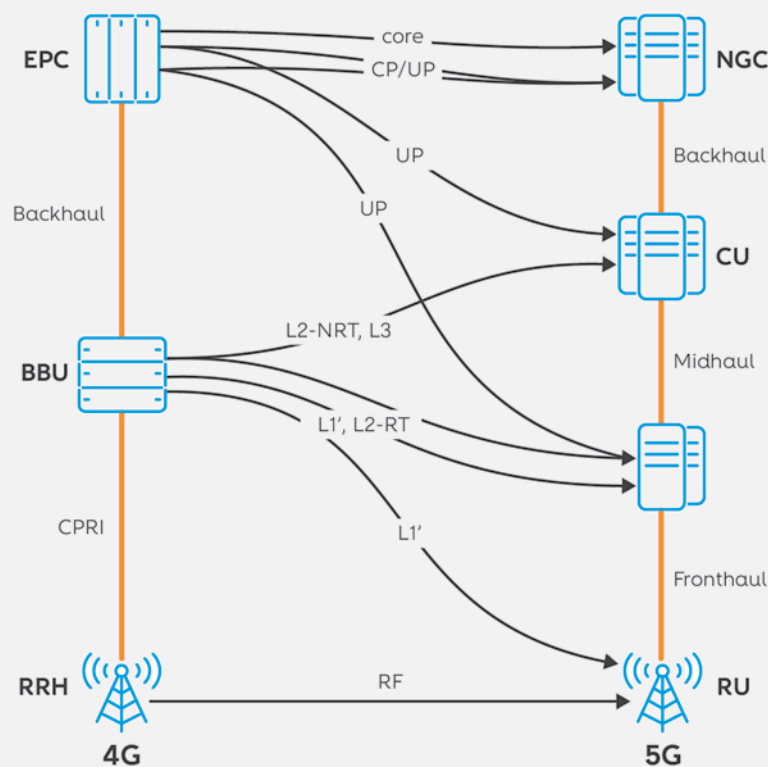
Standardized interfaces

This section will review in detail the role of interface standardization for the various 5G RAN dimensions.

5G-NR logical architecture and functional splits for midhaul/fronthaul

The 5G RAN will evolve from the traditional BBU and remote radio head (RRH) architecture used in 4G networks to a DU, CU, and RU architecture, which will better facilitate RAN virtualization and flexible assignment of computing resources across network entities, depending on the MNO network deployment strategy.

Figure 1 presents the architecture evolution from 4G to 5G [4]. The BBU is disaggregated by moving some of its functions to the RU (Low PHY), DU, and



BBU - Baseband Unit
CP - Control Plane
CPRI - Common Public Radio Interface
CU - Centralized Unit
DU - Distributed Unit
EPC - Evolved Packet Core

L1' - Lower part of the layer 1 (physical layer)
L1'' - Higher part of the layer 1 (physical layer)
L2-NRT - Layer 2 (data link layer) Non-Real Time

L2-RT - Layer 2 (data link layer) Real Time
L3 - Layer 3 (network layer)
NGC - New Generation Core
RF - Radio Frequency
RRH - Remote Radio Head
RU - Radio Unit
UP - User Plane

FIGURE 1 – Evolving from monolithic BBU in 4G to split function architecture in 5G [4]

CU. Part of the user plane (UP) functions are also moved from the evolved packet core (EPC) to the CU. The two new transport links between CU and DU and between DU and RU are frequently called fronthaul-II (or midhaul) and fronthaul-I (or simply fronthaul), respectively. The specific functions deployed in CU, DU, and RU are well defined. However, the way these entities are deployed on the network is flexible and allows distinct strategies, as we will see in the next sections.

To disaggregate the BBU functions, 3GPP defined eight functional split options for midhaul (CU-DU) and fronthaul (DU-RU) and selected the packet data convergence protocol (PDCP) / high radio link control (RLC) - option 2 - as the high layer split point, staying open for any low layer split, respectively. Other standardization bodies, namely

Small Cell Forum (SCF), O-RAN Alliance, and the Common Public Radio Interface (CPRI) cooperation, have also made some efforts to identify different split points. **Figure 2** maps the different splitting points from these different groups.

Basically, the optimal splitting point is a trade-off between coordination gain from functional centralization and latency and bandwidth requirements in the transport network, as shown in **Figure 3**. Centralized RAN considering lower layer splits (LLS) requires high transport capabilities (with both high bandwidth and low latency) and, in conventional fronthaul (option 8), continuous bitrate transport for very high transport applications. However, it allows the centralization of all high layer processing functions and coordination gain. On the opposite side, a distributed RAN

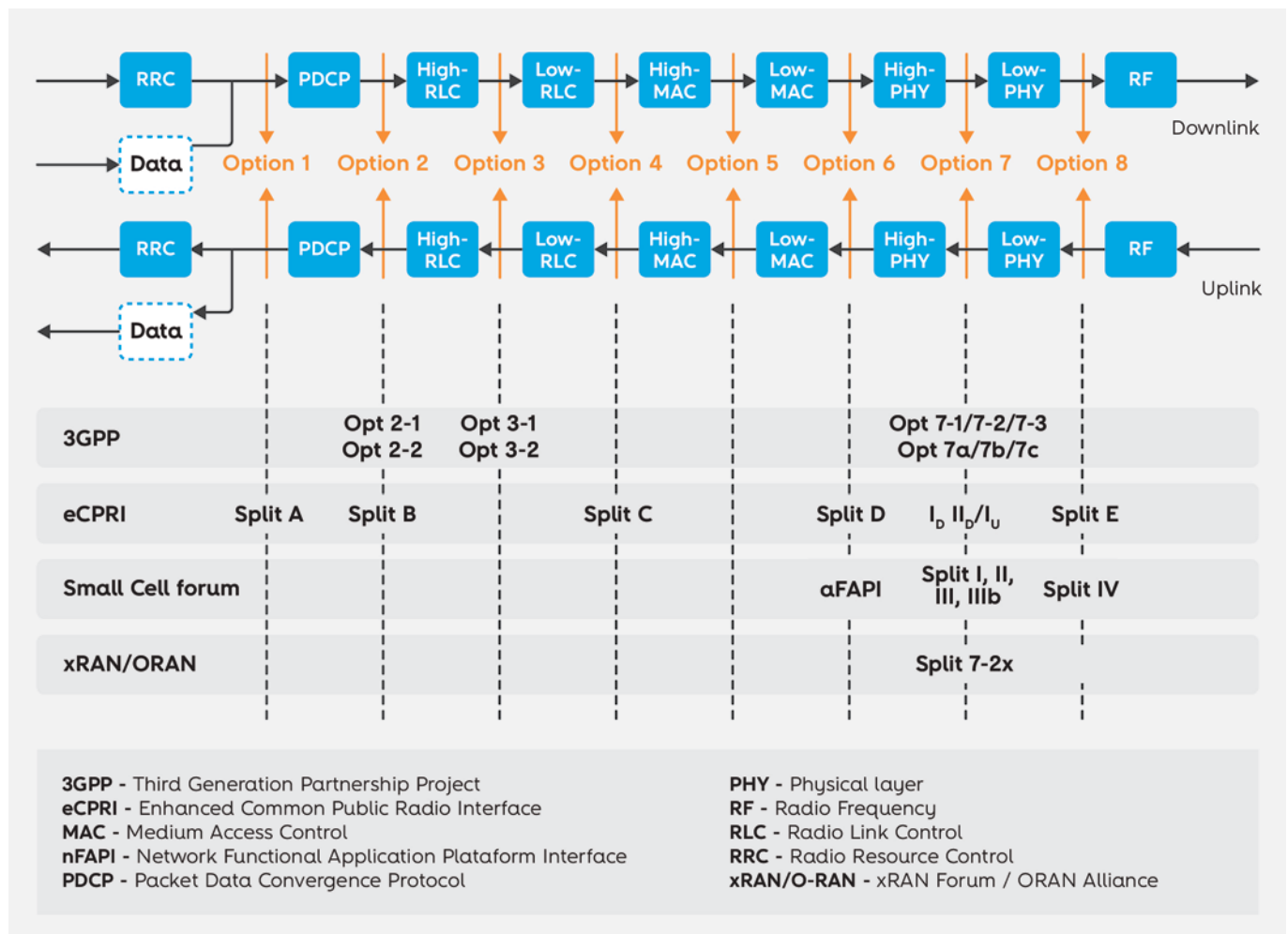


FIGURE 2 – Mapping different split points to the 3GPP model in 3GPP, CPRI cooperation, SCF, and O-RAN [5]

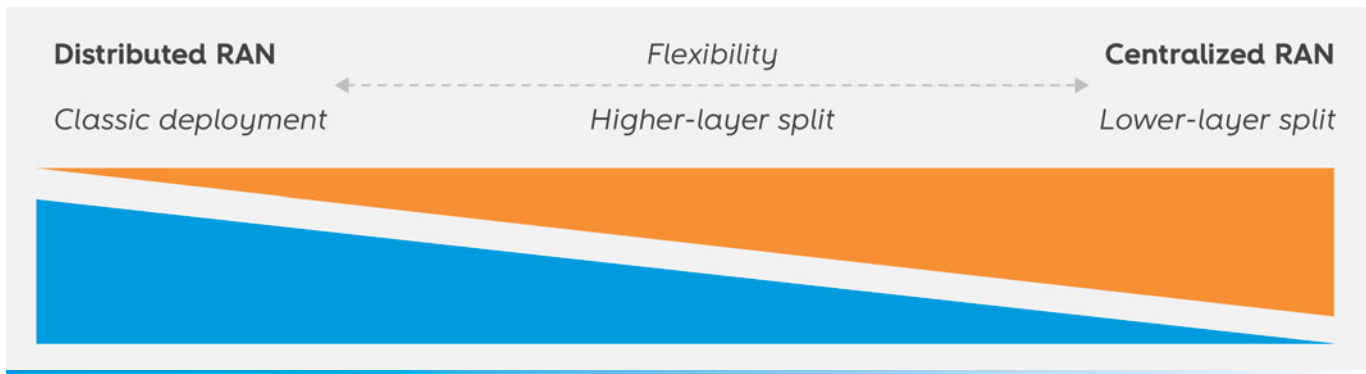


FIGURE 3 – Centralized vs. distributed RAN [6]

architecture considering backhaul or higher layer splitting (HLS) options makes the transport requirements soft but implies higher site cost and complexity and limited coordination between cells.

The choice between HLS and LLS is not always easy and aims to find the optimal economic and performance balance point for each MNO. Moreover, it may make sense to use different models for different regions (rural vs. urban) or different use cases. For example, HLS is more desirable for capacity use cases in dense urban areas, while LLS will be the optimum solution for coverage use cases. Cascaded-split architecture is also considered to allow additional flexibility.

Open interfaces – standards

The open RAN concept assumes full interoperability between RAN elements from different vendors. An MNO can deploy a fully compliant functional split architecture, but unless the interfaces between RU, DU, and CU are open, the RAN itself will not be open [7]. In this way, standardization constitutes a mandatory feature.

Currently, only split option 2 presents a standardized interface (the F1 interface), the primary new interface for midhaul, and was already specified by 3GPP with TS 38.470 to TS 38.475. It supports control and user plane separation (F1-C and F1-U) and separates radio and transport network layers.

Beyond the commonly accepted split 2, splits 6 and 7 are the ones the industry has, so far,

highlighted for fronthaul. In fact, the option 7 split point has been further diversified by several groups. One of the earliest standards and the most accepted is O-RAN open fronthaul interface specified by O-RAN Alliance WG4 that considers split 7-2x. This open standard details all of the signaling formats and control messages needed for multi-vendor DU and RU equipment to interoperate. It supports both enhanced CPRI (eCPRI) and radio over Ethernet (RoE) transport mechanisms and separates control, user, synchronization, and management planes (CP, UP, SP, and MP). The standard has been in development since 2017, and the latest version of this specification, Release 3, is now available on the O-RAN Alliance website [8]. There are already available some commercial deployments using the O-RAN fronthaul specification.

On the other hand, SCF has defined the network functional application platform interface (nFAPI) to use with split 6. This interface is an evolution of FAPI, an internal interface within an integrated or disaggregated small cell, and started its release in July 2019 [9]. However, SCF225, the network FAPI for the physical layer (PHY) and medium access control (MAC) split specification, is still under development.

Note that not only the midhaul/fronthaul interfaces are relevant for an open RAN architecture, but also the 3GPP standardized interfaces must be really open. One example is the optional X2 interface in legacy 4G that, even though being standardized by 3GPP,

many incumbent vendors intentionally did not implement or used many proprietary messages. However, to guarantee a seamless function in a multi-vendor environment, this interface becomes essential. It is even more relevant in 5G non-stand alone (NSA) deployments and is forcing MNO to deploy 5G using their existing 4G vendors [10].

Transport options for midhaul and fronthaul

5G deployment foresees a massive number of cell sites. To achieve this, the MNO need to rely, as much as possible, on the currently installed network infrastructure. Passive optical network (PON) technologies and architecture present a good trade-off between network coverage, ease of integration, available resources, and fitness for the considered network scenarios. The PON networks present as a strong candidate to allow the massive deployment of 5G cells, both due to the evolution of the PON technologies that will tend to support bandwidths of 50 Gbps and above, and its extensive geographical coverage and termination points density. The PON allow

different transport options and strategies, depending on the specific requirements of implementation. **Figure 4** depicts how the PON covers those different transport options.

There are advantages and disadvantages to any of these approaches, and all these options may be adopted in different situations.

Cloudification and virtualized RAN

One consequence of the previously described functionality desegregation is the ability to, once decoupled, place these different functions in separate physical locations, allowing for simpler and less expensive hardware implementations (for example, in remote locations with more stringent requirements in terms of power and/or space constraints). Furthermore, this process can be optimized by distributing the more typically centralized elements across multiple cloud

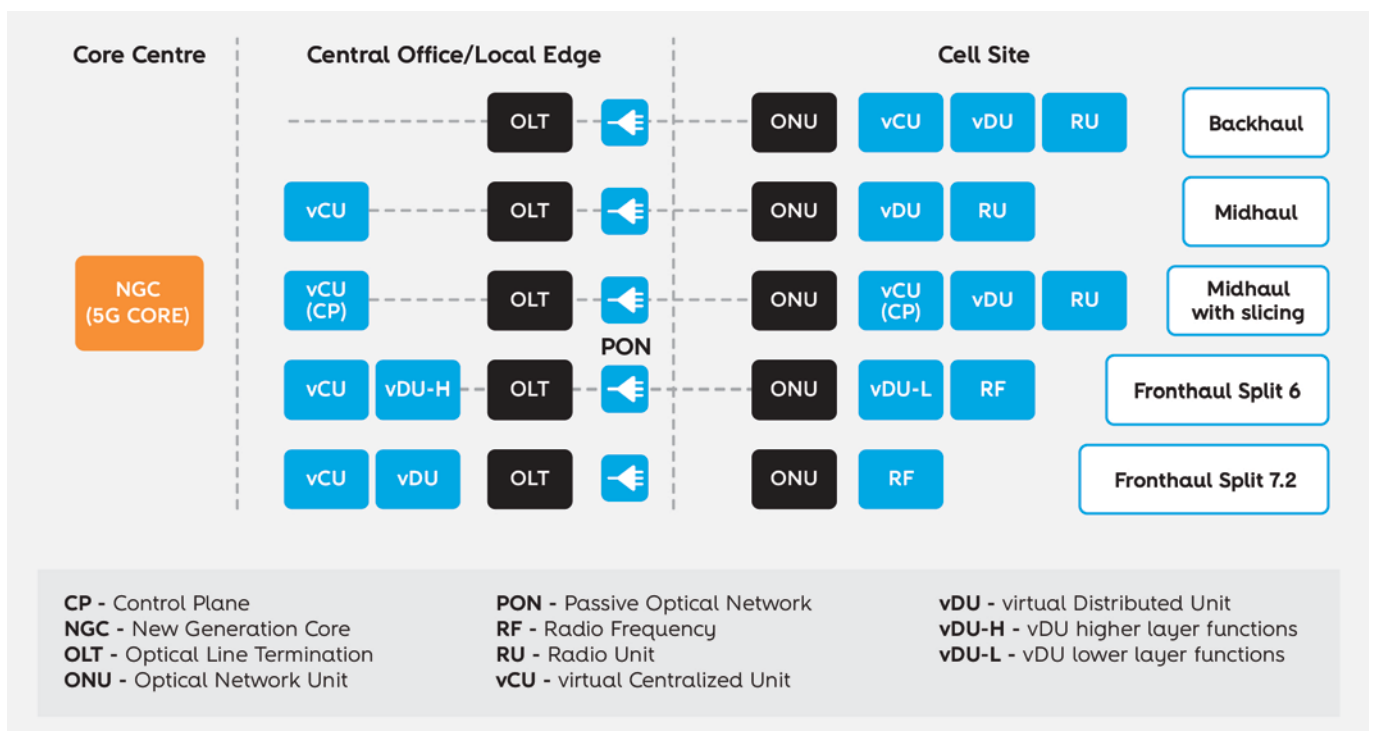


FIGURE 4 – Open RAN deployment scenarios considering PON as the transport network

environments (e.g., edge cloud, large datacentres, etc.) [11].

In essence, network cloudification allows for the extension of cloud platform technologies and their virtualization capabilities throughout a communication network, resulting in the increment of flexibility, agility, and scalability that the new 5G telecommunication network deployments require.

Cloud technologies, which fundamentally changed the way we look at computations, and more importantly, the pace of innovation, build upon a combination of principles:

- **Disaggregation:** Breaking vertically integrated systems into independent components with open interfaces;
- **Virtualization:** Being able to migrate components from custom-built nodes and run multiple independent copies of those components on a common (generic) hardware platform;
- **Commoditization:** Being able to elastically scale those virtual components across commodity hardware bricks as workload dictates [11].

With the advent of open RAN for 5G, which advocates for open, interoperable interfaces

and hardware-software disaggregation, the implementation of such cloud technologies becomes a major technological enabler for 5G networks.

Cloud technology presents innovative alternatives for such RAN deployments, complementing the existing and proven purpose-built solutions by implementing RAN functions over a generic compute platform and by managing RAN application virtualization using cloud-native principles. This way, selected 5G RAN functions (e.g., CP and UP functions in the CU or latency-sensitive radio processing functions in the DU) can be implemented through COTS hardware platforms [12] [13].

This process can be extended and replicated by distributing the more centralized elements across various clouds, including large datacentres that already benefit from elasticity and economies of scale, as depicted in **Figure 5**.

Of particular importance is the concept of network function virtualization, allowing dynamic scaling (in and/or out) of functions according to the demand (capacity, throughput, and load balancing).

Currently, MNO are looking into virtualized RAN solutions also as an enabler to reduce the total cost of ownership (TCO) [14].

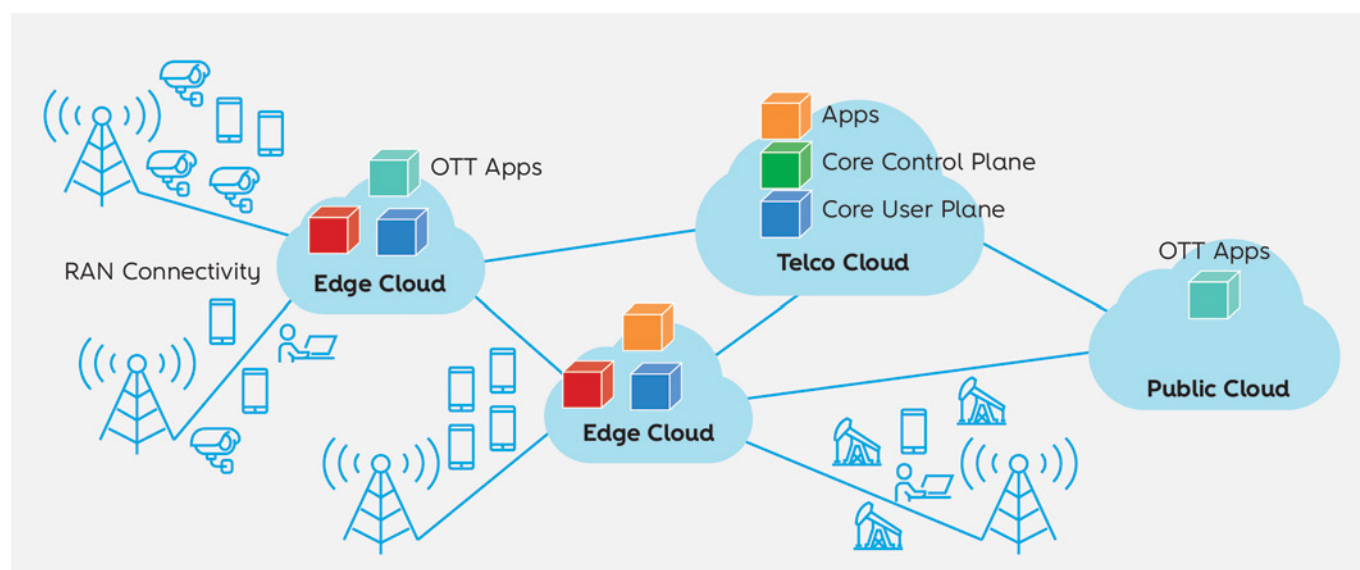


FIGURE 5 – Multi-tenant / multi-cloud (including virtualized RAN resources and conventional compute, storage, and network resources) hosting both TELCO and OTT services and applications

White box hardware architecture

In parallel to the trend of using COTS hardware to provide the higher layer functions (as presented before), the MNO and industry alliances are also looking into open hardware for the lower layer functions, based on the white box concept.

The O-RAN White Box Hardware Working Group (WG7) released two specifications focused on the utilization of open hardware architectures for the implementation of 5G base stations, namely, the “Deployment Scenarios and Base Station Classes for White Box Hardware” and the “Indoor Picocell Hardware Architecture and Requirement (FR1 Only) Specification”. The second document presents the architectural diagrams, the functional module descriptions, and the interfaces for the CU, DU, RU, and fronthaul gateway (FHGW) modules,

considering the functional splits 8, 7-2, 6, and 2. It defines the performance, interfaces, environmental, electromagnetic compatibility, mechanical, thermal, and power requirements for all the supported splits.

Figure 6 presents the functional modules of an open RU (O-RU) accordingly to the functional splits 8, 7-2, and 6, as well as a DU+RU monolithic box in case of split 2. The radio frequency (RF) processing unit remains the same independently of the functional split adopted. On the other hand, most of the operations performed by the digital processing unit depend on the considered split. The figure shows both the common and the specific operations depending on this design/ deployment decision. Regardless of that, the digital processing unit can be efficiently implemented on a digital programmable device, such as an FPGA or a multiprocessor programmable system-on-a-chip (SoC), containing both reconfigurable logic and hardwired multicore processors. That means the same device and implementation

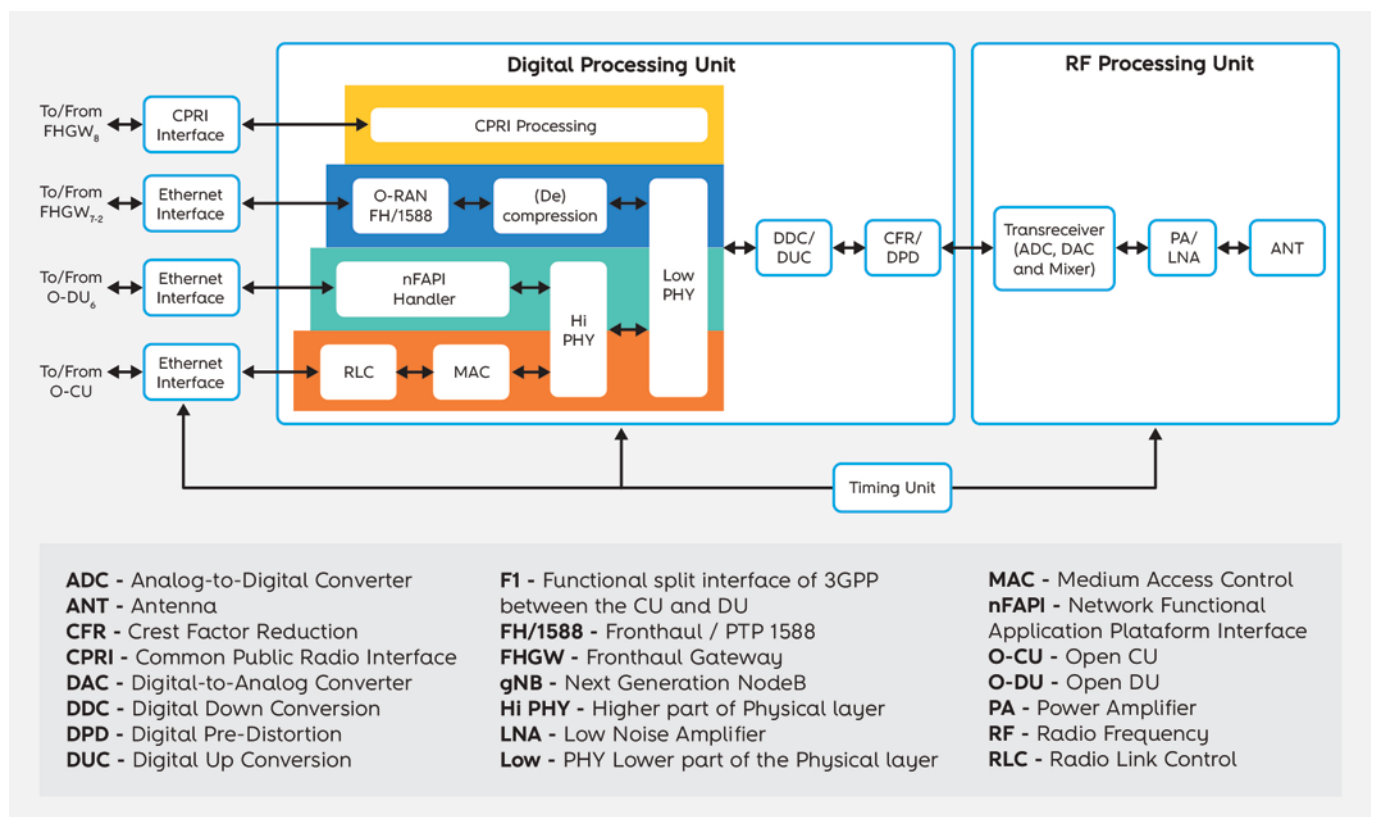


FIGURE 6 – Functional modules of an O-RU accordingly to the functional splits 8, 7-2, and 6, and a monolithic gNB DU+RU in case of split 2

platform can be used for distinct deployment scenarios. Multicore hardwired processors are particularly adequate for implementing the RLC and MAC layers, while the programmable logic of the multiprocessor SoC (MPSoC) is used for the remaining digital processing unit operations that are more processing-intensive and/or require timing accuracies at the clock cycle level.

Moreover, since the physical interfaces, both network and RF, are the same, regardless of the splitting options, it is feasible the dynamic modification of the deployed split as well as the installation of field upgrades.

Requirements and drivers for open RAN

There are several businesses and technical drivers to embrace an open RAN architecture. Managing CAPEX and OPEX in the RAN is critical as continuous growth in data traffic can drive the TCO of mobile access networks up by three times [15]. CAPEX and OPEX need to be kept at a lower level because of the need for network densification and for cases where economies of scale are not applicable, such as in rural or enterprise vertical deployments, requiring much lower cost solutions to stimulate further deployments. From a technical point of view, centralization and virtualization are an operator's old desire because of scalability limitations of traditional architectures and the constraints of incumbent vendors lock-in. They are also seeking for 5G new business models and use cases consolidation.

OPEX and CAPEX reduction

Standardized interfaces and software/hardware disaggregation allow opening the infrastructure market to more flexible and agile companies, which will enable reducing the network cost in the medium/long term. Software and hardware disaggregation allow scalable, cost-effective, and fast network deployments, upgrades, and swaps,

if that hardware and software components are interoperable and can be mixed and matched from different vendors. Network architectures where CU and DU functions tend to be at central locations and away from location-constrained cell sites will allow MNO to benefit from reduced cell site hardware footprint and resources pooling gains. RU and DU separation also allow lower-cost radios for network densification as less intelligent RU will cost less. Open RAN implementations will potentially also allow MNO to significantly reduce OPEX through remote operations and maintenance [16].

Technical drivers

Splitting up the next generation node B (gNB) between CU, DU, and RU, and virtualizing them will bring the necessary flexibility to the network. The gNB can be scaled flexibly from a small (single DU) to a large size (accommodating multiple DU), agnostic of DU hardware types for various deployment environments. The CP and UP may also be dimensioned and scaled independently. CU-UP can be sliced into multiple CU-UP and can be deployed in independent locations (as shown in **Figure 4**). This separation also enables adaptation to various use cases and the QoS that needs to be supported (i.e., gaming, virtual/augmented reality, etc.) [7].

Aggregating CU and/or DU at centralized locations allows coordination between different RU (co-located or not) for performance features, like coordinated multi-point (CoMP), load management, real-time performance optimization, and more reliable mobility.

Increasing the supply chain diversity (i.e., having more vendors), in addition to cost reduction, will also promote innovation. New vendors need to create new markets, innovation, and service markets that large incumbent vendors either have no interest in or cannot provide solutions for. For example, deploying private cellular networks for small-to-medium enterprises (SME) is not a market where tier-one vendors are interested due to specific requirements and smaller individual contracts. This is where new and smaller vendors could excel and create innovative solutions [16].

Key challenges

The success of open RAN will be, essentially, dependant on the following three key challenges.

- **Interoperability and integration** – A truly fully interoperable solution must be achieved to allow multi-vendor deployment scenarios and avoid vendor lock-in. Some initiatives are taking place to facilitate integration and interoperability validation. The Open Test and Integration Center (OTIC) initiative was launched to verify, integrate, and test components functional compatibility to O-RAN specification [17] [18]. The goal is to develop an ecosystem with many different solutions, assured to work together, from which system integrators can select to build solution portfolios. Standard entities as O-RAN Alliance are also specifying interoperability tests for the new open interfaces [19] [20].
- **Operational complexity** – Traditionally, MNO rely on a single vendor to resolve issues and problems. A multi-vendor environment brings additional challenges, as it might not be immediately clear the cause of a specific problem and the product/vendor responsible for it, imposing higher operational risks [21]. For example, it can be difficult to establish with precision where bottlenecks are located when experiencing delays. To mitigate this, a service level agreement (SLA) with each vendor should be defined, just like the multi-vendor traditional approach (e.g., between EPC and RAN).
- **RU market under-development** – The RU market supporting the open fronthaul 7.2x from O-RAN Alliance is still under development. Additionally, as referred to previously, there are still open interface specifications under development. If these open solutions take too long to get mature, there is a high risk that the traditional, vendor-specific solutions are adopted due to the operators' urgency to deploy 5G quickly.

Use cases and business opportunities

When considering dense built-up areas where propagation through obstacles, such as buildings and trees, can be an issue, operators need to densify their mobile networks with small cells for 5G coverage and QoS enhancement. Such use cases of coverage extension and densification are considered the main scenarios for open RAN network deployment with non-incumbent vendors [22].

There are several attributes of the 5G-era use cases and 5G-era technologies that make small cells ideal candidates for the roll-out of 5G, as shown in **Figure 7**. For example, the massive density of the 5G-era internet of things (IoT) use cases suggests using small cells, as they can be deployed in high-density areas due to their small physical form factors. Additionally, small cells bring several deployment benefits, as it has already been demonstrated in the 3G & 4G eras.

Next, we present some relevant practical use cases where the 5G deployment approach mentioned above can play a relevant role.

Outdoor hotspots

MNO will look at small cell technology in order to add data capacity in areas of traffic congestion. A dense, small cell network increases both the radios per subscriber and provides subscribers improved signal quality for more efficient data transfer. The shorter distance between radio sites also helps overcome the higher frequency 5G radio spectrum's short signal reach. As a result, small cells are becoming the leading solution in growing the network's data capacity.

In addition to the possibility for an easier and less costly 5G network densification, 5G small cells also allow increased network flexibility and reduced network expansion complexity.

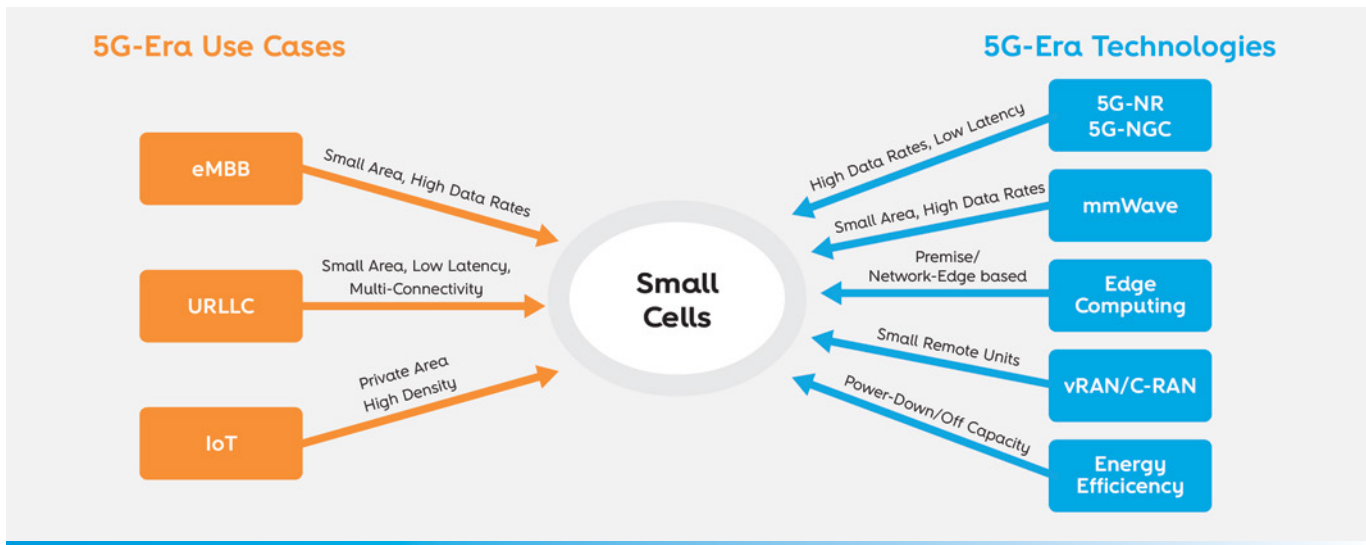


FIGURE 7 – Rationale for 5G small cells [23]

Neutral host providers

Neutral host providers (NHP), a third-party non-operator entity, will arise specifically to deploy 5G small cells in urban centers, historical downtowns, or public buildings. In many of these cases, there is no business case for large MNO to invest in their own network densification or, there are local entities or regulatory constraints. This is an opportunity for NHP to deploy a network to be rented to different MNO and potentially reduce operators' OPEX and CAPEX (shown in **Figure 8**).

Private networks

Many large enterprises, businesses, and public entities, who want to control security or guarantee it, are exploring private 5G networks, independent end-to-end small/medium-sized 5G networks, recurring to the 5G small cells and open RAN architecture (depicted in **Figure 9**). This may be of interest, particularly in the following context:

- Industrial centers that require critical communications, i.e., needing availability, reliability, QoS, and security;

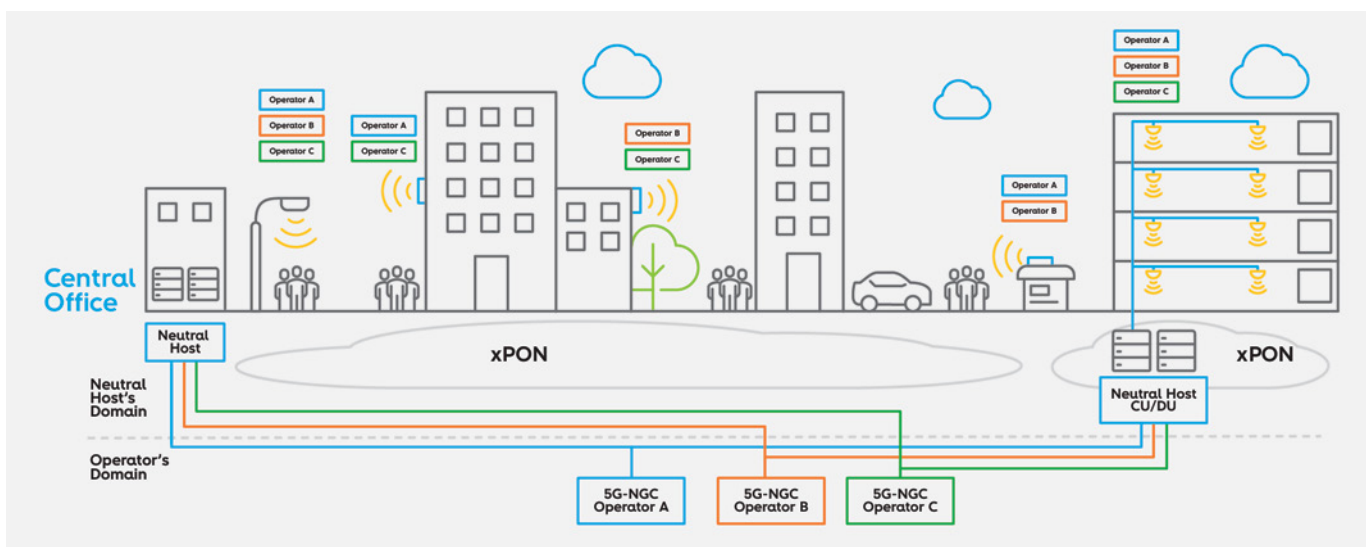


FIGURE 8 – Neutral host networks use case

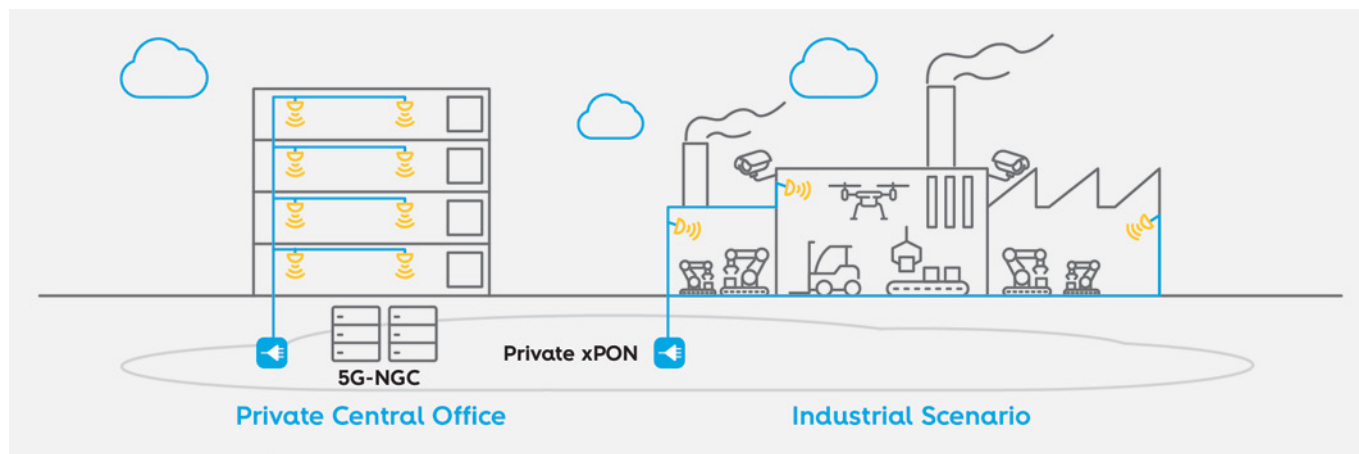


FIGURE 9 – Private networks use case

- Large companies and facility owners that require secure networks, high throughput, and QoS;
- Municipalities that aim to deploy smart cities solutions.

Other use cases

Other use cases for 5G small cells implementation using open RAN architecture are:

- Indoor small cells solution to solve coverage/capacity problems for medium/large businesses and facility owners. RU may work as an indoor distributed antenna system (iDAS);
- Rural small cells for coverage in extensive areas of low population density. This allows MNO to comply with the population coverage objectives at a reduced cost and provide broadband access in remote zones, otherwise non-existent, while providing social well-being.

5G open RAN @ Altice Labs

There are two main open RAN R&D paths at Altice Labs that complement each other. The first one aims to test and optimize midhaul and fronthaul

transport (in an O-RAN architecture) over the PON. The second one intends to design and implement a RU prototype also incorporating the optical network unit (ONU) (e.g., XGS-PON) functions. To achieve the proposed goals, and taking into consideration that (i) a complete C-RAN is needed for integration and test; and (ii) it is very complex and out of our current scope to develop the DU and CU entities, Altice Labs has decided to survey the market and select a 3rd party solution for the missing components. As a result, an evaluation kit (EVK) from ASOCS [24] was acquired. This evaluation kit is a completely functional 5G C-RAN (as present in **Figure 10**), and it is being used to support the ongoing R&D activities.

This kit provides end-to-end cellular connectivity for 5G NR - stand alone (SA) from the new generation core (NGC) to the end device. The system is virtualized by software that runs on COTS servers and interfaces with RU using ethernet fronthaul, which is compliant with the ORAN-FH (split 7.2, Fronthaul) interface. The CU-DU interface is 3GPP compatible and implements split 2 (midhaul). The CU server runs the CU application, and the NGC/5G core (5GC) application can be externalized from third-party Metaswitch [25]. It also runs the license manager and management system.

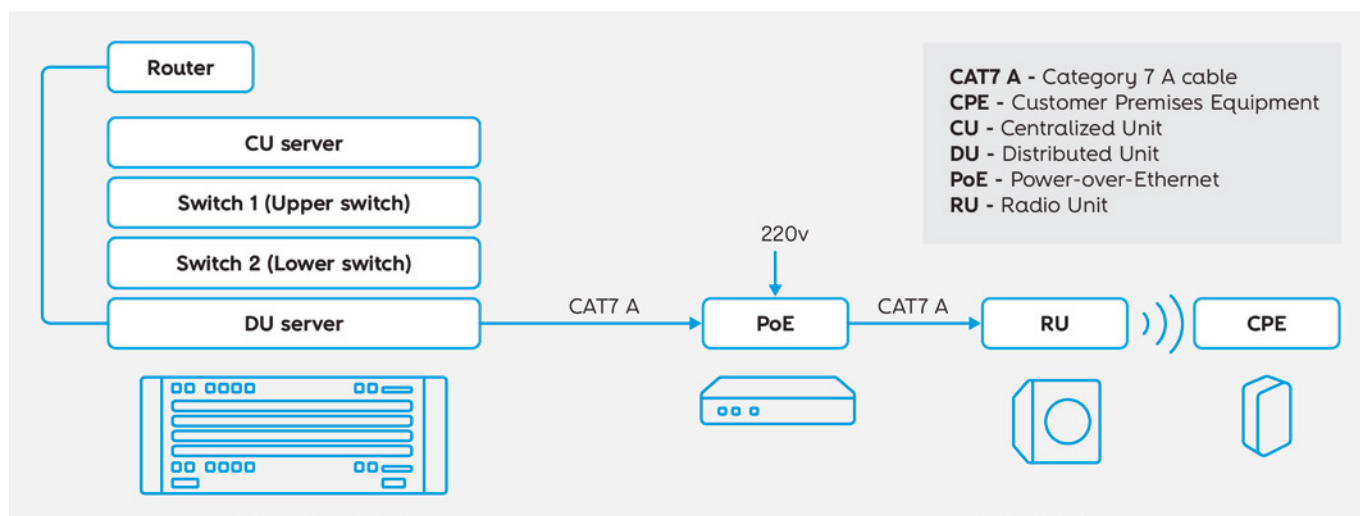


FIGURE 10 – ASOCS open RAN evaluation kit

PON integration for midhaul and fronthaul transport

The ongoing research aims to evaluate the constraints of using PON technologies both on the fronthaul (DU-RU connection) and on the midhaul (CU-DU). We are using an OLT and an optical network unit (ONU) with XGS-PON – 10G/10G.

We need to evaluate the impact of PON latency, jitter, and particularly the asymmetry between downstream and upstream. Maximum fiber distance and bandwidth consumption are also important aspects to be evaluated. The need to have G.1588 precision time protocol (PTP), a phase and time synchronization protocol, on the PON (OLT and ONU) will be evaluated to both transport options under different network conditions.

RU prototype design and implementation

As referred, an immediate main challenge for open RAN is the RU availability. Altice Labs, in collaboration with Instituto de Telecomunicações de Aveiro (IT Aveiro), is prototyping an RU that will be used, in integration with the ASOCS EVK, to support many of the ongoing 5G R&D activities at Altice Labs. The main goal is to achieve a

prototype that combines the RU functions with the ONU functions in a compact design. The final goal is that these research activities lead to an open RAN RU product or product line. **Figure 11** shows this RU prototype.

As stated before, the RU prototype under development will be used to support demonstration scenarios from multiple ongoing research projects. One of them will be a 5G small

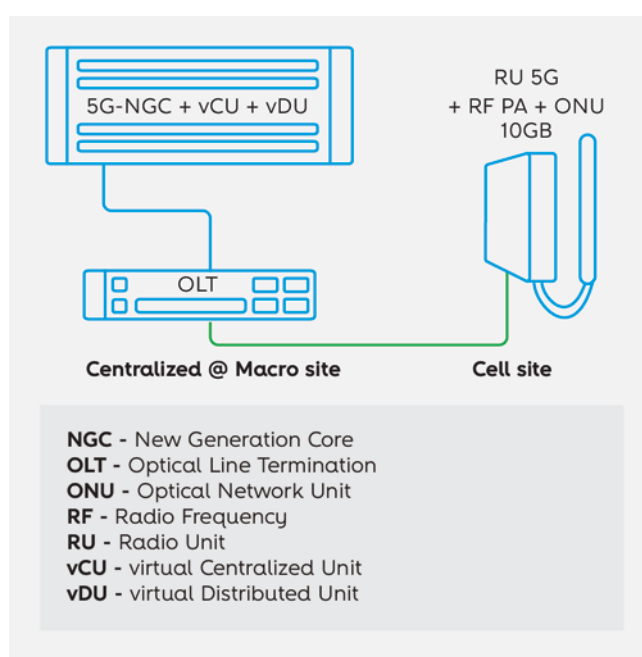


FIGURE 11 – RU prototype for European R&D projects


cell scenario for railway coverage, monitoring, and control in Aveiro seaport, under the H2020 5Growth European Project framework. This project addresses both enhanced mobile broadband (eMBB) and ultra-reliable and low-latency (URLL) use-cases. In the first one, HD video 16Mbps should be transmitted from a camera installed in the railroad crossing to the moving train. In the second case, railroad crossings should be controlled by sensors installed in the train line. Both use cases will be using a 5G cell. On top of it, a distributed, low footprint solution is required due to the lack of space and installation restrictions.

In the scope of this, some key challenges are being addressed. One challenge is the RF power amplifiers' market availability, working in the new 5G n78 frequency band (TDD 3.5GHz). Another challenge is the existence of some incompatibilities between O-RAN products that requires some adaptations.

Conclusions

There is growing enthusiasm for open RAN with some products already available on the market and some ongoing deployments. Standardization is moving forward, but in some cases, it is not yet completed.

Of the main players, MNOs are the most interested in open RAN for the promise of cost reduction that may enable the 5G business case, greater flexibility, a decrease of lock-in situations related to legacy vendors, and enhancing innovation. Other small players are also interested but will have to form an open ecosystem to move more safely. The large vendors are being pushed into this architecture, but they are advancing with moderate steps.

Altice Labs is working in this area to develop an open and integrated RU with the PON portfolio and try to take advantage of the opportunities mentioned here, particularly for small cells and 5G densification. 

References

- [1] G. Intelligence, "The Mobile Economy," 2020. [Online]. Available: https://www.gsma.com/mobileeconomy/#key_stats
- [2] G. Brown, "Open Mobile Networks : Systems Integration and Automation," 2019. [Online]. Available: <https://cache.techmahindra.com/static/img/pdf/systems-integration-and-automation.pdf>
- [3] O-RAN Alliance, "No Title." <https://www.o-ran.org/>
- [4] China Mobile Research Institute, "Toward 5G C-RAN: Requirements, Architecture and Challenges," 2016
- [5] ITU-T, "5G wireless fronthaul requirements in a passive optical network context," 2019
- [6] G. Brown, "New Transport Network Architectures for 5G RAN," 2018
- [7] Eugina Jordan, "Open RAN 101–RU, DU, CU: Why, what, how, when?," 2020. https://www.rcrwireless.com/20200708/open_ran/open-ran-101-ru-du-cu-reader-forum

- [8] O-RAN Alliance, "Published O-RAN specifications," 2020. <https://www.o-ran.org/specifications>
- [9] Small Cell Forum, "5G Fapi: Phy Api," 2020. [Online]. Available: www.smallcellforum.org
- [10] Parallel Wireless, "Why We Need the Open RAN Movement Even Though 3GPP Interfaces Are Already Open," 2020. <https://www.parallelwireless.com/why-we-need-the-open-ran-movement-even-though-3gpp-interfaces-are-already-open/>
- [11] L. Peterson and O. Sunay, *5G Mobile Networks: A Systems Approach*. 2020
- [12] E. Parsons and G. Foglander, "The four key components of Cloud RAN," 2020
- [13] Intel, "Intel 5G and Cloudification: Laying the Foundation for Innovation." <https://www.intel.la/content/www/xl/es/wireless-network/5g-cloud-computing.html>
- [14] G. Shenbagaraman, "Who disaggregated my RAN? Part 7: Virtualized RAN: Closer than you think," no. July 13, 2020, [Online]. Available: https://www.rcrwireless.com/20200713/open_ran/who-disaggregated-my-ran-part-7-virtualized-ran-closer-than-you-think
- [15] F. Grijpink, A. Ménard, H. Sigurdsson, and N. Vucevic, "The road to 5G: The inevitable growth of infrastructure cost," no. February, pp. 1–8, 2018, [Online]. Available: [https://www.mckinsey.com/~media/McKinsey/Industries/Telecommunications/Our Insights/The road to 5G The inevitable growth of infrastructure cost/The-road-to-5G-The-inevitable-growth-of-infrastructure-cost.ashx](https://www.mckinsey.com/~media/McKinsey/Industries/Telecommunications/Our%20Insights/The%20road%20to%205G%20The%20inevitable%20growth%20of%20infrastructure%20cost/The-road-to-5G-The-inevitable-growth-of-infrastructure-cost.ashx)
- [16] D. Mavrakis and M. Saadi, "OPEN RAN : MARKET REALITY AND MISCONCEPTIONS," no. June, 2020
- [17] iGillottResearch Inc, "Open RAN Integration : Run With It," 2020
- [18] China Mobile Limited, "Global Operators Collaborate with Industry Partners to Facilitate O-RAN Testing and Integration," 2019. <https://www.prnewswire.com/in/news-releases/global-operators-collaborate-with-industry-partners-to-facilitate-o-ran-testing-and-integration-882975147.html>
- [19] O-RAN Alliance, "O-RAN Fronthaul Working Group Conformance Test Specification," 2020
- [20] O-RAN Alliance, "O-RAN Fronthaul Working Group Fronthaul Interoperability Test Specification (IOT)," 2019
- [21] N. Shusina, "3 CHALLENGES YOU MIGHT FACE WITH OPEN RAN DEPLOYMENT," 2020. <https://blog.viavisolutions.com/2020/04/29/the-challenges-in-open-ran/>
- [22] M. Paolini, "OpenRAN : the operators ' perspective A survey for Mavenir," 2019
- [23] Small Cell Forum, "5G-era IoT use cases and enterprise small cell networks," 2019
- [24] "ASOCS Cloud." www.asocsccloud.com
- [25] "Metaswitch." www.metaswitch.com

Acronyms & Terms

2	2D/3D	Two/Three-dimensional
3	3G/4G/5G	Third, fourth and fifth generation mobile networks
	3GPP	Third Generation Partnership Project, a collaboration between groups of telecommunications standards associations
5	5GC	5G Core
	5G-NR	5G New Radio
6	6DoF	Six Degrees of Freedom
A	ABE	Attribute-Based Encryption
	ADC	Analog-to-Digital Converter
	AES	Advanced Encryption Standard
	AFR	Annualized Failure Rate
	AGF	Access Gateway Function
	AGF-C	Access Gateway Function Controller
	AGF-M	Access Gateway Function Manager
	AGORA	Altice Labs' network management solution for its network products
	AI	Artificial Intelligence
	AI HLEG	HighLevel Expert Group on AI
	AIOps	AI on operations
	AMF	Access and Mobility Function
	AN	Access Network
	ANT	Antenna
	AOI	Automatic Optical Inspection
	API	Application Programming Interface
	AR	Augmented Reality
	ARaNI	AR and Natural Interaction for Smart Living, a collaborative project with UTAD
	ASOCS	ASOCS Ltd., a privately held company focus on deploying of on-premise cloud solutions for industries
B	B2B	Business-to-Business
	B2C	Business-to-Consumer
	BAA	Broadband Access Abstraction
	BBF	Broadband Forum
	BBU	Baseband Unit

Bluetooth	A wireless technology standard for exchanging data over short distances using short-wavelength ultra-high frequency radio waves
BMI	Body Mass Index
BNG	Broadband Network Gateway
BNG-C	BNG Controller
BNG-M	BNG Manager
BNG-U	BNG Unit
BoM	Bill of Materials
BSS	Business Support System

C	CAPEX	Capital Expenditures
	CAPIF	Common API Framework
	CAT7 A	Category 7 A cable
	CAVE	Cave Automatic Virtual Environment
	CCO	Cloud Central Office
	CCODO	CCO Domain Orchestrator
	CCPA	California Consumer Privacy Act
	CDC	Centers for Disease Control and Prevention
	CFR	Crest Factor Reduction
	CNI	Critical National Infrastructure
	CO	Central Office
	CO-CO	Commercial Owned – Commercial Operation
	CoMP	Coordinated Multi-Point
	COTS	Commercial Off-The-Shelf
	COVID-19	Coronavirus disease 2019
	CP	Control Plane
	CP Funct.	CP Functions
	CPE	Customer Premises Equipment
	CPRI	Common Public Radio Interface
	C-RAN	Cloud Radio Access Network
	CSL	Cybersecurity Law, of the People's Republic of China
	CSP	Communication Service Providers
	C-Suite/C-Level	The C-suite/C-Level is deemed the most important and influential group of individuals within a company
	CU	Centralized Unit
	CU-C	CU – Control plane
	CUPS	Control and User Plane Separation
	CU-U	CU – User plane

D	DAC	Digital-to-Analog Converter
	DBNG	Disaggregated Broadband Network Gateway
	DC	Dual Connectivity
	DCSDN	Data Center SDN
	DDC	Digital Down Conversion
	DFM	Design For Manufacturing
	DHCP	Dynamic Host Configuration Protocol
	DPD	Digital Pre-Distortion
	DPU	Distribution Point Unit
	DSP	Digital Service Providers
	DU	Distributed Unit
	DUC	Digital Up Conversion
	DU-H	DU - High
	DU-L	DU - Low

E	E2E	End-to-End
	E2ESO	E2E Service Orchestrator
	EAD	Ethically Aligned Design
	EC	Edge Cloud
	ECDC	European Centre for Disease Prevention and Control
	e-commerce	Electronic commerce
	eCPRI	Enhanced Common Public Radio Interface
	EDGEAPP	3GPP architecture for enabling Edge applications
	EDPB	European Data Protection Board
	e-health	A healthcare practice supported by electronic processes and communication
	e-Learning	Electronic learning is the delivery of learning and training through digital resources
	eMBB	Enhanced Mobile BroadBand
	EMC	Electromagnetic Compatibility
	ENISA	European Union Agency for Cybersecurity
	EPC	Evolved Packet Core
	ETSI	European Telecommunications Standards Institute
	EU	European Union
	EVK	Evaluation Kit
	e-Wallet	An electronic device, online service, or software program to allow electronic transactions. A digital wallet.

F	F1	Functional split interface of 3GPP between the centralized unit and distributed unit
	F1-C	F1 Control Plane
	F1-U	F1 User Plane
	FCAPS	Fault, Configuration, Accounting, Performance, and Security
	FCS	First Customer Shipment
	FH/1588	Fronthaul / PTP 1588
	FHE	Fully Homomorphic Encryption
	FHGW	Fronthaul Gateway
	FMIF	Fixed-Mobile Internetworking Function
	FMIF-C	FMIF - Controller
	FMIF-M	FMIF - Manager
	FMIF-U	FMIF - Unit
	FPGA	Field Programmable Gate Array

G	GDP	Gross Domestic Product
	GDPR	General Data Protection Regulation
	GIV	Global Industry Vision (from Huawei)
	gNB	Next Generation NodeB
	GPS	Global Positioning System
	GPU	Graphical Processing Unit
	GSMA	Global System for Mobile Communications Association

H	HD	High Definition
	HE	Homomorphic Encryption
	Hi PHY	Higher part of Physical layer
	HLS	High Layer Splitting

I	IAB	Integrated Access and Backhaul
	ICT	In-Circuit-Test
	iDAS	Indoor Distributed Antenna System
	IEEE	Institute of Electrical and Electronics Engineers
	IIoT	Industrial Internet of Things
	ILO	International Labor Organization
	INESC TEC	Instituto de Engenharia de Sistemas e Computadores, Tecnologia e Ciência
	IOPS	Isolated Operation for Public Safety

	IoT	Internet of Things
	IP	Internet Protocol
	IPS	Indoor Positioning System
	IPTV	Internet Protocol Television
	ISG	Industry Specification Group
	ISP	Internet Service Provider
	IT	Information Technologies
	IT Aveiro	Instituto de Telecomunicações, Aveiro
	ITS	Intelligent Transport Systems
K	KGC	Key Generation Center
	KPI	Key Performance Indicators
L	L1'	Lower part of the physical layer (L1) of the OSI reference model
	L1''	Higher part of the physical layer (L1) of the OSI reference model
	L2-NRT	Layer 2 - Non-Real Time, the data link layer of the OSI reference model communication channel
	L2-RT	Layer 2 - Real Time, the data link layer of the OSI reference model communication channel
	L3	Layer 3, the network layer of the OSI reference model
	LGPD	Lei Geral de Proteção de Dados of Brazil
	LLS	Low Layer Splitting
	LMS	Learning Management System
	LNA	Low Noise Amplifier
	Low PHY	Lower part of the Physical layer of the OSI reference model
	LTE	Long Term Evolution
M	M&C	Manager and Controller
	MAC	Medium Access Control
	MA-M	Mobile Access Manager
	MANO	Management and Network Orchestration
	MBMS	Multimedia Broadcast Multicast Service
	MCiOPS	Mission-Critical Isolated Operation for Public Safety
	MCX	Mission-Critical Services
	ME	Multi-access Edge
	MEC	ME Computing
	MEC M&C	MEC Manager and Controller

	MEP	Mobile Edge Platform
	MEPM	MEP Manager
	MIT	Massachusetts Institute of Technology
	ML	Machine Learning
	mmWave	Millimeter Wave
	MNO	Mobile Network Operator
	MP	Management Plane
	MP Funct.	MP Functions
	MPC	Multi-Party Computation
	MPSoC	Multiprocessor System on a Chip
	MR	Mixed Reality
	MTBF	Mean Time Between Failures
	MTC	Machine-Type Communications
	MVNO	Mobile Virtual Network Operator

N	n78	3.5 GHz 5G band, or C-band 5G, the most commonly tested and deployed 5G frequency
	NaaS	Network-as-a-Service
	NB	Northbound
	NE	Network Element
	NEF	Network Exposure Function
	NETCONF	A network management protocol developed and standardized by the IETF
	nFAPI	Network Functional Application Platform Interface
	NFV	Network Function Virtualization
	NFV MANO	NFV Management and Network Orchestration
	NFVI	NFV Infrastructure
	NFVO	NFV Orchestrator
	NGC	New Generation Core
	NHP	Neutral Host Provider
	NPI	New Product Introduction
	NSA	Non-Stand Alone
	NTN	Non-Terrestrial Network
	NUI	Natural User Interface

O	OBA	Out of Box Analysis
	OB-BAA	Open Broadband - Broadband Access Abstraction
	O-CU	Open Centralized Unit
	O-DU	Open Distributed Unit
	OECD	Organisation for Economic Co-operation and Development
	OLT	Optical Line Termination

ONT	Optical Network Terminal
ONU	Optical Network Unit
OPEX	Operational Expenditures
O-RAN	Open RAN
ORAN-FH	ORAN Fronthaul split 7.2
ORT	Ongoing Reliability Test
O-RU	Open Radio Unit
OS	Operating System
Os-Ma-CCDO	Operations Systems - Management - CCO Domain Orchestrator, a reference point between the CCODO and the E2ESO
OSS	Operation Support System
OTIC	Open Test and Integration Center
OTT	Over-the-Top

P	PA	Power Amplifier
	PCB	Printed Circuit Board
	PCF	Policy and Charging Function
	PDCP	Packet Data Convergence Protocol
	PET	Privacy Enhancing Technology
	PHE	Partial Homomorphic Encryption
	PHY	Physical layer of the OSI reference model
	PISS	Personal Information Security Specification
	PNF	Physical Network Function
	POC	Proof-of-Concept
	PoE	Power-over-Ethernet
	POI	Point-of-Interest
	PON	Passive Optical Network
	PPDR	Public Protection and Disaster Relief
	PPRL	Privacy-Preserving Record Linkage
	PTP	Precision Time Protocol

Q	QoE	Quality of Experience
	QoS	Quality of Service

R	R&D	Research and Development
	RAN	Radio Access Network
	RDT	Reliability Demonstrations Test
	RESTCONF	An IETF HTTP-based protocol that provides a programmatic interface for accessing data, using the datastore concepts defined in the NETCONF

RF	Radio Frequency
RFID	RF Identification
RLC	Radio Link Control
RMA	Return Merchandise Authorization
RoE	Radio over Ethernet
ROI	Return on Investment
RRC	Radio Resource Control
RRH	Remote Radio Head
RU	Radio Unit

S	SA	Stand Alone
	SCF	Small Cell Forum
	SDN	Software-Defined Network
	SDN M&C	SDN Manager and Controller
	SDO	Standards Development Organization
	SE	Searchable Encryption
	SEAL	Service Enabler Architecture Layer
	SHE	Somewhat Homomorphic Encryption
	SL	Sidelink
	SLA	Service Level Agreement
	SME	Small to Medium Enterprise
	SMF	Session Management Function
	SoC	System on a Chip
	SP	Synchronization Plane
	SPI	Solder Paste Inspection
	STB	Set-Top Box

T	Tbps	Terabits per second
	TCO	Total Cost of Ownership
	TDD	Time Division Duplex
	TELCO/TELCOS	Telecommunications Operators
	TM Forum	A non-profit industry association for service providers and their suppliers in the telecommunications industry
	TR	Technical Report
	TTM	Time To Market
	TV	Television

U	UE	User Equipment
	UI	User Interface
	UK	United Kingdom
	UO-CO	User Owned - Commercial Operation
	UO-UO	User Owned - User Operated
	UP	User Plane

	UPF	UP Function		xRAN/	xRAN forum / ORAN Alliance, a	
	UPF-C	UP Function Controller		O-RAN	world-wide community operating	
	UPF-M	UP Function Manager			in the Radio Access Network	
	UPF-U	UP Function Unit			industry	
	URL	Uniform Resource Locator				
	URLLC	Ultra-Reliable Low-Latency Communication		Y	YANG	A data modeling language used to model configuration and state data
	US/USA	United States of America				
	USD	United States Dollar				
	UTAD	Universidade de Trás-os-Montes e Alto Douro				
	UX	User eXperience				
V	V2X	Vehicle-to-everything				
	vBNG	virtual Broadband Network Gateway				
	vCU	virtual Centralized Unit				
	vDU	virtual Distributed Unit				
	vDU-H	vDU implementing higher layer functions				
	vDU-L	vDU implementing lower layer functions				
	VIM	Virtualized Infrastructure Manager				
	VNF	Virtual Network Function				
	VNFM	VNF Manager				
	VoIP	Voice over Internet Protocol				
	vOLT	virtual Optical Line Termination				
	vOMCI	virtual Optical Network Terminal Management Control Interface				
	VPN	Virtual Private Network				
	VR	Virtual Reality				
	vRAN	virtualization of Radio Access Network				
W	WHO	World Health Organization				
	Wi-Fi	IEEE 802.11x - Wireless Network (Wi-Fi Alliance)				
	WSP	Wi-Fi Positioning System				
X	X2 interface	Evolved Node B to Evolved Node B Interface				
	XGS-PON	10-Gigabit-capable Symmetrical Passive Optical Network				
	xPON	Designation for several Passive Optical Network technologies				
	XR	eXtended Reality				

Acknowledgments

Year after year, InnovAction is the result of powerful teamwork. Several persons from Altice Labs get involved and, along with external partners, contribute with their knowledge and time to grant this magazine's quality and ensure each edition has a diversified collection of articles.

Thus, we would like to thank all authors (identified in each article) for their contributions and share of the knowledge resulting from their research and work.

We also want to leave a note of gratitude to all technical and editorial reviewers that did a relevant and meticulous job on improving all articles' quality and excellence and, therefore, of the entire magazine.

Finally, a special word and acknowledgment to our designer for the excellent job of granting an appealing and coherent design across the entire magazine.

Strategic team:

Ana Patrícia Monteiro, Fausto de Carvalho,
Mário Rui Costa, Paula Cravo,
Paulo Pereira and Pedro Carvalho

Editorial team:

Ana Patrícia Monteiro and Paula Cravo

Art coordinator and graphic edition:

Cátia Santos Pinto

Technical reviewers team:

Álvaro Gomes, Ana Patrícia Monteiro,
António Manuel Amaral, Clara Magalhães,
Fausto de Carvalho, Fernando Morgado,
Helena Margarida, Isabel Borges,
Isilda Costa, Lourenço Moura,
Nuno Alexandre Seixas and Paula Cravo

