RCRWireless News
INTELLIGENCE ON ALL THINGS WIRELESS

May 2024

TELCO CLOUD & EDGE FORUM

KEY FINDINGS REPORT

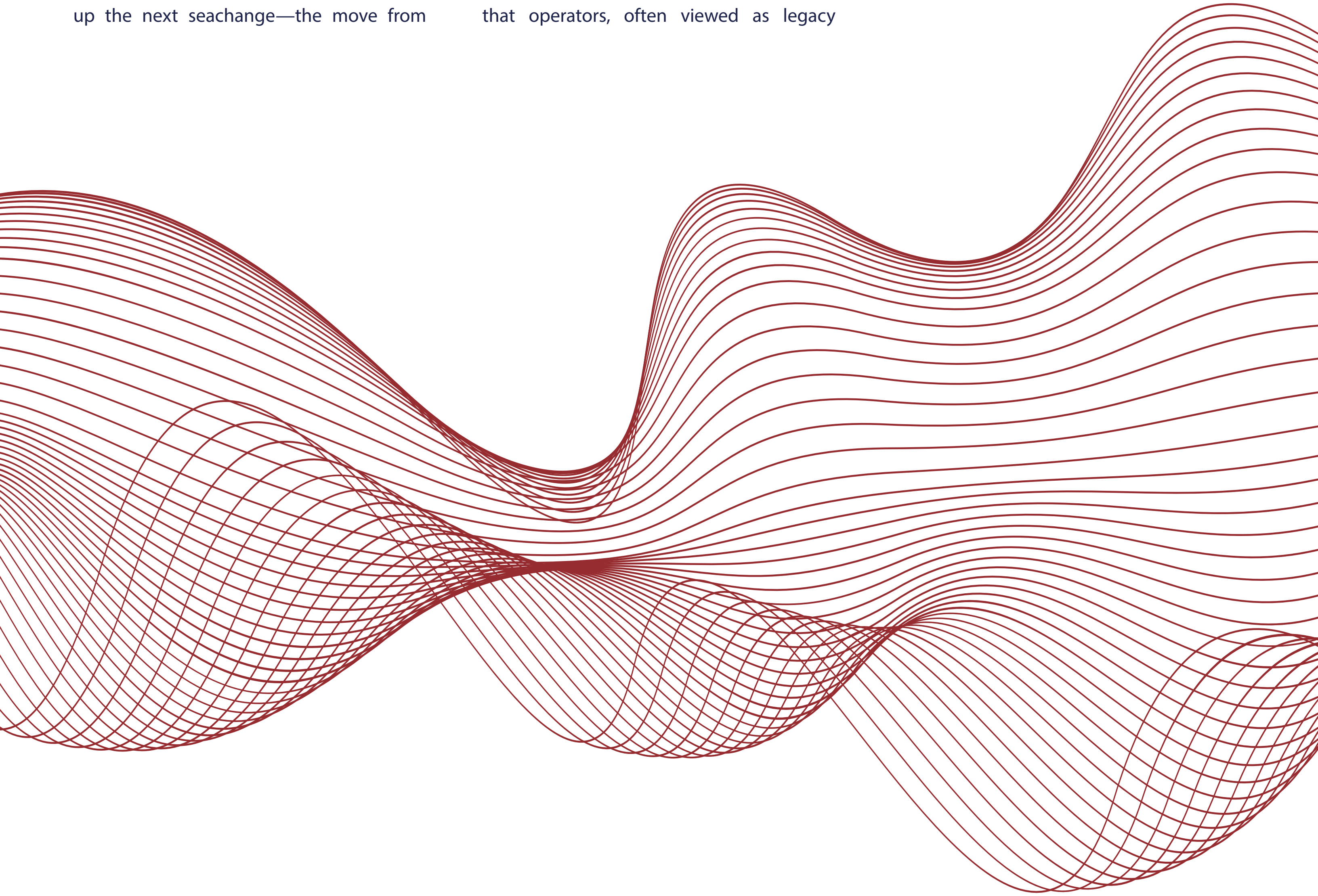
IT'S ALL ABOUT AGILITY, SCALABILITY, RESOURCE EFFICIENCY, COST EFFICIENCY AND INNOVATION

Sponsored by

f5 KORE spirent VIAVI Solutions VOLT ACTIVE DATA

INTRODUCTION

Whether for purely economic reasons, in an effort to better monetize network-enabled services, or to build a future-ready horizontal platform, or all three, it's clear that cloud and software will consume telecoms. And that's a good thing. The slow march to disaggregated networks replete with specialized software running in the cloud on highly-distributed commoditized hardware sets the stage for software development expertise as a key competitive differentiator. It also queues up the next seachange—the move from cloud-native to AI-native. But, while it's a good thing, it's also a difficult thing. The good news is that operators can look to colleagues in the worlds of hyperscale cloud computing and enterprise IT to bring longstanding best practices from those sectors into the world of mobile networking—with some domain-specific expertise added in of course. The bad news is cloud-native software development is an in-demand skillset, as is anything related to the innerworkings of AI, meaning that operators, often viewed as legacy organizations, are competing against dedicedly techcos in their own effort to shed the telco skin in favor of a new techco coat. This is a concern; as we learned during the recent Telco Cloud and Edge Forum, getting cloud right is as much, if not more, an exercise in organizational overhaul than in technology upgrades. In these pages, we recap, summarize and otherwise share the lessons learned from assembled industry experts.



(Image courtesy of 123RF)

UNDERSTANDING TELCO CLOUD STRATEGIES—WHO PUTS WHAT WHERE AND WHY?

TELEFONICA EXEC: "THERE IS NO ONE SINGLE TYPE OF A CLOUD THAT SERVES EVERYTHING EQUALLY"

Panelists at the event discussed the future of telco cloud strategies as they work to balance the need for innovation and the ability to scale with the very real risks associated with vendor lock-in and in giving up some amount of network management control.

PUBLIC VS. PRIVATE CLOUD FOR OPERATORS

When it comes to the question of what to run on the public vs. private cloud, Independent Telco Technologist and ex Red Hat Chief Technologist Timo Jokiaho said that there are "extremes" in telco cloud strategies. "Some service providers, they just don't touch public clouds," he continued. "The other extreme, of course, is that operator wants to run pretty much everything related to telco network on the public cloud." Then there are those that want a healthy mix of the two — known as a hybrid approach.

Jokiaho's recommendation to telcos is to "just leave" the user plane-related functionalities and entities—such as Open RAN and vRAN—on a private, on-prem cloud platform, and then "carefully" offload control plane functions like Access and Mobility Management Function (AMF) and Session Management Function (SMF) onto the public cloud.

Telenor Director of Cloud Strategy and Architecture Pål Grønsund offered the perspective of his telco on the matter: "We … have a public cloud first strategy," he shared, adding that the majority of IT functions, in particular, are going to be on public clouds. He added, though, that functions on the network side are still running in private clouds. "Most of the network functions we have today are more on virtual machines, but now transitioning into cloud native," he explained.

Francisco-Javier Ramón, the Multi-Cloud Tools Manager, GCTIO Unit at Telefónica and Chair of ETSI OSM, shared further that his company's cloud strategy emphasizes the importance of developing the capabilities that enable it to deploy workloads in "different type[s] of infrastructure," whether that's public or private.

"There is no one single type of a cloud that serves everything equally," he said, adding that the characteristics for the workloads and applications should help dictate where each should be run. "I think that this is the key in order to get the most from the different environments and that requires adopting a way that is cloud-agnostic for deploying, for monitoring, for managing the infrastructure setups."

Ramón was clear about the importance of one other cloud consideration: "We need always to develop the ability to manage the workloads in a manner that is cloud-agnostic," he said, explaining that doing so helps operators retain control of their supply chain. "You can't trust your supply chain 100% in one provider anyway. It would be unsafe for a critical infrastructure like this, so we need always to develop the ability to manage the workloads in a manner that is cloud-agnostic to some degree because we are already also acquiring the other part of the supply chain that is our own software that is running on top … In the end, it's a matter of having proper processes, proper modeling of those workloads so they can be managed in a cloud-agnostic manner. This is not about public or private clouds; it's … having … a healthy relation[ship] with your ecosystem," he stated.

VENDOR LOCK-IN AND THE ROLE OF HYPERSCALERS

You can't discuss the future of the public cloud without talking about the ones providing the public cloud, which, of course, are the hyperscalers. The big three are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), and according to Jokiaho, they have developed their cloud stack or cloud platform to "be suitable for pretty much any workload."

He continued: "We have seen that there are cases where hyperscaler stacks are deployed on premises at telco data centers, even on the edge or Open RAN, which proves that they do have — maybe not all, but some of them — technical functionality and technical features, which can host any workload. It's only a matter of where to deploy that cloud platform, on premises or on the public data center. I think hyperscalers are very well on the way to be able to host any workloads either on premises, on Telco data center or public data centers."

However, telcos remain concerned over the risk of vendor or hyperscaler lock-in as it creates additional complexity in the architecture and management of network functions. "When we look at the different cloud technology stacks from hyperscalers and other cloud platform vendors, from [an] application point of view, when you need to onboard [an] application and execute the application, they are not compatible [with] each other," explained Jokiaho. "That's probably one of the pain points to select the right hybrid model."

TIMO JOKIAHO
Independent Telco Technologist, former Red Hat CTO

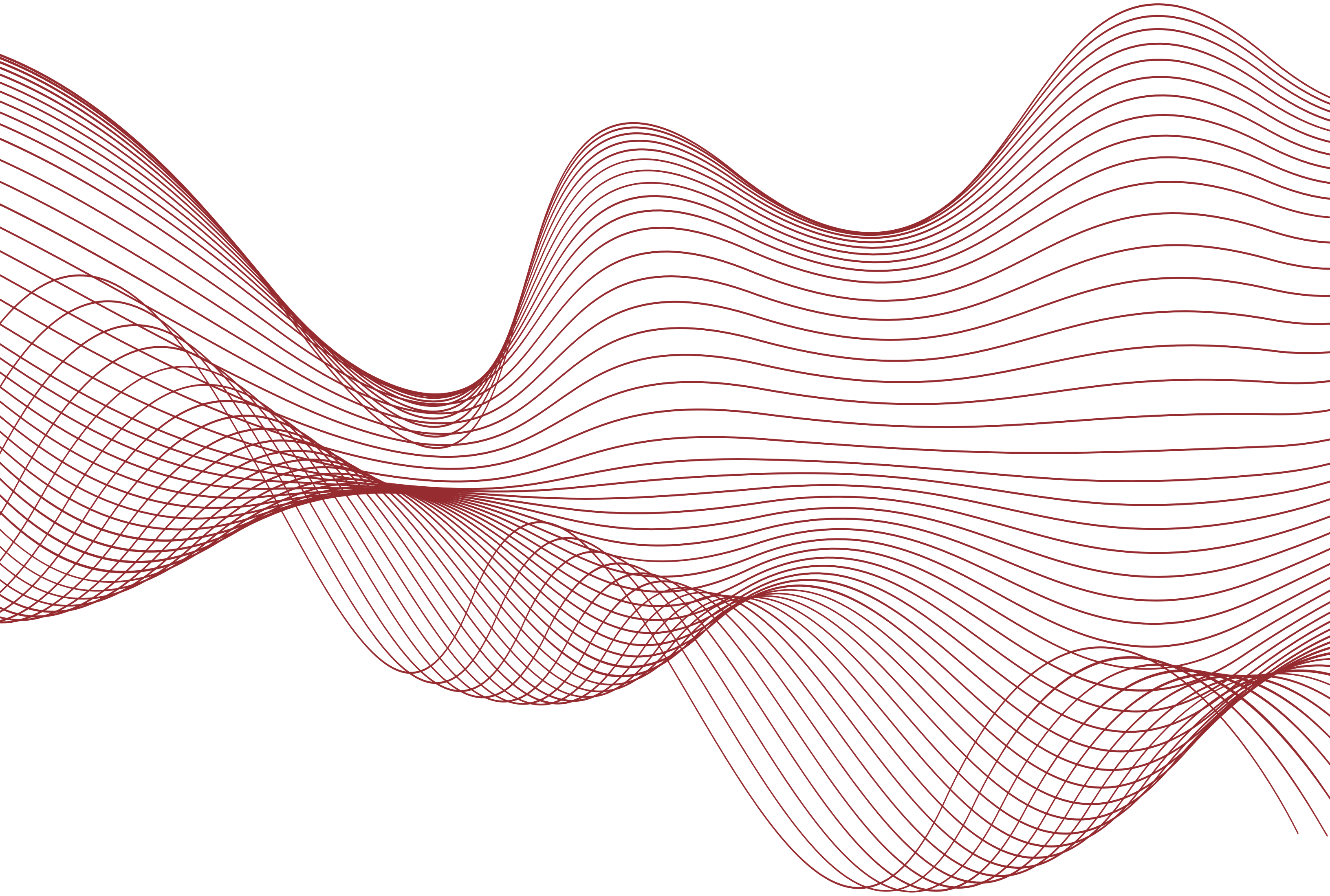
PÅL GRØNSUND
Director Cloud Strategy and Architecture, **Telenor**

FRANCISCO JAVIER RAMON
Multi-Cloud Tools Manager, GCTIO Unit, **Telefónica**

Telenor, then, is careful to remain “mindful” of vendor lock-in and the risks associated with it, said Grønsund. “How can we move around? Who is controlling what? For instance, around observability, are you using some proprietary observability tooling, or is it more open source out of the cloud providers? These things need to be managed and who is controlling that management and orchestration layer?” he continued.

Grønsund added further that there must be orchestration capabilities that support multi-clouds to enable enough flexibility to put the telco in control. “That can also ease the migration of workloads across when needed,” said. “We need to be in control of that orchestration on top of the cloud and orchestrating those network functions, multi-cloud wise.” This multi-cloud piece is of particular importance to Telenor as it enables the use of cloud service offerings from multiple cloud providers in multiple locations, including its hyperscaler and other cloud provider partners across the public and private cloud, depending on the unique needs and requirements of its customers and application providers.

The three panelists agreed that the issue of lock-in has yet to be fully addressed. Jokiaho, specifically, said that while there have been a few industry initiatives aimed at improving cloud platform compatibility, none of them have proven particularly successful. “We have quite a few going on as we speak, like a cloud native compute foundation and Linux Foundation Sylva project, which are addressing this point as we speak, but how successful will they be? Nobody really knows,” he said, adding, however, that even though it remains a “tough question,” he firmly believes it’s a “solvable” problem.



VIAVI Solutions

LEVEL UP YOUR NETWORK WITH AI-POWERED SOLUTIONS

VIAVI's AI-powered "Digital Twin" technology enables new predictive capabilities that strengthen networks against disruptions. By creating a virtual model of your network in the lab, you can quickly and effectively manage network behaviors, ensuring **peak performance** round the clock.

VIAVI's advanced AI systems set a new standard in network **security**, **resilience**, and **efficiency**, providing unique value with minimal risk.

Experience excellence.

viavisolutions.com/digitaltwins

(Image courtesy of Orange.)

ORANGE DISCUSSES ITS CLOUD-NATIVE STRATEGY AND VISION

NEW PARADIGMS AROUND INFRASTRUCTURE AUTOMATION AND SOFTWARE DEVELOPMENT ARE GUIDING THE CLOUD-NATIVE REINVENTION OF ORANGE

Change is afoot in the telecom industry as the move to cloud-native operating and technological principles push and pull operators into new paradigms. With a renewed sense of conviction about the network as a platform for innovation—not just a utility-like network of dumb pipes—multinational communications service provider Orange is undertaking a massive reinvention, from telco to techco if you like, that's all about "agility, scalability, resource efficiency, [and] cost optimization," as Philippe Ensarguet, vice president of software engineering, explained.

Citing a renewed interest in leveraging network APIs via consortia like Linux Foundation's CAMARA and GSMA's Open Gateway Initiative, Ensarguet said, "We are at a moment where telecom operators basically are more and more convinced about the value of their network…The pjatformization model is something that is super, super important." And in this shift, he said there are lots of lessons to be learned from hyperscalers and enterprise IT, sectors that he reckoned are at least five years ahead of telecoms.

"It's happening," though, Ensarguet said. "The software transformation, the cloud transformation, the data transformation… it is happening right now. It means we are entering into new paradigms to implement our infrastructure. And I want to talk about the move from the very closed and proprietary, I would say, vertical model toward the horizontal model that is heavily…cloud-based. And driving this shift definitively for us opens new ways to operate our services and to be more efficient."

PHILIPPE ENSARGUET
Vice President of Software Engineering, **Orange**

The big picture here, in terms of guiding principles in the shift to cloud-native telecom networking, was laid out in a manifesto published last year by the Next Generation Mobile Networks (NGMN) Alliance with contributions from Bell Canada, BT, Chunghwa Telecom, Deutsche Telekom, Orange, Telia, Telus, Turkcell and Vodafone.

The cloud-native guiding principles as articulated in that paper are as follows:

- Decoupled infrastructure and application lifecycles over vertical monoliths
- API first over manual provisioning of network resources
- Declarative and intent-based automation over imperative workflows
- GitOps principles over traditional network operations practices
- Unified Kubernetes (or the like) resource consumption patterns over domain-specific resource controllers
- Unified Kubernetes (or the like) closed-loop reconciliation patterns over vendor-specific element management practices
- Interoperability by well-defined certification processes over vendor-specific optimization.

BORROWING CLOUD-NATIVE BEST PRACTICES FROM HYPERSCALERS AND IT

While this is something of a sea change for many operators, Ensarguet pointed out that it isn't like the goal is to reinvent the wheel. "We all know that basically the operating model for cloud-native is GitOps. So when you are using GitOps, basically you are using technology and components and projects that are coming from those [hyperscaler/IT] ecosystems." The big changes, he said, are around intent-based, automated operations of a disaggregated network, and the move to a distributed, service-oriented architecture.

Beyond this technological overhaul, Ensarguet stressed the importance of workforce and organization mindset shifts; essentially a departure from business as usual. For instance, he said, the idea of service reliability engineering, borrowed from Google, has been adapted for telecoms to network reliability engineering. And, of course, the rise of artificial intelligence, both classical and generative, sets up further necessary skill adjustments.

"When you're learning, you are learning about the tech, you are learning about the methodology, but you are also learning about also how the skills need to be transformed," he said. We are not in front of a simple evolution…We are in front of what I'm calling a revolution because it's about, I would say, the culture…It's about bringing a way to measure where the products are, where the services are. So it's about assessment, gap analysis, and then it's about educating, bringing awareness. We have an intense program of upskilling and reskilling."

In an AI world, experts are hard to find, expensive and very much in demand. This reinforces the need to upskill/reskill; when the people you need are hard to get, you have to count on the people you already have, he said.

(Image courtesy of 123.RF)

CLOUD-NATIVE BEST PRACTICES ON THE PATH TO AI-NATIVE NETWORKS

As it relates to how telecom networks were built and operated, not much changed between 1990 and 2010; physical networks were (and some still are) built using specialized, proprietary hardware and were operated manually. The decade ending in 2020 was all about virtualizing networks using software running on virtual machines to increase flexibility. Now we're on to cloud-native networks that leverage cloud computing principles to optimize performance using agile, resilient and open infrastructure. While AI-native networking is up next, Orange Innovation Networks Senior Project Manager and Research Ilhem Fajjari shared her perspective on the revolution that is the transition to a cloud-native telco.

Speaking during the forum, Fajjari called out a number of challenges operators will have to navigate as they move from the old to the new. She touched on integration of cloud-native solutions with legacy tech, an expertise shortage, security and regulatory compliance, managing multi-vendor complexity and the attendant push to interoperability, and aligning automation and orchestration efforts with operational efficiencies and improved user experience.

"To be able to achieve our cloud native transformation journey, as an operator we need to deal with challenges…A concrete implementation of our progress…it's not magical. We need to go through several steps to be able to become really cloud native."

ILHEM FAJJARI
Senior Project Manager and Researcher, **Orange Innovation Networks**

Fajjari laid out a four-step process for implementing cloud native technologies and operations.

Step 1: Adopt a lift and shift approach that leverages virtualization in the transition to cloud-native IT with an end goal of reducing complexity and avoiding vendor over-dependence.

Step 2: Foster a collaborative culture that actively embraces and promotes cloud-native principles, while also making a significant investment in continuous development of workforce skills. That all includes taking a fail-fast approach.

Step 3: Treat small scale experiments as testbeds for innovation, and allow for the exploration of new technologies in a controlled, manageable environment.

Step 4: Forge new network supplier relationships while also strengthening collaborations with other operators.

Fajjari described a horizontal approach to multilevel automation that includes the network infrastructure and functions across all network domains, as well as orchestration of the end-to-end services. She noted the ability to effectively provide end-to-end service assurance, monitoring and quality as part and parcel of providing network slicing which many operators are billing as a potential revenue driver.

She also focused in on data observability as a primary foundation for network automation. However, Fajjari also acknowledged that "because we need to collect the metrics coming from heterogeneous equipment" across the radio, transport, core and IT domains, there's an added complexity in the data collection that underlies observability.

Fajjari concluded her presentation with six best practices and principles to ease the transition to cloud-native telcos:

- Separate infrastructure and application lifecycles to increase agility and reduce complexity.
- Prioritize the use of APIs for network resource provisioning and management to enable automation and integration.
- Use intent-based, declarative automation over imperative workflows to streamline operations.
- Implement GitOps principles for network operations to ensure a single source of truth.
- Utilize unified consumption patterns, such as those provided by Kubernetes, to standardize resource management across different domains.
- Ensure interoperability through well-defined certification processes that encourage network equipment provider-agnostic solutions and prevent vendor lock-in. Foster an open ecosystem by adhering to standards and encouraging collaborative development across the industry.

(Image courtesy of 123.RF)

IN A FLEXIBLE, CLOUD NATIVE NETWORK, THE ATTACK SURFACE HAS BEEN 'OPENED UP'

UNDERSTANDING THE ROLE OF CI/CD IN SECURING CLOUD NATIVE NETWORK ENVIRONMENTS

Emerging technologies like cloud, edge and AI represent serious opportunities for telcos when it comes to network performance, efficiency and potential new revenue streams; however, they also present a host of new security risks in the form of container-based vulnerabilities, unsecured APIs, data breaches, insecure network connections and cloud misconfigurations. To address these rising threats, speakers at the event outlined the importance of a holistic, continuous approach to security testing and patch delivery in the form of CI/CD, or Continuous integration (CI) and continuous delivery/deployment (CD).

CI/CD is a software development principle or method in which automation is introduced into the entire lifecycle of software or application development, from testing to deployment. In this context, the automatic and continuous nature of CI/CD will allow operators to get security updates and fixes more quickly, efficiently and reliably into the network.

As a brief characterization of the main challenge ahead, Spirent's Senior Product Manager for security test solutions Sashi Jeyaretnam explained that cloud-native and edge environments inherently present a much more "open, flexible, software driven approach to networking, and therefore it opens up the attack surface a lot more."

As such, the potential for bad actors and malicious activities increases because more network layers are introduced. "There are so many moving parts in this environment," she added.

According to F5's Senior Solutions Engineer Greg Robinson, telemetry — which collects network traffic data to analyze it for threats — will become more critical in a more complex and disaggregated network.

"It's going to be important for developers to incorporate code that exports statistics and status out to dashboards so that [the] status can be seen regardless of where the service or what the container is running," he said, adding that the company is also looking into microservice based security and micro-segmentation through service meshes to gain insight into what's going on between those microservices running in Kubernetes environments.

Amy Zwarico, the director of cybersecurity at AT&T, also mentioned the growing importance of telemetry, recommending that telcos explore various techniques to monitor every layer of their network. to better determine if "something anomalous [is] happening."

Cloud-native and edge environments are very much "API-driven," as Jeyaretnam pointed out, and Spirent is finding that many telcos do not have a secure API and efficient token management. Other notable issues, she continued, include access control like privilege escalation, improper admission controls and role-based access controls, as well as "low-hanging fruit" like misconfigurations and credentials being default credentials.

"And to minimize these risks, it's all about having a holistic approach," she said, reiterating the fact that there are a lot of layers in a cloud native infrastructure — the Kubernetes operating system, the compute infrastructure, the network functions, those that validate the network functions themselves, and so on — and each and every layer must be validated and assured to make sure that this network evolution is function properly. "Having that comprehensive, holistic approach that covers all of those layers and can be assessed on a continuous basis is going to be the key to be able to resolve or mitigate those gaps that customers are finding in this environment," she claimed.

Therefore, all three panelists agreed that testing network security defenses in routine intervals won't be enough; testing must be a continuous process, and it must be automated.

"Making [testing] part of a complete automated process, you are going to be able to do your testing that used to take you months to do with a little bit of optimization in terms of lab automation and being able to use parallelization for testing and consolidating reports and so forth. You will be able to bring that testing cycle down from months to hours," said Jeyaretnam.

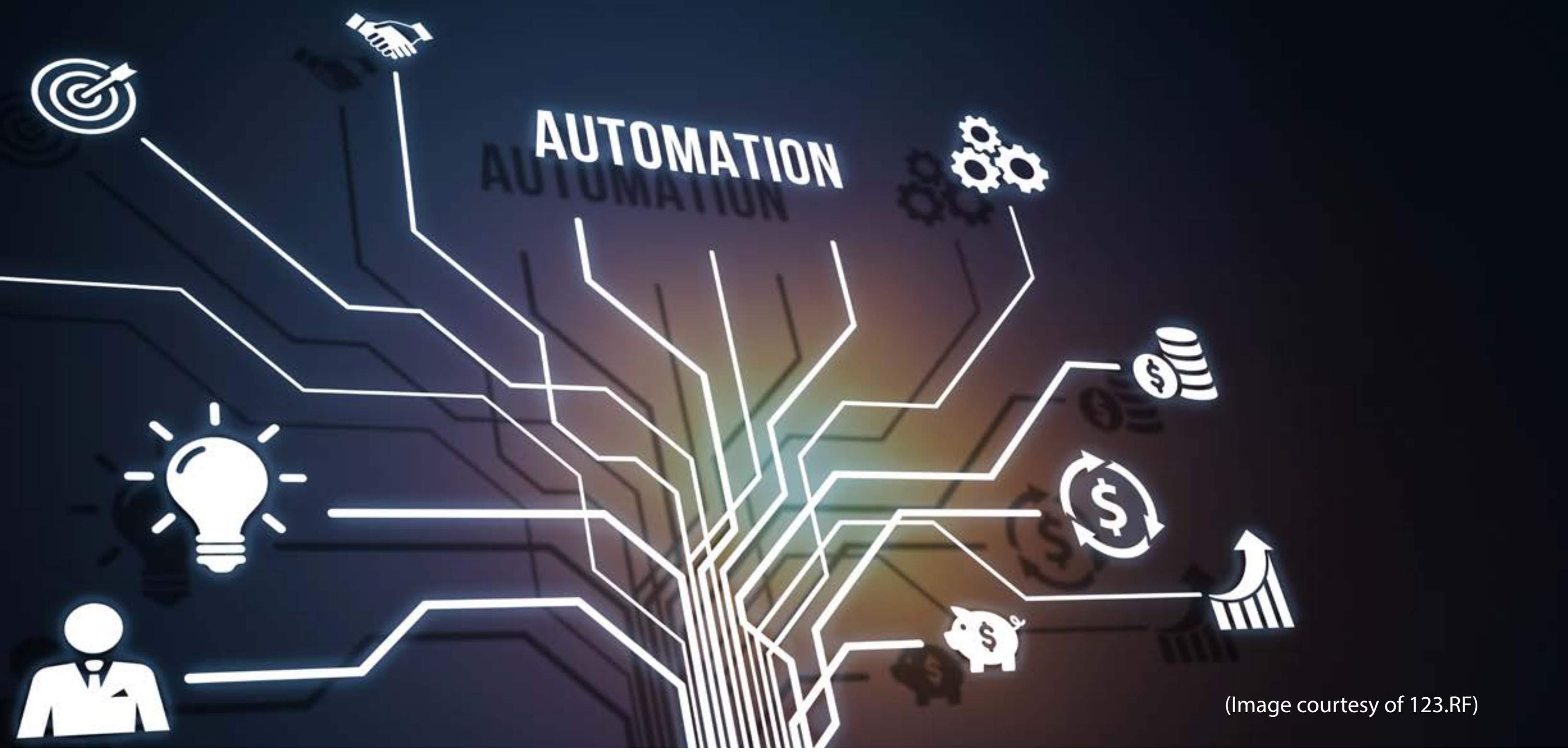
However, these CI/CD pipelines will become more complicated. That's because, with hardware and software coming from different vendors, per the promise of Open RAN, each layer of the architecture will require different patching cycles. "Think about the operating system on the cloud itself, then you've got a Kubernetes layer, then you have network functions and they're all separate," explained Zwarico. "They could all be coming from different places with really different release schedules. Vendors are going to have to address the complexity of aligning their operational and their security practices to be able to provide very frequent security updates and patches. I think this is going to be a big change … Telcos are not used to that rapid model in their mobility networks."

Jeyaretnam agreed that the CI/CD process will be complex and suggested that telcos prioritize the CI/CD pipeline early on. "They have to start planning for it as they're designing their networks and making their vendor choices and picking the right solutions," she argued. "And as they're developing these networks, they should be building their test cases and test plans around these elements that they're introducing into their network design."

SASHI JEYARETNAM
Senior Director of Product Management, Security Solutions,
Spirent

GREG ROBINSON
Senior Solutions Engineer,
F5

AMY ZWARICO
Chief Security Officer,
AT&T



(Image courtesy of 123.RF)

'BEAUTIFUL END-TO-END AUTOMATION'—HOW WILL OPERATORS INFUSE AI INTO THEIR NETWORKS?

TODAY OPERATORS ARE USING AI TO DETECT NETWORK ANOMALIES AND CONDUCT ROOT CAUSE ANALYSIS

Telecom companies have been using artificial intelligence (AI) and machine learning (ML) in their operations for years. However, the current telco environment sets the stage for further innovation around AIOps, or Artificial Intelligence for IT Operations. That's because as 5G continues to evolve, it also continues to become more complex. Virtualization and disaggregation are happening in tandem with deployment of network workloads in hybrid cloud environments. As a result, configuring, provisioning and assuring networks through manual — or even the standard automation strategies that telcos have been relying on for years — is no longer possible. Panelists spoke to this transformation, addressing key questions like how do advancements in generative AI (GenAI) fit into the conversation, how are operators using AI in their operations and what challenges persist?

In addition to complexity, Chris Murphy, regional CTO for EMEA at VIAVI Solutions, told the audience that the availability of reliable data is also a challenge in modern networks. "We have more disaggregation and more interfaces that we can hope to get data out [of] and understand how the network is performing, root cause problems, and understand how we can resolve those," he said, but added that the data must be collected, harmonized, cleaned and correlated.

he said, but added that the data must be collected, harmonized, cleaned and correlated.

"Different network layers, different parts of the network. It's not always easy to bring the data together to come up with a coherent view of what's going on so we can perform the advanced analytics and autonomous decisions that need to be made. But, in terms of the opportunities, I think the opportunity and the imperative really that we have to deliver is the intent-based, end-to-end automation, which is I think what we're ultimately aiming for," he continued.

Murphy shared that Viavi is starting to see consumer-level AI, like chatGPT, being merged into operational networks. "There's a clear trajectory that the industry is moving towards," he said, adding also that things like anomaly detection, root cause analysis, opening trouble tickets automatically are some specific examples of where AI is being used today.

For its part, AT&T is already using OpenAI's chatGPT for an internal application called Ask AT&T. Released in June, the application helps coders and software developers become more productive and translates customer and employee documentation from English to other languages, and even simplifies that same documentation and make it easier to use. Future use cases for GenAI, according to AT&T, include upgrading legacy software code and environments; making its care representatives even more effective at supporting customers; and giving employees quick and simple answers to HR questions.

More broadly, though, AT&T is using AI as a sort of co-pilot, the carrier's Network Chief Technology Officer Ajay Rajkumar told event attendees. AI currently helps the operator perform certain automated network optimizations, such as acting as an additional quality agent and providing recommendations for network parameter changes. The reason AT&T is taking the copilot approach to AI in its operations, rather than allowing it to fly solo, is because the carrier is still approaching AI — and GenAI, in particular — with caution.

"If there are biases or hallucinations — as is a problem with typically generative AI— and I'm drawing a distinction because it is generating new ideas from either what it has seen or what it has learned … those need to be really curtailed," said Rajkumar. "You could just not … say that [a] chatGPT-like structure could be used in [an] operational network … The cost of small mistakes or one singular mistake can be huge. These are critical networks … Once there is a reliability, we may be able to move forward with the level of automation that we're hoping we'd be able to get."

Right now, though, he said using AI as a co-pilot to assist operations with root cause analysis at an early stage or in real time is a very real possibility. But, for GenAI to be truly ready for operational networks on a wider scale, Rajkumar argued that significant and specific foundational model training must be performed. "Not generic network data, but … very specific network data for a given operator or a circumstance," he clarified.

A final consideration in this discussion is, of course, security, as there are always concerns around where the data is coming from and who can view said data. However, Murphy noted recent developments in the industry, such as secure enclaves two sets of data owned by different entities can be accessed by the AI system, but the data itself cannot be shared. "They can both benefit from bringing their own data, which has personal identifiable information and sensitive commercial information in it. Bring it together into an enclave and then ask it a question and see what the answer is, and it hides the data from each of the parties who's showing it … maybe there's a role for that sort of thing down the road," he said.

CHRIS MURPHY
Regional CTO, EMEA,
Viavi

AJAY RAJKUMAR
Principal Member of Technical Staff
AT&T

So, perhaps there are still a few kinks to be worked out. However, both panelists were optimistic about AI's future role in network management and optimization: "We'll have beautiful end-to-end automation of autonomous networks," Murphy predicted.

(Image courtesy of DISH Wireless)

FOUR CLOUD-NATIVE STRATEGY TAKEAWAYS FROM DISH WIRELESS

DISH WIRELESS EVP EBEN ALBERTYN ON LESSONS LEARNED FROM BUILDING AND OPERATING A CLOUD NATIVE

5G STANDALONE OPEN RAN NETWORK

After more than a decade of strategic spectrum acquisition, and given the regulatory go-ahead related to the T-Mobile US acquisition of Sprint, DISH Wireless has built out a 5G Standalone network that covers 70% of the US population and provides extensive VoNR service. Following cloud-native and Open RAN principles, DISH Wireless worked with multiple infrastructure and software vendors, serving as its own primary system integrator, to build out the network largely during the COVID-19 pandemic. DISH Wireless Executive Vice President and Chief Technology Officer Eben Albertyn discussed lessons learned from this process, and shared advice with others in the telecoms ecosystem about how to do cloud native.

EBEN ALBERTYN
EVP and CTO,
DISH Wireless

While the four takeaways delineated here focus on systems integration, the primacy of silicon, effective ecosystem development, and software development expertise, a cross-cutting theme in his commentary—and in many other discussions hosted during the forum—was the workforce and organizational changes necessary to depart from legacy ways of doing business and taking full advantage of the technology assets in place.

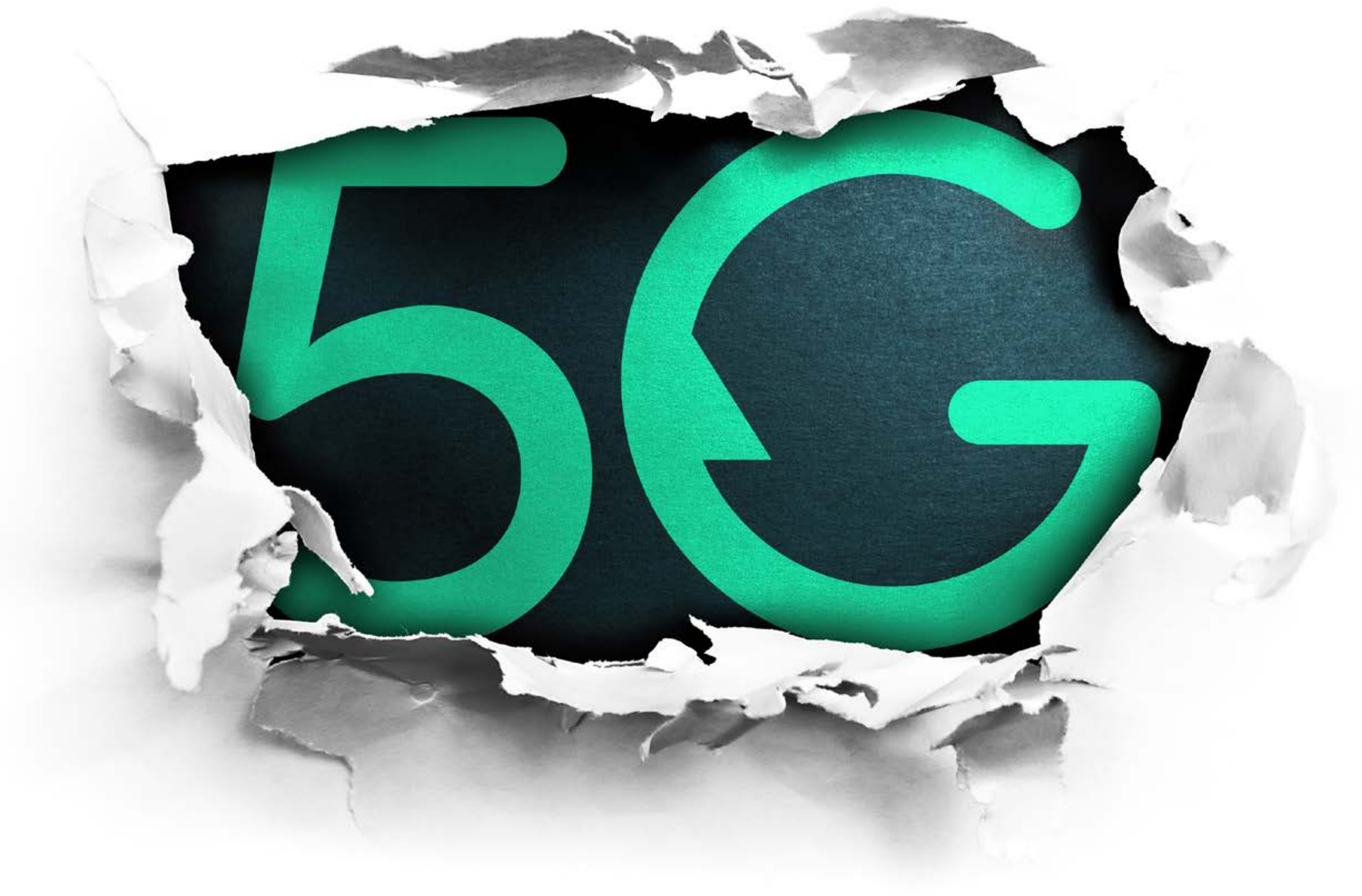
Editor's note: These comments are extracted from a longer interview which we'll further cover soon, and are lightly edited for length and clarity.

1. "Embrace wholeheartedly the challenge of being that end-to-end systems integrator, having to understand all the tech almost better than the partners that bring that tech and not standing back from the challenge of what it will mean to integrate, connect, manage, run, orchestrate, whatever you want to call it…Day one, embrace that, stop lying to ourselves, stop trying to make up all kinds of excuses as to why this is not the role of a classical telco. Just really embrace it and get on with it."

2. "Leverage silicon…chipsets and architecture. So we've designed the networks so that common data repositories are intrinsically inside of everything that we do. And it's all common because we want the ability for AI to be intrinsically used in any part of the network…Start using that capability—the silicon and the architecture—the power that unleashes. Start to use that sooner."

3. "Manage that ecosystem. As an example, one of the really big things we had to do was drive and drive and drive and drive and push standards for Open RAN, be part of forums like CAMARA and other places, and really push to get things practically done and get things really standardized and locked down so we can move forward. And I think sometimes we acted a little bit like a passenger on that train. The reality is if you're going to make things happen, you need to really take ownership and start managing that ecosystem and start really participating in that ecosystem. That doesn't mean dictating to everybody. It means really participating and really working with people on that."

4. "Software development expertise and how that relates to network in the cloud and embracing those worlds like they are one, because they've become one. So not being allergic to new technologies or network-as-a-code or routing as software or embracing things as they become available and being clear on the objectives that you're trying to reach and then using any and all technological means at your disposable to be able to address those. It's a culture of not having some religious conviction around some piece of technology being sacrosanct and therefore we're not going to use it or we're not going to part ways with it. It's about the end objective, which is building a great network for our customers."


5G

(Image courtesy of Rakuten)

RAKUTEN SEES 'HUGE POTENTIAL' FOR OSS—'THIS IS THE HOME OF INNOVATION'

IN A CLOUD-NATIVE WORLD, THE OSS SHOULD SERVE AS AN APP STORE FILLED WITH TOOLS FOR AUTOMATION, ORCHESTRATION, WORKFLOW ENGINES AND MORE

Rakuten Group, with its operator Rakuten Mobile and hardware/software/services vendor subsidiary Rakuten Symphony, don't live in the legacy world. The greenfield network is new, built using cloud-native and Open RAN principles; the processes and workflows are new—it's all about automating what can be automated while creating net new value; and it's about new thinking. As this relates to operational support systems (OSS), Managing Director and President of OSS Rahul Atri talked through this new way of thinking and what it means for OSS.

Before looking at the present and future, he looked at the past. "When we designed the OSS system, it was for management of the network functions and figuring out if the network is performing good, bad, and connecting the dots.

RAHUL ATRI
Managing Director and President, OSS, **Rakuten Symphony**

It has evolved into a service assurance [tool] where you could actually see services and know what the behavior of the services are. Now, when we see how we are evolving in terms of ecosystem technology, things have been super fast."

This "super fast" evolution includes an embrace of IT and cloud-native computing best set practices, things like GitOps, AIOps, and other areas that are all new to the world of telecoms. And all in pursuit of the expectation that networks will become "agile, infinite and always available for any kind of use case to be supported." In the march to network slicing, scaling in and scaling out, disaggregating hardware and software, pushing the user plane function to the edge and more, "I think OSS is a perfect place to have those synergies and figure out how we can convert multiple brains into applets. One of the functions could be automation, could be orchestration, could be workflow engines, and also about the digital maps which you need across the lifecycle management. I see OSS as a huge potential. I'm still trying to figure out what should be the right name for it. But, for me, this is the home of innovation, and if we want to do cultural revolution…think about future use cases, OSS has to be the platform."

In this revolution, Atri recommended a departure from buzzwords and a real, clear-eyed definition of "what is success...It's also important to understand what problem we're solving, what solutions are best…That can be OSS, that can be your automation platform, that can be [an] AI platform in the future. But the North Star vision of where we want to end up is the key, and that's how the organization itself gets aligned."

Atri is a regular on the conference circuit and he's generous with his time when it comes to talking to the trade press. One thing that comes up in conversations with him is a sort of dual focus on cutting-edge technology but also tried-and-true management theory. As the move to cloud-native networking highlighted, a lot of the problems to be solved have more to do with people than with the technology those people have at their disposal. As he put it, "Technology is not a problem…It's about how your organizations are structured."

One issue Atri addressed was striking the right balance between designing and deploying standards-compliant solutions in an era when cloud-native is broadening the pool of "telco" tech and moving faster than any standards body could match.

For operators, he acknowledged the need for standardization but also noted that parallel developments in open source communities, not to mention firms like Rakuten taking a do-it-yourself approach, is where "the innovation comes in. Standard could be an end-state, doesn't have to be a starting point, doesn't 'have to be a checkpoint…We should always look for innovation and the success criteria and obviously evolve together."

Regardless of whether an operator builds or buys an OSS, Atri circled back to his point around defining outcomes and success. "If it is agility, if it is automation, if it is efficiency, it is ROI. Let's define that."

(Image courtesy of 123.RF)

THREE OPEN API CHALLENGES THE INDUSTRY WILL HAVE TO ADDRESS IN PURSUIT OF NEW MONETIZATION OPPORTUNITIES

THERE'S MONETIZATION POTENTIAL INHERENT IN CLOUD NATIVE NETWORKS, BUT OPERATORS HAVE TO SIMPLIFY THE INTERFACE FOR THIRD-PARTY DEVELOPERS

While open Application Programming Interfaces (APIs) were a big topic at this and last year's Mobile World Congress in Barcelona thanks to the GSMA Open Gateway Initiative, APIs in general are not a new concept for telcos. What is new, according to Principal Analyst at STL Partners Emma Buckland, is the potential to expose the networks to a large audience of developers through open, non-proprietary APIs.

Buckland moderated an event panel with fellow experts to examine some of the biggest challenges opening up the API ecosystem might present, even as it promises a potential path to new revenue.

A COMPLEX CHAIN OF AGGREGATORS

Telcos are urgently seeking ROI as the deployment of 5G Standalone (SA) advances in tandem with the cloud-native network, and as such, are recognizing that in order to monetize the potential inherent in cloud-native networks, they must simplify the interface for developers. In an open API ecosystem, telcos, in general, will sell their network APIs to developers, either through their own platforms or via aggregators or hyperscalers. And then some aggregators might be aggregating APIs coming from another aggregator. This, Buckland pointed out, is quite complicated.

"You'd be a fool not to be in favor of this, but you'd also be a fool... to ignore the commercial and human friction that's going to be added," said panelist David Rolfe, head of product marketing at Volt Active Data. He explained that a complex chain of developers and aggregators makes it difficult to assess which vendor is responsible when things go wrong, and so guaranteeing quality of service becomes a challenge. As a result, extensive monitoring and diagnostics will be critical so ensure that you understand what's not working and why it's not working. A lot of the time, he continued, will be "simply the system watching itself."

But whose job is it to do this observation? "If I've got a downstream customer saying, 'Hey, my app isn't working.' Who investigates? Who owns the problem?" Rolfe continued. "You can have layers and layers of people in between you and that could actually undermine the commercial success of this if we … don't have clear chains of accountability and clear ways of handing off responsibility."

EMMA BUCKLAND
Principal Analyst,
STL Partners

DAVID ROLFE
Head of Product Marketing,
Volt Active Data

ANIL KOLLIPARA
VP of Product Management, Test and Assurance, **Spirent**

JORIT KRONJEE
VP of Engineering and Platform Development, **KORE Wireless**

ENSURING NETWORK CAPABILITY

The network must also be capable of responding to the request of the API. "Features like … dynamic slicing, you want to make sure that even before you open this up to the market, you have these underlying functionalities that a 5G SA core is supposed to provide," said Anil Kollipara, VP of product management, test and assurance at Spirent Communications. "Take … latency as an example. The network APIs, because it's an API, either the requester can request variable metrics or variable levels of latencies through profiles, so you want to make sure that your network can support 30-millisecond latency, right? There's a performance aspect purely from a quality of service… perspective. You want to make sure that your network is ready to handle those kinds of requests."

Rolfe agreed: "If you're going to offer quality of service, you damn well better be able to deliver it ... there has to be measurement, it's almost meta-APIs may be needed to monitor the performance of the API and who's using it, and how it's being used," he stated.

NOËL WIRZIUS
Product Lead,
Deutsche Telekom

HEIGHTENED SECURITY RISKS

KORE Wireless' VP Engineering and Platform Development Jorrit Kronjee told event attendees not to forget about the security risks opening up APIs presents. "You need to think about potential denial-of-service attacks, but you also need to think about what kind of data may I be leaking inadvertently through this API," he said. Therefore, he continued, telcos must be thinking seriously about security as open APIs is new territory for them, even if they already have a good approach to network security in general.

Basically, in an era of open APIs, API security issues typically seen in the enterprise space — denial-of-service attacks, distributed denial-of-service attack, man-in-the-middle attacks, and so on — are now applicable to the telecom networks. "API management solutions would have to be rolled out and plenty of security testing before things become public," Kronjee argued.

BUT THE BIGGEST RISK OF ALL? MISSING OUT

This isn't to say that there aren't critical opportunities for telcos in open APIs. Noël Wirzius, who is the product lead of network APIs Camara and Open Gateway at Deutsche Telekom, shared that interest in leveraging APIs into the cellular network is, in fact, quite widespread. Specifically, the carrier is seeing traction in the automotive industry, where there is a growing focus on what 5G SA can bring to the future generation of cars. Streaming companies and manufacturers also top the list, he added. "It's really, really big focus," he said. "It's not like one area of customer, one type of customer. I think it's really nearly every industry can be covered with this API… it's really hopefully everywhere in the future."

Kollipara added: "You lose a 100% of the shots that you don't take, so the biggest risk in my opinion is losing out on the opportunity … We've had wounds from the past; we've lost a lot of revenue in the telco industry to the outside players, so the biggest risk in my opinion is not taking the opportunity."

(Image courtesy of 123.RF)

HOW CAN TELCOS ENSURE RESILIENCY AT THE EDGE?

EDGE RESILIENCE, ACCORDING TO VOLT ACTIVE DATA'S CHIEF PRODUCT OFFICER DHEERAJ REMELLA, IS A 'MULTI-PRONGED ENDEAVOR'

While Application Programming By utilizing edge technology, telecom operators can improve their own operations and enable new applications and use cases; however, the edge must be close to the premises in order to deliver low latency.

Further, managing, securing and backing up multiple edge locations is no small task. Panelists discussed how telcos and their partners can ensure that their edge locations remain resilient as they continue to evolve and scale their edge efforts.

First things first, said Volt Active Data's Chief Product Officer Dheeraj Remella, you cannot run all of your resilience in the same edge because it's a constrained environment. "It defeats the purpose of resilience because [if] the edge location goes, your resilience [on that edge] goes," he continued. "So, how do you actually transfer from edge to edge and be able to transfer the control from a downed edge to a nearby edge peer, so to speak?"

Another challenge, according to Remella? Moving assets. "If assets are moving, how do you determine which edge is the closest to a given asset? … How do you control that asset's home edge versus roam edge?" he questioned.

Edge resilience, then, is a "multi-pronged" endeavor. "It's hardware, software, data center people, processes. It's a comprehensive view that you need to … plan for," Remella said. A possible example of such a plan might be an "archipelago architecture" in which nearby edges back each other up, with "clusters" of geographically distributed archipelagos that form "the resiliency basis" for your edge network.

DHEERAJ REMELLA
Chief Product Officer,
Volt Active Data

RONALD WESTRATE
VP of CaaS Delivery,
KORE Wireless

RAVI SINHA
VP of TechDev and Solutions
Reliance Jio

YAMINA KELM
Product Manager Edge Computing
and Innovations, **Deutsche Telekom**

LEVERAGING ESIM AND MULTI-IMSI

At KORE Wireless, edge resiliency is established using the SIM or eSIM — a digital version of the physical SIM card. "We use … Multi-IMSI [Multiple International Mobile Subscriber Identities], which allows us in roaming [to have] multiple networks in a certain country," explained the company's VP of CaaS Delivery Ronald Weststrate. "That's one level of resilience. But also, these roaming sponsors that we use, we piggyback on their roaming agreements." He added that when an issue pops up with one of these roaming sponsors, KORE can use another sponsor. "So, it might not even be that a local network is down, but it might be that a roaming sponsor has an issue in the path back to our core network."

As such, KORE Wireless considers Multi-IMSI to be a "very important tool" for ensuring resiliency.

Weststrate further detailed a scenario in which an eSIM is used in combination with local profile management provides additional resiliency: "Imagine a truck … driving through the U.S. Let's say normally [it's] using an AT&T profile, very happy with that, and then you hit a blind spot… Then, locally, you can switch to a secondary profile already on the SIM. Of course, that might be Verizon or might be your global connectivity profile … So, you then have a secondary profile on the card to ensure you got resiliency."

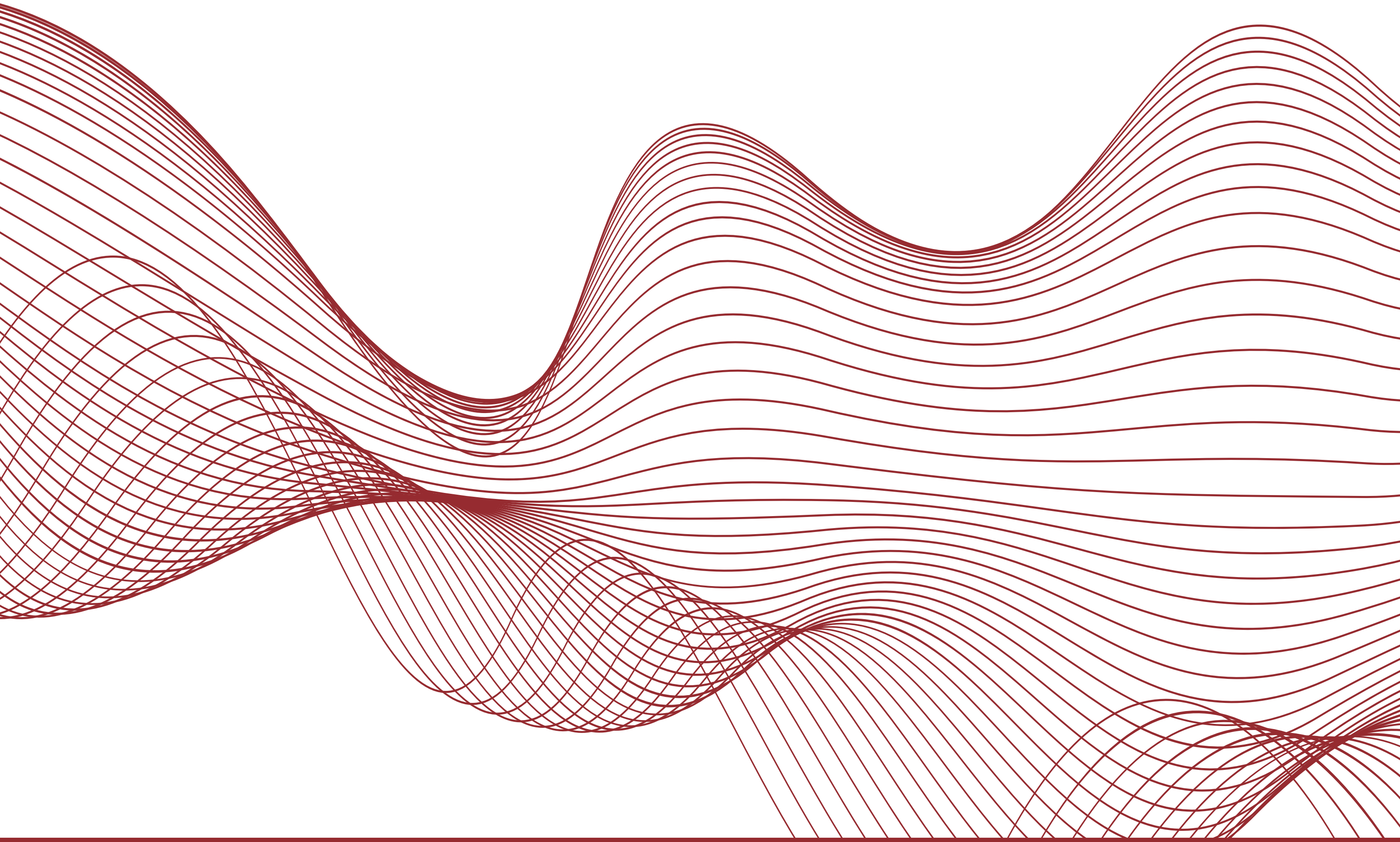
INTELLIGENT INFRASTRUCTURE

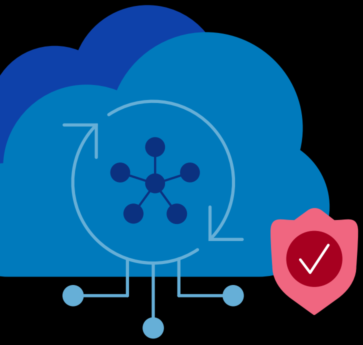
For Ravi Sinha, the VP of TechDev and solutions at Reliance Jio, the emphasis on resilience should be centered around the telco infrastructure itself. "That also includes my RAN pieces, that also includes my software modules [that] have RAN, that also includes the core modules or any kind of authentication model, whatever is needed … locally," he said, adding, though, that the economic restraints of communications infrastructure can sometimes compromise resiliency at the telco edge.

He also is hoping that in as little as two or three years to see artificial intelligence not just through the physical level stack and orchestration, but also in the end-to-end orchestration of the entire edge slice, from the code to transport to the RAN as well. And further, he hopes that this injection of end-to-end AI is done in such a way that "resilience is given a high priority."

A STRONG CLOUD-TO-EDGE CONTINUUM

Finally, Deutsche Telekom's Product Manager Edge Computing and Innovations Yamina Kelm claimed that in order to have a strong "fallback option" for your edge locations, it's critical to build a "strong cloud-to-edge continuum," where all network components feed into one another in an effective and efficient way. Part of achieving this is deploying the right solution is in the right place. "You ... need to distinguish what do you want to achieve when putting a workload on a specific infrastructure and in of how the application looks like and what the application needs, you need to decide which one's the best fitting for your purposes," she said.





Simplify hybrid and multicloud networking

Simplify network connectivity and security across public cloud, edge, and on-premises sites. F5® Distributed Cloud Services is a SaaS-based service that provides full-stack networking connectivity across distributed locations.

Simplicity

Reduce the number of tools required to connect and extend networks between clouds and on-premises data centers. Seamlessly integrate with existing cloud provider network constructs through automatic provisioning and orchestration.

Centralized Visibility

Centralize network and service performance observability across distributed public cloud and on-premises locations. Easily identify issues before they become disruptive for faster remediation.

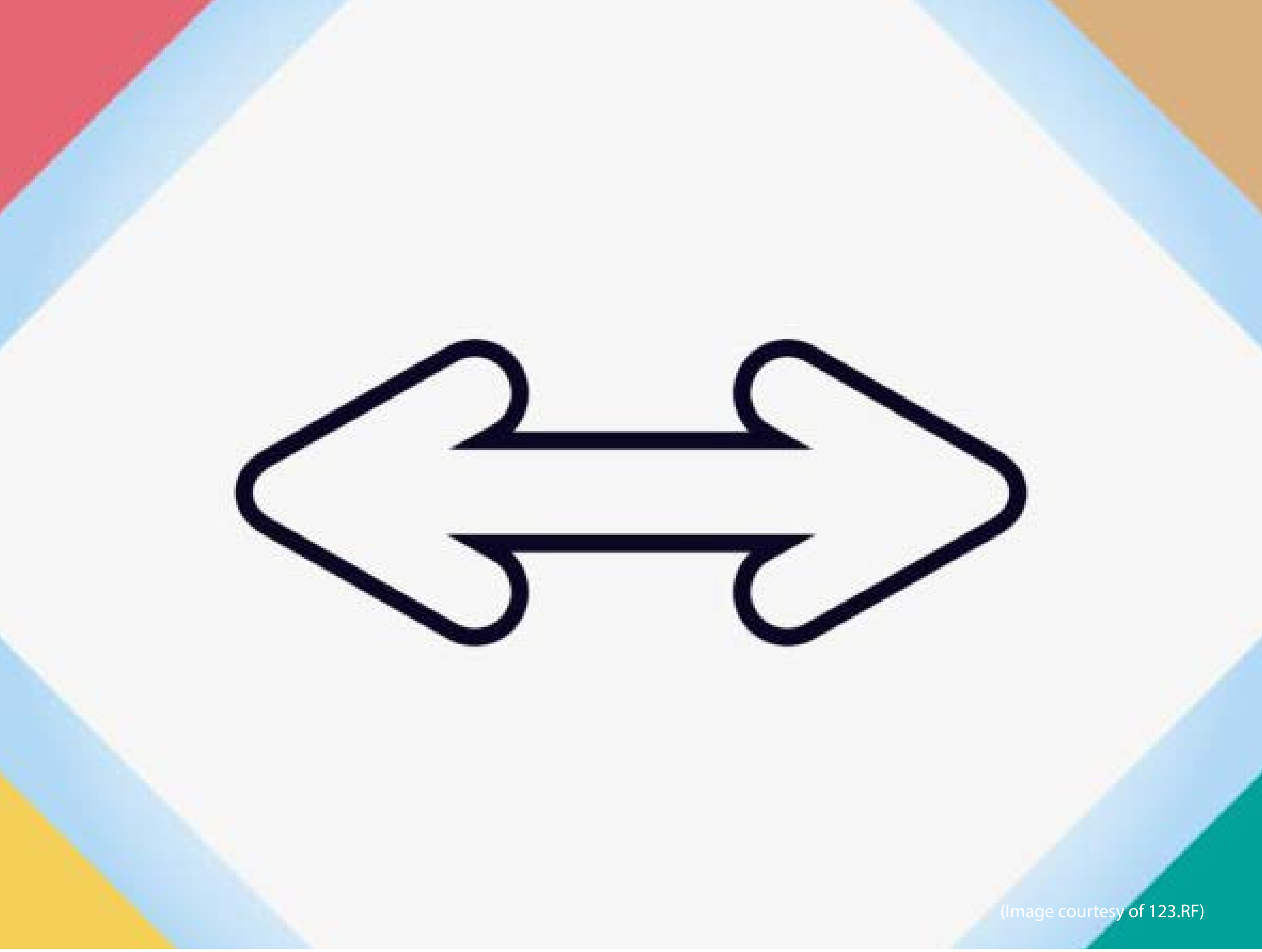
Increased Agility

Accelerate time-to-service for new application deployments by eliminating manual ticketing processes and one-off provisioning for network services.

Improved Security

Integrate network and application security across hybrid and multicloud environments, with consistent policy enforcement eliminating risks of business downtime and exposure to Internet threats.

Learn more about F5 solutions for secure multicloud networking at f5.com/multicloud



(Image courtesy of 123.RF)

ACHIEVING END-TO-END AUTOMATION IN A MULTI-CLOUD ENVIRONMENT

QUALITY DATA, DIGITAL TWINS AND AI/ML WILL HELP OPERATORS

ENABLE END-TO-END AUTOMATION IN A MULTI-CLOUD WORLD

Managing the complex components of a multi-cloud environment is proving to be a monumental challenge for network operators, especially coupled with the growing need for automation techniques driven by AI and ML to streamline operations.

GABRIELA STYF SJÖMAN
Managing Director, Research and Network Strategy
BT Group

However, as Viavi Solutions' Regional CTO Chris Murphy explained, it's more than worth it for operators to overcome these hurdles because the opportunities around end-to-end automation in a multi-cloud environment are "wealthy."

Murphy was joined by BT Group's Managing Director of Research and Network Strategy Gabriela Styf Sjöman, who was able to provide the telco perspective. Automation is nothing new, she said, but added that now, the operator is starting to "expand" its use of this capability throughout the "telco cloud environment" in a way that is more "horizontal."

"We're doing … more horizontal automation. Where we predominantly are exploring all of these opportunities, and … use[ing] AI for performance optimization, power tuning, assurance," she continued. "We're doing quite a lot around anomaly detection, and we're using this across all our domains, both in the fix and the mobile network today."

Styf Sjöman was adamant that a cloud-native, decoupled network is "critical," particularly because it is the only way to enable what she called "auto-healing."

"Today in the telco world, even when it's cloudified, many of our services are hardcore integrated down to the infrastructure… Even when we cloudify, we still have these silo stacks. And then you cannot have the network doing it by themselves … [T]o be able to do … this auto healing … you need [to be] truly cloud-native. Even the applications need to be cloud native, the CNFs need to be truly cloud-native," she argued.

For Murphy, digital twins also are key to enabling end-to-end automation in a multi-cloud environment: "Digital twin is emerging as a very powerful enabler for this sort of thing because it allows you to model your network, not just simulate it, but represent it as something which is a proxy for reality, which means you can run what if scenarios, you can understand where your weaknesses in your network," he said.

DON'T MOVE THE DATA!

Another important consideration in this discussion, according to both experts, is data: where to put the data, how to get the data, what to do with the data and so on. All of these decisions require a great deal of consideration. "Not all data is the same," noted Murphy, adding, therefore, you must be "careful that data is collected correctly" as it can be subject to human error.

Styf Sjöman also warned against moving data. "Data should not be moved around. Instead, we have to be able to kind of abstract that data and create a layer, democratize the data, but we feel that moving around data and putting it somewhere is not the way to go," she explained further. "It's very costly, probably doesn't add a lot of value, but then that's where we are, and I think [it's] still up for discussion."

In general, Murphy agreed with this sentiment, commenting that data will be "very, very location specific" in most circumstances and so it's "most relevant to where it's being generated," suggesting that we shouldn't be "hauling it around."

"Because we need to achieve the end-to-end intent-driven automation and autonomous networks … we do need models to help us to drive the AI to do that because we can't do it manually, particularly if we've got infinite network slices … and we do need the quality of data," stated Murphy, adding though, that the industry must approach data generation and analytics with caution, as well as how emerging technologies are being used.

CHAS LESLEY
Senior Solutions Engineer
F5

F5, he continued, has a "balanced" edge computing model, in which its global network delivers applications with telco tie-ins, but it also pushes those workloads out to the customer edge, whether that is remote sites, remote data centers, remote branches or offices. "We can actually push [and] run applications closer to the client, closer to the consumer, wherever they may be," he said, adding that the balance of centralized control and presence at the edge is "critically important in how [the company] get[s] applications closer to consumers."

However, for F5, it's not just about delivering these applications at the edge, but it's also crucial to secure them once they're there. "Being able to layer in different security offerings as we deliver those applications, those API endpoints, that enable us to get resources to the edge as we've been talking about, is quintessentially important," he explained. "Be able to offer the same security in an IoT form factor as maybe we were doing in a public cloud connectivity model, if you will, or a telco facility or tier one data center."

He added that when providing edge security, F5 aims to be "consistent" and deliver analytics and visibility, and driving both through automation. "We want to … make that an automatic journey in terms of being able to deploy quickly, be very agile," he said.

F5 makes this possible because of what it does in its compute stacks. "This is where we get into SaaS-based controls, what we do in our global network architecture to deliver this security, but also at the customer edge, at the IoT edge, being able to use small form factor hardware appliances that have integrated connectivity services, but being able to run those services in a form factor like a node … in terms of getting resources out to the edge and being able to extend the same level of security services, delivery services that we do in our global network," he said, explaining further that the company does this at the edge via mesh services, where its networking and security stacks tie in and deliver services, but also offer multi-tenant distributed Kubernetes models to deliver applications in additional to that network connectivity.

He called this model "hugely powerful" and shared that F5 is seeing a lot of traction across in the market from modern manufacturing to medical care facilities.

Finally, Lesley spoke of the importance of ensuring ecosystem visibility across a multi-cloud network. Doing so, he said, enables "pipeline control" for providers as they modernizing their ecosystems. "We're doing infrastructure as code, we're doing networking, more networking as code in terms of what we're looking at in deployment models, being able to tie directly in and automate that fleet of services, if you will, at the edge," he said.

And while that's happening, he continued, there should be a "very rich context of telemetry" where it's possible to not only see how the networks are performing in terms of flows and other performance metrics, but also at the environments from an application performance standpoint. "We talked about the concept of anywhere at the beginning, being able to say, well, I have a fleet of services at maybe my retail edge, or I have a fleet of services that are backhauled at the public cloud, there's API frameworks or having other connectivity models that support application architectures," stated Lesley. "Being able to see how the services are responding across those ecosystems is incredibly important."

FIVE CORE NETWORK DESIGN CONSIDERATIONS FROM 5G TO 6G

The evolution from 5G to 6G core networks includes new requirements for AI, interoperability, positioning, sensing, sustainability and more

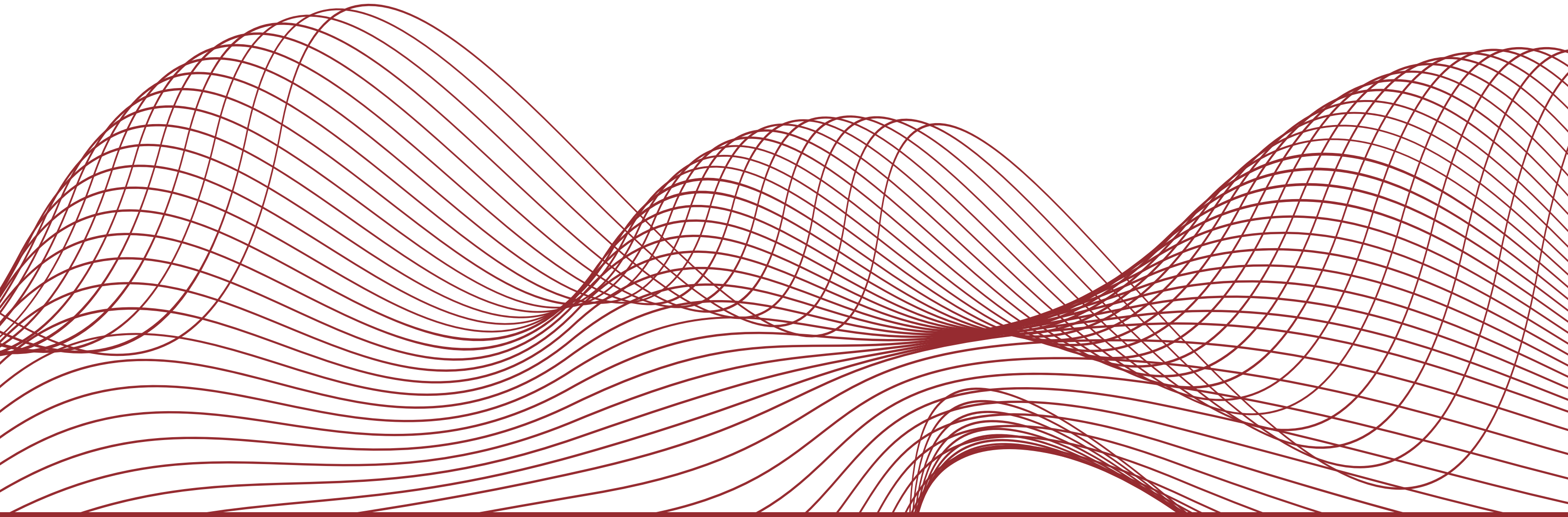
The current emphasis on bringing cloud-native technology and operating principles into 5G—with the move to a Standalone 5G architecture and cloud-native 5G core the next major transition—will inform how 6G is designed, standardized and deployed. Beyond a number of 5G core enhancements that will go into 6G, the next generation of cellular will also include a number of new requirements.

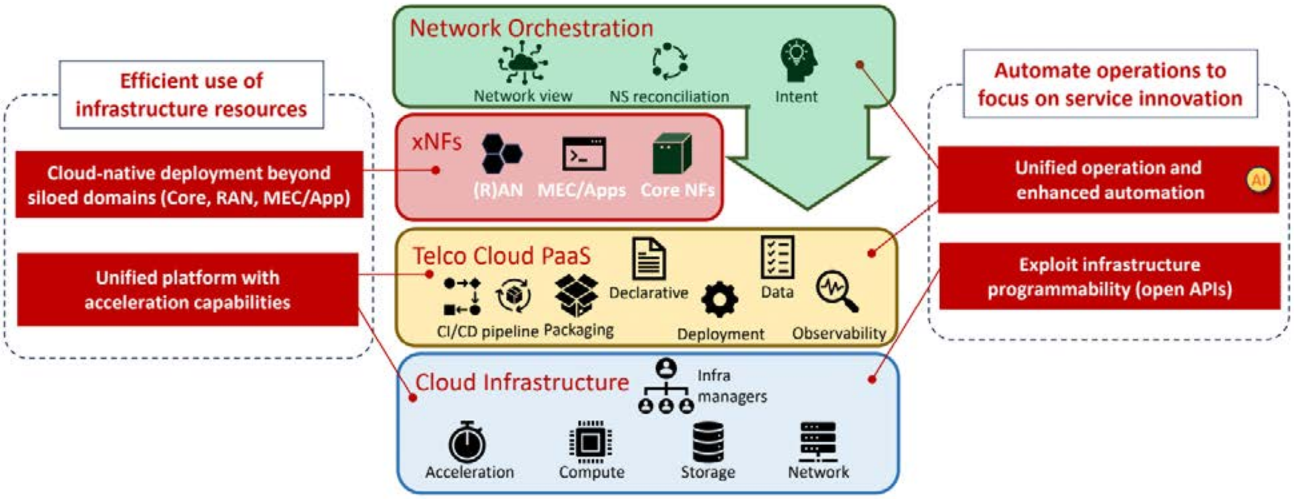
Riccardo Guerzoni, director of the core network group at Docomo Euro-Labs, laid out the path from 5G to 6G with an emphasis on core network considerations. He focused on five design considerations that, broadly speaking, speak to infrastructure/platform and 3GPP architectural perspectives.

An overarching point, according to Guerzoni is that 6G, and the enhancements and new requirements that will come with it, need to be aligned with the economic reality operators are facing and need to deliver a clear return on investment. "These new requirements for beyond 5G are challenging in terms of environmental sustainability, which means energy efficiency, hardware longevity and economic viability," he said.

RICCARDO GUERZONI
Director, Core Network Group,
Docomo Euro-Labs

"These innovative services that are expected in the 2030s that required enhanced performance of the network and new functionalities, and that must be justified in terms of return of the investment. So the point is how to make these new services that are very demanding economically viable."



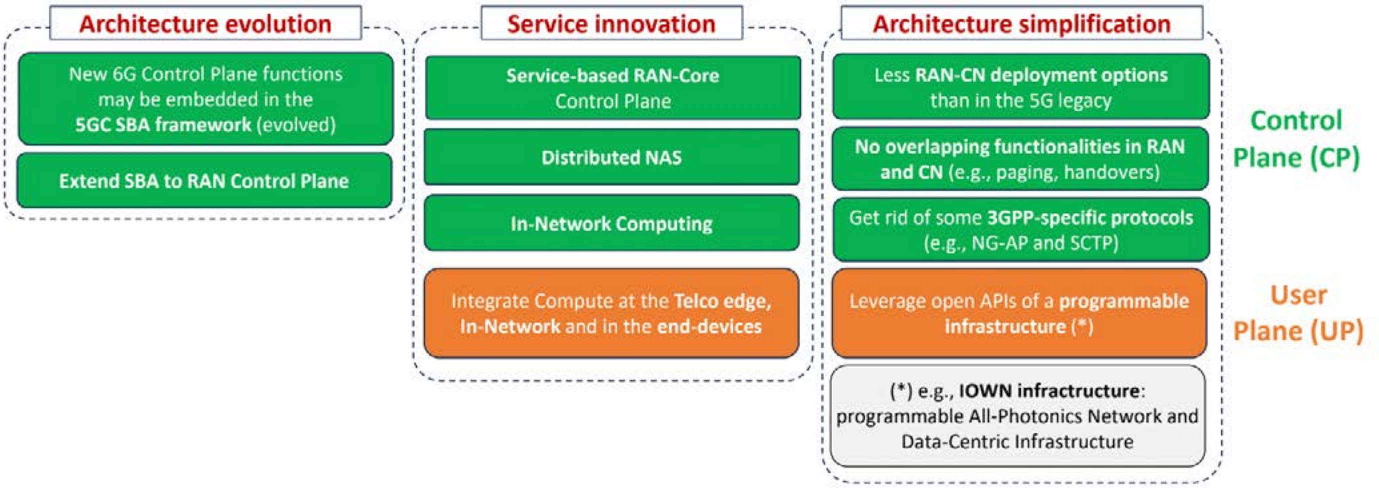

Efficient use of infrastructure resources
Cloud-native deployment beyond siloed domains (Core, RAN, MEC/App)
Unified platform with acceleration capabilities
Network Orchestration
Network view
NS reconciliation
Intent
xNFs
(R)AN
MEC/Apps
Core NFs
Telco Cloud PaaS
CI/CD pipeline
Packaging
Declarative
Deployment
Data
Observability
Cloud Infrastructure
Infra managers
Acceleration
Compute
Storage
Network
Automate operations to focus on service innovation
Unified operation and enhanced automation
AI
Exploit infrastructure programmability (open APIs)

(Image courtesy of Docomo Euro-Labs.)

The first set of considerations articulated by Guerzoni speak to the infrastructure/platform piece. **Efficient use of infrastructure resources** contemplates cloud-native deployment that dispenses with legacy silos, e.g. core, RAN, mobile edge computing and network applications, and a unified underlying platform with acceleration capabilities. Then, **automated operations that enable service innovations** covers unified automation and operations, and explaining infrastructure programmability via network APIs.

"There is a cloud infrastructure with the telco cloud platform as a service built on top of it, and that's the enabler for a unified platform with acceleration capabilities," Guerzoni explained. "So acceleration capabilities are important to deploy not only the core network functions like it is in 5G, but also run components [like open distributed units]... And also applications. So the idea is that these acceleration capabilities will be used not only to host RAN components, but also application-related components that can be provided by the operator itself, or also on behalf of third parties."

He continued: "And at the same time the standardization of equipment that's been done as an example in that particular case on COTS servers sort of allows for the operators to ride the commodity curve down and basically help reduce capex. Now at the same time, Intel is doing its part to help improve TCO and we recognize that vendor interoperability is still underway and it's going to take some time for the ecosystem to get more mature and we are helping to contribute towards that. And in fact we've been deploying now three generations of equipment as well as offering blueprints that help improve g -to market for a number of these service providers. And in every generation of these deployments we have increased capacity by offering better compute, reduced power very considerably and increased the density on the Ethernet side."


Architecture evolution
New 6G Control Plane functions may be embedded in the 5GC SBA framework (evolved)
Extend SBA to RAN Control Plane
Service innovation
Service-based RAN-Core Control Plane
Distributed NAS
In-Network Computing
Integrate Compute at the Telco edge, In-Network and in the end-devices
Architecture simplification
Less RAN-CN deployment options than in the 5G legacy
No overlapping functionalities in RAN and CN (e.g., paging, handovers)
Get rid of some 3GPP-specific protocols (e.g., NG-AP and SCTP)
Leverage open APIs of a programmable infrastructure (*)
(*) e.g., IOWN infractructure: programmable All-Photonics Network and Data-Centric Infrastructure
Control Plane (CP)
User Plane (UP)

(Image courtesy of Docomo Euro-Labs.)

As it relates to the 3GPP-defined architecture, there are three primary considerations:

- **Architecture evolution**—new 6G control plane functions potentially embedded in an evolved 5G core service-based architecture framework, and extending the service-based architecture to the RAN control plane.

- **Service innovation**—a service-based RAN/core control plane, distributed non-access stratum, in-network computing, and integration of compute at the telco edge, building on compute in-network and on-device.

- —fewer RAN/core deployment options, no overlapping RAN/core functions like paging and handover, removing some 3GPP-specific protocols like NG-AP and SCTP, leveraging the programmable infrastructure, and programmable all-photonics network and data center infrastructure.

"Regarding the extension of the SBA architecture defined for 5G to host the 6G control plane functions, the figure [above] shows a possible perspective that can be used as an approach in the 3GPP standardization, where 6G core network functions and 6G RAN controlpPlane function could be hosted in the same 5G SBA framework, enhanced of course," Guerzoni said. "The enhancement is necessary if we consider that currently the 5G core functions are deployed in a centralized cloud, while if we involve the SBA framework also functions at the edge, like RAN control plane functions, then we need to potentially make the protocol stank more resilient."

He also pointed out that with 6G "there is no Non-standalone option...That's a lesson learned from the 5G experience...The 6G RAN is only integrated with 6G core network functions, and it doesn't interact directly with the 5G core network functions. And the interworking is realized by means of service-based interaction between the 5G core and the 6G core."

Drawing from the cloud-native descriptor applied to 5G, 6G is often characterized as AI-native. Speaking to this point, Guerzoni said, "AI capabilities can be embedded to make more efficient the network... functionalities. And reduce the energy consumption, optimize the control plane behavior, quality of experience, quality of service, and so on and so on. So there will be AI models embedded in different part[s] of the network, and this is of course a big opportunity but it's also a challenge from the mobile network operator point of view because these [machine learning] models need to be managed in order to build the models, deploy them, monitor the performance, make them controllable, train and evaluate the models. So this is a quite important topic for our mobile network operators—how to make controllable and observable these ML models that are deployed in the different parts of the network."

Featured Companies

F5

F5’s portfolio of automation, security, performance, and insight capabilities empowers our customers to create, secure, and operate adaptive applications that reduce costs, improve operations, and better protect users. **Learn more.**

KORE

F5 is a hybrid and multi-cloud application services and security company committed to bringing a better digital world to life. F5 offers a comprehensive suite of solutions for network and IT uses cases that makes it easy to meet any challenge. From cloud-native infrastructure deployments, mobile or fixed-line subscriber services, security solutions for network and IT infrastructure that address scale and performance, and front office security measures that stop digital fraud. **Learn more.**

Spirent

Spirent provides innovative products, services, and managed solutions that address the test, assurance, and automation challenges of a new generation of technologies from the lab to the real world, including 5G, SD-WAN, Wi-Fi, O-RAN, cloud, autonomous vehicles, and beyond. **Learn more.**

VIAVI Solutions

VIAVI is a global provider of network test, monitoring and assurance solutions for telecommunications, cloud, enterprises, first responders, military, aerospace and railway. VIAVI is also a leader in light management technologies for 3D sensing, anti-counterfeiting, consumer electronics, industrial, automotive, government and aerospace applications. **Learn more.**

Volt Active Data

The Volt Active Data Platform enables companies to unlock the full value of their data and applications by making it possible to have scale without compromising on speed, accuracy, or consistency. Based on a simplified stack and an ingest-to-action layer that can perform sub 10-millisecond decisioning, Volt’s unique, no-compromises foundation gives enterprises the ability to maximize the ROI of their 5G, IoT, AI/ML, and other investments, ensure “five 9’s” uptime, prevent fraud and intrusion, deliver hyper-personalized customer engagement, and save on operational costs. **Learn more.**