A SPIRENT E-BOOK

Open RAN – An Introduction

Contents

Why Open RAN?

Describing what Open RAN is (which we'll do shortly) is important, but probably more important is describing why Open RAN was created. We'll start there because it is easier to understand what Open RAN is if we first know why it is being built.

The bulk of the costs (CapEx and OpEx) for operators lie within RAN, and 5G requires a massive increase in the number of cell sites and radio types, which drives RAN costs even higher. In recent years, the number of RAN vendors has declined, reducing competition in the market.

Open RAN (O-RAN) attempts to solve this problem. By disaggregating and splitting the RAN, supporting standardized open and interoperable interfaces, and allowing key functions to run as virtualized software functions on vendor-neutral hardware, an environment evolves where networks can be deployed with a more modular design. This offers the option of not being dependent upon a single vendor and, in turn, provides multiple benefits.

O-RAN vs. OpenRAN vs. vRAN

No discussion of the Open RAN (O-RAN) technology movement is complete without the context of virtual RAN (vRAN). Both O-RAN and vRAN are technological approaches. Instead of the traditional RAN, which is supplied by a single vendor using proprietary hardware and software, both O-RAN and vRAN are technology approaches that differ from the traditional RAN, which is supplied by a single vendor using proprietary hardware.

Open RAN is focused on opening proprietary protocols and interfaces between the various disaggregated RAN subcomponents to drive multivendor radio, hardware, and software deployments. vRAN is similar in that it is focused on decoupling RAN software features from custom-built hardware platforms to enable proprietary software to run on generic hardware compute platforms.

Specific aspects of Open RAN include:

The O-RAN Alliance: The organization focused on publishing specifications for a new Open RAN for 4G and 5G. The organization is also focused on facilitating the testing of new O-RAN devices.

OpenRAN: OpenRAN is a standard led by the Telcom Infra Project (TIP). It aims to "accelerate innovation and commercialization in RAN domain with multi-vendor interoperable products and solutions that are easy to integrate in the operator's network and are verified for different deployment scenarios." It is committed to creating an Open RAN for 2G, 3G, 4G, and 5G.

In practice, there can be an overlap between Open RAN and vRAN. The reality is that this is not exclusively an "either/or" approach, but one where "the whole can be greater than the sum of the parts," with some experts suggesting they are destined to inevitably combine.

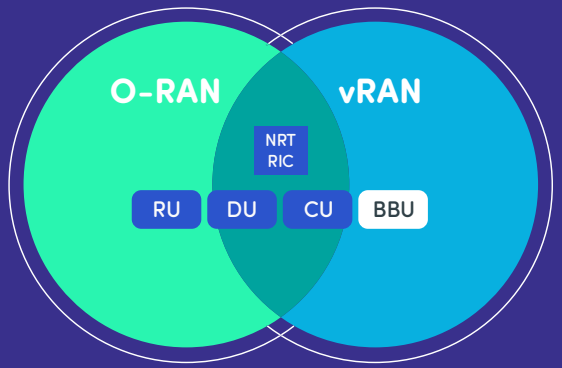


FIGURE 1

Open RAN Overview: A high-level description of Open RAN would include the following...

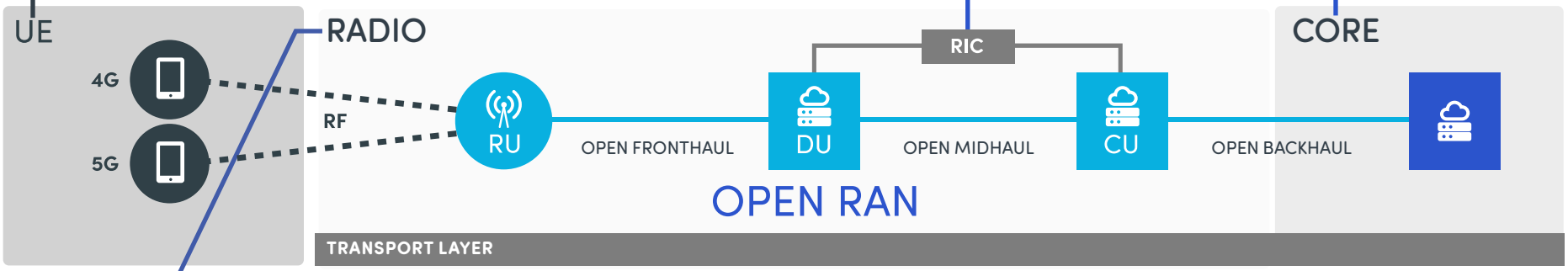
UE (User Equipment)

These are the endpoints connecting to the network. It could be smartphones, but it is increasingly including next-generation endpoints, such as IoT devices (ATMs, factory equipment, smart meters, etc.). These devices communicate with the network via radio frequencies (RFs) connected to RUs (radio units), which are geographically dispersed to be near the user.

RAN Intelligent Controller (RIC) is a hosting platform for micro-service-based software applications. Servicing both real-time and non-real-time (RT and non-RT) platforms, RIC provides a disaggregation of RAN orchestration, automation, management, and optimization through open interfaces.

CORE

The mobile core network enables end-users access to services (phone calls, internet access, etc.). It also handles operational tasks such as subscriber location, profile and authentication of services. Finally, it provides switching functions for voice and data sessions.



RADIO

This is where radio signals from end-user devices are converted to digital signals for the network or vice versa. This transport segment handles transforming the radio signal from the user equipment into a digital packet that can run across the core network.

RU (Radio Unit).

These RF transceivers are part of the base station, co-located with the antennas that capture inbound (or transmit outbound) signals from (or to) end-user equipment.

The RU is where the radio frequency signals are transmitted, received, amplified, and digitized. The RU is located near, or integrated into, the antenna.

DU (Distributed Unit).

The DU is where the real-time baseband processing functions reside. The DU can be centralized or located near the cell site and works with the lowest layers of the protocol stack (RLC, MAC, and physical layer). This is commercial off-the-shelf (COTS) hardware, which can also be virtualized or containerized. It consolidates and processes inbound traffic from, or processes, breaks out, and distributes traffic to, multiple RUs.

The processing performed by DUs is beyond the scope of this eBook, but it is important to note that the segment comprised by the RUs, the DU, and the transport between the two is collectively called the fronthaul. Notably, O-RAN calls this the lower-layer split (LLS).

CU (Centralized Unit).

The CU sits between the DUs and the core network. The CU handles the higher layers of the protocol stack, where the less time-sensitive packet processing functions typically reside (SDAP, RRC, and PDCP). A single CU handles many DUs.

Open DU and CU can be run as virtualized software functions on vendor-neutral hardware. CUs are also virtualized and run on inexpensive COTS hardware.

The transport layer, which handles end-to-end communication over the Open RAN network, is split into three communication links:

Open Fronthaul. The RU, DU, and transport between the two, including the use of the enhanced common public radio interface (eCPRI), comprise the open fronthaul.

Open Midhaul. The DU, CU, and transport between the two comprise the open midhaul.

Open Backhaul. The transport between the CU and the mobile core network comprises the open backhaul.

Much of the above is virtualized, runs on COTS hardware, and uses open interfaces in an Open RAN environment, including RIC and CORE.

Benefits of Open RAN

Delivers lower costs for vendors and operators.

More vendors = more competition. And increased competition drives prices lower. In addition, virtualizing the various components of RAN allows operators to utilize COTS hardware, which further lowers costs.

Provides the ability to serve smaller, tightly defined 5G networks.

By lowering RAN costs, providers can service more cost-sensitive 5G network use cases, such as rural markets or private commercial 5G networks (e.g., at a factory site). A big driver for cloud service providers (CPs) is traditional macrocellular network coverage.

Spurs innovation and accelerates time to market.

Increased competition naturally speeds up innovation. Virtualizing RAN systems means innovation can be implemented in software, which is quicker to deliver than hardware changes. As traditional RAN continues to innovate, it promotes greater O-RAN participation, thus spurring innovation further. Within this dynamic environment, more and newer players will independently innovate and provide richer solutions at a much faster pace, thereby reducing the time to market for new offerings.

Facilitates new monetization opportunities.

Open RAN will help stimulate a vibrant vendor ecosystem, quickly delivering new services to customers, reducing the risk of "vendor lock-in" and introducing "best-of-breed" network solutions and thereby facilitating new monetization opportunities.

The benefits of Open RAN are clear and compelling, with the promise of lower costs, diverse supply chains, and gear interoperability. However, building a new O-RAN from the ground up and ensuring it performs as planned is a massive undertaking—especially when coupled with a move to 5G, which is already pushing technical boundaries. With this background, we will examine precisely what O-RAN is.

KEY TAKEAWAY

The benefits of Open RAN are clear and compelling, yet building a new O-RAN from the ground up, and ensuring it performs as planned, is a massive undertaking.

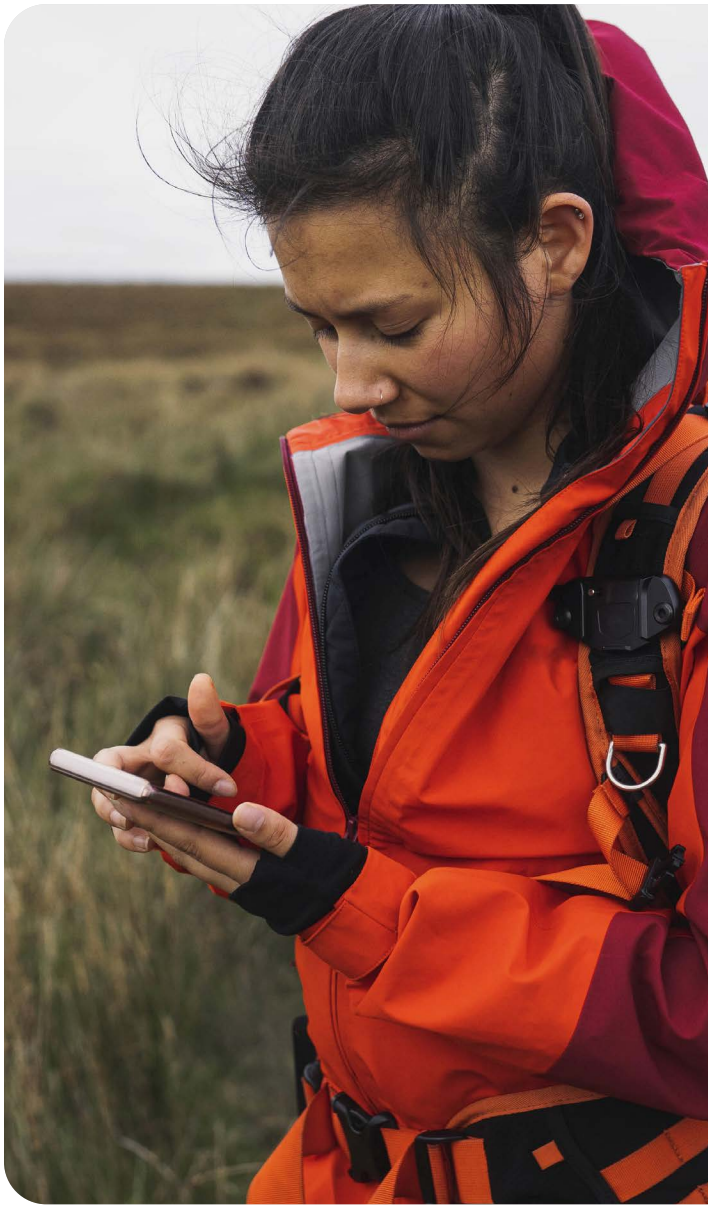


FIGURE 2

The Flexibility of Open RAN: Disaggregating RAN affords tremendous flexibility to network architects.

Deployment Topologies

Split 7.2x & 2

Disaggregated

Co-Located RU/DU

Co-Located DU/CU

The standards bodies have defined "splits" that allow the RU, DU, and CU to be flexibly distributed or centralized in a variety of ways to meet operators' business requirements or address local constraints such as transport costs and distance to edge clouds for rural sites. For example, the DU can be co-located with the CU, or the DU can be bundled with the RU. The DU can also run standalone. This flexibility allows architects to address a wide variety of use cases.

Frequency Support

4G

Low (MHz)	Mid (MHz)
200-300	1800-2600

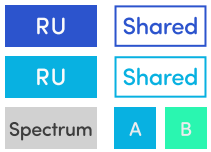
5G

Mid (GHz)	High (GHz)
3.3-4.2	26-39

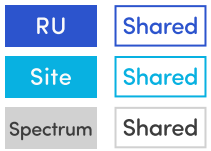
To support the frequencies used by both 4G and 5G, operators require Open RAN to support a wide range of frequencies with various transmission modes, output power values, and bandwidth requirements.

RAN Sharing

MORAN



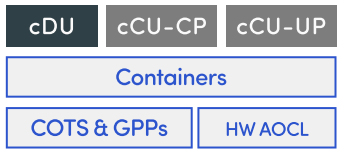
MOCN



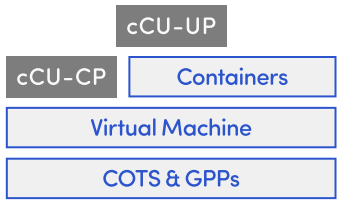
There are two standards that allow operators to share a RAN – MORAN (Multi-Operator Radio Access Networks) and MOCN (Multi-Operator Core Networks). Both are required for Open RAN. With MORAN everything in the RAN except the radio carriers is shared between two or more operators. With MOCN, two or more core networks share the same RAN, meaning the carriers are shared. The existing core networks could be kept separate. MOCN allows operators to pool their respective spectrum allocations for greater efficiency.

O-Cloud Architectures

Containers

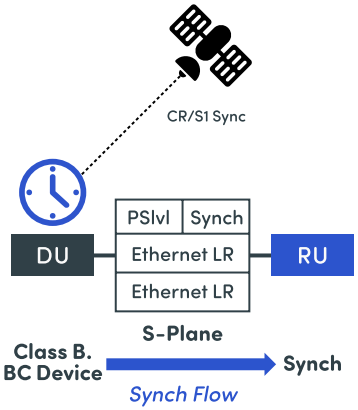


Virtual Machines



Open Cloud (O-Cloud) implementation will be based on general-purpose processors (GPPs) and hardware accelerators supporting an acceleration abstraction layer (AAL), all ideally running on containerized network functions (CNFs) on bare metal or virtual machines.

Synchronization Profiles



Loss of synchronization is a challenge with disaggregating RAN (especially with multiple vendors). To maintain critical synchronization performance in networks with greatly varying deployment scenarios, Open RAN provides a set of defined synchronization configurations from which to choose that also reference associated profiles and standards from IEEE and ITU-T to help inform robust implementations.

The Challenge of Making Open RAN Work

The promise of Open RAN is clear: lower costs, faster innovation, and new monetization opportunities. But there are also significant challenges the industry must address while building out Open RAN.

In a recent poll, Spirent asked providers what the biggest challenges for Open RAN were in the near term. Responses fell into four main categories:

Maturity.

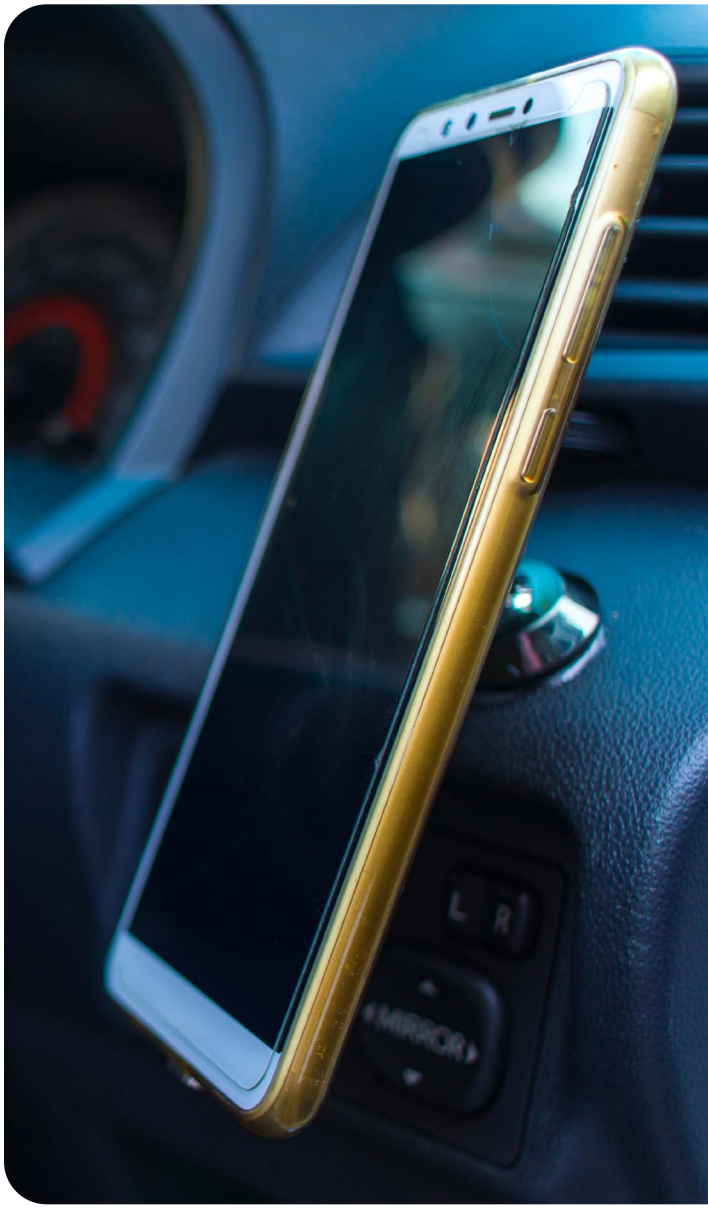
There are concerns about multi-vendor interoperability. The standards are not 100% complete. Worries persist that, in the rush to bring Open RAN to market, some vendors will forge ahead with their own proprietary flavor of Open RAN, which will involve the need for heavy systems integration to make the multi-vendor products work in harmony.

Providers were also concerned about the performance and robustness of Open RAN in live deployments. They were unequivocal that Open RAN must have parity with traditional RAN. A common fear they voiced was losing synchronization, as the RAN was disaggregated, moved to different locations, and comprised of disparate vendors.

Security Risk.

The combination of disaggregation and introducing multiple vendors expands the threat surface. This requires adding security safeguards throughout the Open RAN. The fear is that this added security overhead will offset potential cost savings.

Included in this assessment is the perception that many of the new, smaller vendors appearing in the new Open RAN landscape will not provide bulletproof 24x7 support. Consequently, the realization is growing that service providers may need to provide that support on behalf of smaller vendors.



Costs.

Installing and operating Open RAN will be significantly more complex and time-consuming compared to traditional RAN. And, just like security, not all the newer, smaller vendors will be up to the integration task. An emerging view is that large system integrators (SIs) or even service providers may need to intervene as the overall integrator. The fear is that expense from such a model may offset Open RAN cost savings.

Operational readiness.

This represents another barrier to entry for SPs, as they must own the operational and automation/DevOps aspects of Open RAN. This is a new high-requirement capability, with numerous complexities and requirements for knowledge, technical capabilities, and qualified expertise for them to gain in a compressed period.

KEY TAKEAWAY

Open RAN has the potential to deliver game-changing value across the telecom ecosystem, but rapid uptake will hinge on addressing concerns about maturity, costs, security risks and operational readiness. Early adoption has delivered key advantages to organizations in previous technology trends.

O-RAN Adoption— Keeping an Eye on the Prize

Some business leaders think Open RAN could be a game changer. They will assess its evolution, intent on avoiding business risk, and let the early adopters prove its value before they adopt.
The likelihood of Open RAN's success, however, is not in question. The issue of adoption timing, however, can be a defining factor in an organization's long-term success in the marketplace.

A case in point: The VoIP explosion.
Comparable disruptive changes provide a useful perspective. Similar underlying forces driving O-RAN resulted in the VoIP shift, which in less than 10 years flipped the traditional telephone switching market. As the market exploded and players like Microsoft Skype and Google bounded ahead, an accompanying consolidation resulted in a significant reduction in critical mass players. The VoIP shift favored companies that drove or joined the movement early. It is best to assume Open RAN's benefits are real and to identify the best strategies to adopt effectively sooner rather than risk being too far behind the wave.

Addressing Open RAN Testing Challenges

For Open RAN to achieve its potential and address the many stakeholder requirements and challenges, a comprehensive and proven testing and assurance strategy is key. To achieve accelerated Open RAN adoption, stakeholder confidence is critical.

FIGURE 3

Open RAN Ecosystem Testing Requirements

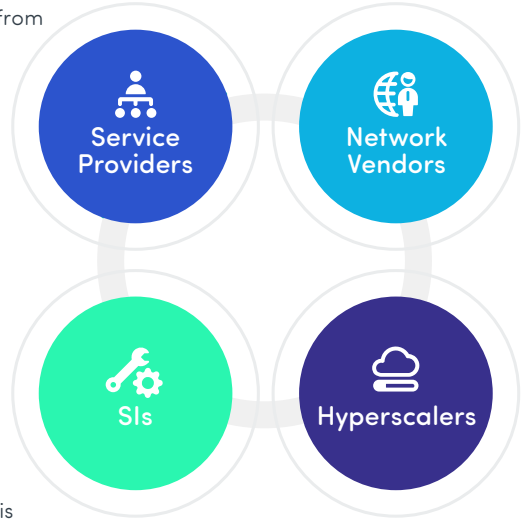
All players in the Open RAN ecosystem must perform rigorous testing to ensure compliance with standards, interoperability, performance, and scalability. In addition, members of the Open RAN ecosystem have a range of targeted test requirements:

Service Providers

SPs must test to ensure every component of their Open RAN environment performs as planned across the lifecycle, from development to operations, as they will be releasing new offerings at the network edge, launching private networks and expanding geographic coverage.

Network Vendors

Network vendors must ensure their components meet 4G/5G and Open RAN specifications, that these components interoperate with another vendor's components, and—once installed—they continue to operate as planned.



System Integrators

The job of ensuring Open RAN works, has sufficient performance and is robust, falls to the system integrator. To accomplish this, the SI needs a full suite of testing capabilities. This is not only for the initial installation, but also for assurance, as the Open RAN ecosystem operates in live deployment, and as a range of factors continually change.

Hyperscalers

Cloud vendors are positioning themselves to host cloud versions of Open RAN or vRAN. These technologies, however, have stringent latency and synchronization requirements that cloud vendors typically have trouble meeting. Therefore, hyperscalers must validate their cloud infrastructure to ensure they meet these standards. Demonstrating this requires objective, vendor-neutral testing. In addition, hyperscalers often act as the system integrator. In such cases, they have the same need for testing as all SIs.

Testing and Assurance for Open RAN

O-RAN must ensure it is robust, interoperable, performant, scalable, provides technical parity with traditional RAN, and is efficient to deploy, operate, and manage. Supply chains must be secure, as regulatory requirements for emergency services are met and new cost overheads are counteracted.

Areas of testing focus appear below. This is where automated testing and assurance play a pivotal role.

KEY TAKEAWAY

To realize success with Open RAN, a comprehensive and mature automated testing strategy must address performance across RU, DU, CU and the Core, while also accounting for security, conformance, interoperability, synchronization, and more.

FIGURE 4

Areas of Testing Focus for Open RAN

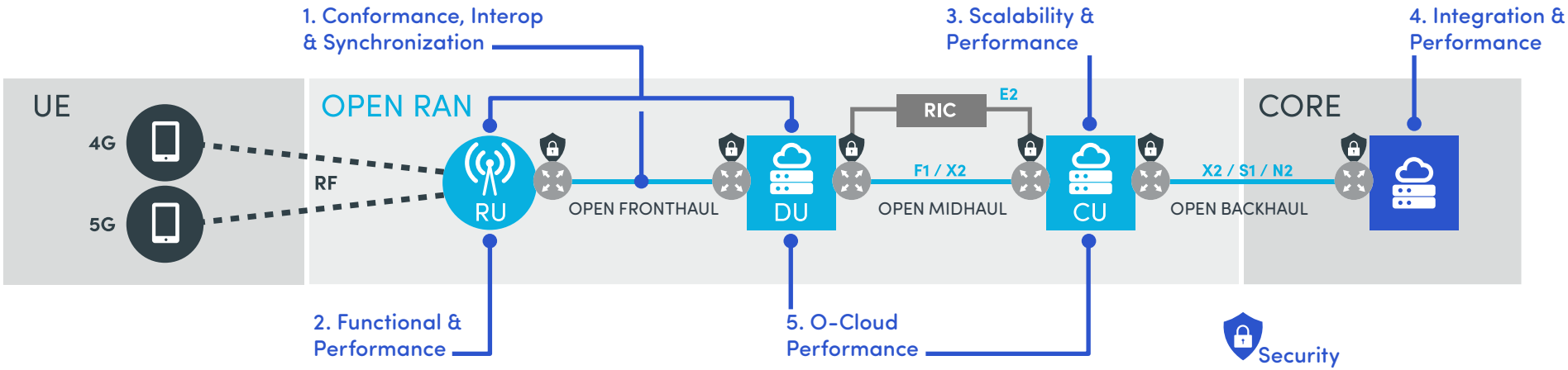
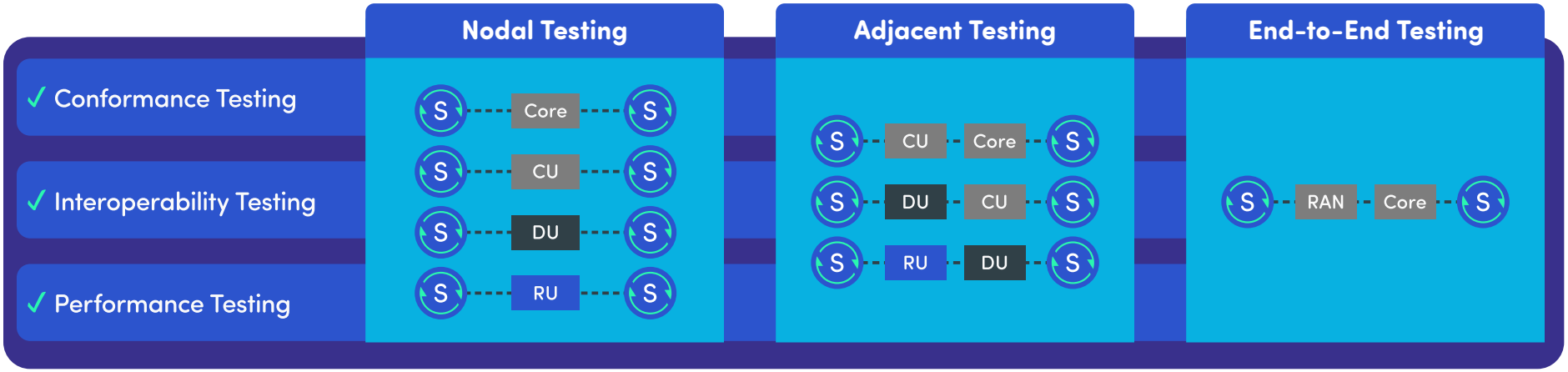


FIGURE 5

Open RAN Testing Strategies



Testing is not a "one and done" activity. Testing and assurance occur at crucial points in the entire life cycle—from lab to live—and ultimately continue as long as components are deployed.

This testing ensures that a specific Open-RAN component meets 4G/5G Open-RAN performance and scalability standards. In this phase, a nodal network function, such as an open central unit (O-CU) or radio unit (RU), is wrapped with emulated network functions and traffic, representing a range of real-world conditions that might exist in the field. The goal is to confirm that individual components can handle the expected traffic and functionality. These components must also be tested at peak performance and capacity levels to ensure they are robust and do not become a weak link out in the field.

Two types of adjacency testing exist. The first entails testing a specific piece of equipment to validate that it works with other components of the environment with which it must interface. The second involves a subset of the Open RAN environment (such as the fronthaul or midhaul), which is tested with other parts of the Open RAN environment (for example, testing midhaul transport with the fronthaul and the backhaul).

In this phase, operators are not just testing for interoperability, but interoperability at scale. They are getting a first look at how critical components will perform together in the field. By this stage, issues are already being identified with individual vendors sorting bug fixes, interoperability challenges, and any network bottlenecks that may be discovered. These hiccups should be expected, as open standards can be subject to interpretation, with unique implementations needing to be fine-tuned in the lab.

The entire Open RAN environment, from the core network to the endpoints (e.g., smartphones or IoT devices), must be tested to ensure the entire Open RAN system meets specifications.

Additional Considerations in Testing

Virtualized Component Testing.

If a component is virtualized, testing should be conducted to validate that the virtual infrastructures—with or without hardware acceleration technology and containerized or virtual functions—perform and scale correctly.

Synchronization Testing.

This assesses, identifies, and validates all aspects of network timing performance.

Continuous Testing.

There is no "final" stage of Open RAN testing. Operators will need to adopt a continuous testing approach to handle the velocity, variety and volume of releases and updates coming from the vendors. To this end, state-of-the-art automated continuous testing will be a cornerstone of any successful Open RAN testing strategy to minimize costs, reduce time to market, and provide higher-quality releases from vendors.

KEY TAKEAWAY

There is no "final" stage of Open RAN testing. Operators will need to adopt a continuous testing approach to handle the velocity, variety and volume of releases and updates coming from the vendors.

Service Assurance Testing.

After comprehensive lab testing is completed successfully, deployment of the full Open RAN system takes place, and service assurance testing begins. Open RAN assurance testing involves continuous validation in real-world conditions in the live network to address the following priorities:

- In an open, virtualized, multi-vendor world, change is continual. Modern development methodologies have adopted the continuous integration/continuous deployment, or CI/CD model, to account for vendors pushing out new software releases at a rapid pace in a continuous telecom innovation pipeline. Even if the entire Open RAN system passed testing yesterday, such test results mean nothing is guaranteed to work today.
- The goal of assurance testing is to spot problems before end users do. This allows you to troubleshoot, isolate the problem, and fix it before dissatisfied customers clog support lines.
- SLA management: The monetization avenues for Open RAN (in conjunction with 5G) include private networks, enterprises, and Edge applications. SPs and SIs can monetize these services if they provide service-level agreements (SLAs) to their end customers. Guaranteeing SLAs requires a proactive approach in which SLAs are monitored 24X7 to catch any degradations quickly and then troubleshoot and isolate the issues so they can be addressed in a timely fashion.

To properly ensure the Open RAN system, traditional service assurance approaches based purely on ***passive monitoring*** and telemetry data are not sufficient for this new disaggregated multi-vendor environment. A continuous proactive approach that can be instantiated anywhere, even across an outside network, is now the key. This approach delivers visibility across the new Open RAN disaggregation and provides the ability to segment and isolate issues across the radio, transport, and core domains.

Active testing represents the cornerstone of a new breed of proactive service assurance. This involves light-weight software-defined test agents generating synthetic traffic or emulating network functions that can be dynamically instantiated across the network on open compute. The agent intelligently tests and continuously monitors various use cases. These include the scale and performance of a new Open RAN node, service chain, or proactively monitored performance through the continuous active testing of SLAs. This incorporates performance metrics for continuously revalidating performance during network or software changes.

Other Testing Use Cases

Network Capacity.

An Open RAN environment must support considerable overhead, which includes firewalls, gateways, encryption, and more. It is an open question whether a given COTS platform has the power to run these extra loads and still meet performance requirements. Testing is required to ensure this.

Supply Chain Security.

The Open RAN consists of a complex supply chain of vendors and components. The security of an entire Open RAN environment depends on the ability to trust each component. The SolarWinds breach demonstrated that attacks not only come from outside the network, but can also gain access through a single internal component. Testing can ensure that each individual component is properly secured and can identify and resolve issues if a specific component is breached.

KEY TAKEAWAY

Active testing represents the cornerstone of a new breed of proactive service assurance. This involves light-weight software-defined test agents generating synthetic traffic or emulating network functions that can be dynamically instantiated across the network on open compute.

Security

One of the challenging aspects of moving from proprietary RAN architecture to Open RAN is the security risk. By disaggregating the RAN, more vendors and layers are introduced, all of which increase the attack surface. Many security experts advise that, in today's wide-open, cloudified world, the safest posture is to assume the worst, with Zero Trust, and conduct continuous testing for security vulnerabilities, evidence of intrusions or attacks forming.

Testing Methodologies for Live Open RAN Networks

Open RAN is a complex, dynamic entity with multiple vendors used for many purposes. Testing Open RAN while it is live is an extremely complicated endeavor that requires multiple methodologies.

Automated Testing. The service provider world has a heritage of traditional waterfall development practices. Open RAN will push vendors into a more modern Agile development methodology. Part of the Agile philosophy is the rapid, automated deployment of new versions—employing a CI/CD methodology.

A core tenet of CI/CD is to "fail fast." The idea is that it is better to innovate, fail quickly, fix, and continue, than it is to work diligently in the lab with the waterfall model, striving for perfection before deploying.

Failing fast, however, only works if you discover root causes of failures rapidly as well, so they can be resolved quickly. Comprehensive test automation is required to achieve this, and it is closely aligned with an Agile methodology. With automated testing, comprehensive test suites are defined and developed in advance and run before any component is released. Then, the same approach is used to validate the deployment of an Open RAN solution to ensure the testing runs automatically every time a new component is released.

Continuous Testing. The Open RAN movement is complex. With so many vendors continuously iterating their software, it is inevitable that issues will always arise. Testing can address this, but performing a full suite of static lab tests (nodal, adjacency, end-to-end) is not possible for an Open RAN environment deployed in a live network.

Continuous testing in the form of active testing is employed, where synthetic traffic simulating real-world traffic is injected into the network. By focusing this synthetic traffic on each domain of the Open RAN, issues are spotted quickly so they can be resolved rapidly before end users are impacted.

Field Testing. The ultimate measure of an Open RAN's performance is the end-user experience. Is the user experiencing satisfactory quality of service (QoS) for phone calls, videos, and data streaming? The only way to reliably measure this is on the user's actual device in typical locations where services are actually used.

Open RAN–
The Path Forward

We live in exciting times. Edge computing, 5G, and mobile clouds are all transformative technologies that enable bold new business models. Industry 4.0, autonomous vehicles, and remote medicine are examples of the advances these new technologies offer.

Open RAN presents a foundational framework to foster this revolution. It allows this transformation to occur at pace and scale. Open RAN is not easy to build, and ensuring effective interoperability across technologies and domains is no simple undertaking—but the journey is worth it. It will entail years to deploy completely and realize its full value. To achieve this, the industry must contend with the ever-evolving challenges of network maturity, security, and cost.

Testing comprehensively and continuously—from lab to live—with a smart strategy driven by best practices are table stakes to ensure these challenges have been met effectively now, in the real world, and in the future.

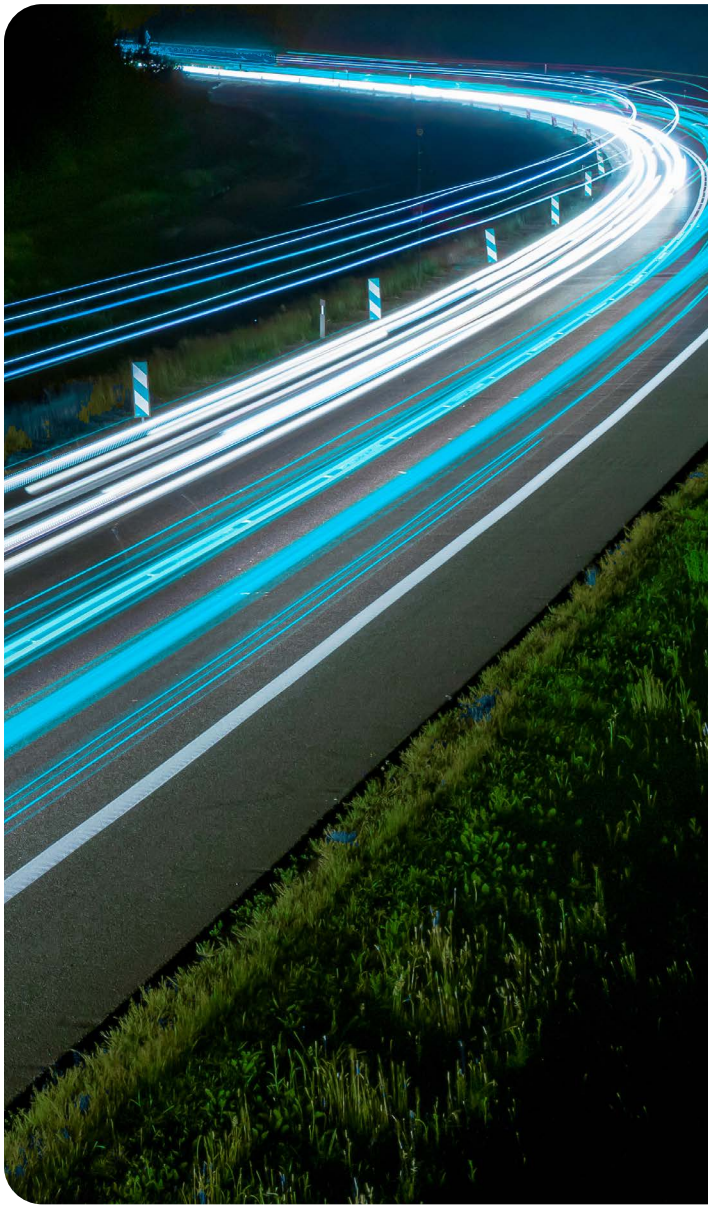
Vendor-neutral testing and assurance are crucial for building industry confidence that Open RAN is a truly safe and viable option.

As an industry leader in test and assurance, Spirent is trusted across the end-to-end telecommunications ecosystem, and our Open RAN solutions and expertise are helping to:

- Continuously validate performance, robustness, and parity to traditional RAN
- Ensure multi-vendor interoperability, collaboration, and open ecosystems
- Realize cost efficiencies, innovation benefits and accelerate time to market

KEY TAKEAWAY

Vendor-neutral testing and assurance are crucial for building industry confidence that Open RAN is a truly safe, viable and beneficial in the long term.



COMPUTER CONTROLS

Computer Controls AG distributes electronic components, IoT applications, software, test and measurement solutions. We support our customers in selection, integration and maintenance, translating requirements into complete electronic solutions and customizing systems according to individual specifications. We are a qualified partner for solution-orientated cutting-edge technology.

Computer Controls AG
Industriestrasse 53
8112 Otelfingen
Switzerland
Phone: +41 (0) 44 308 66 66
E-mail: info@ccontrols.ch
Web: https://www.ccontrols.ch

About Spirent

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information visit: www.spirent.com

About Spirent Communications
Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled. For more information visit: www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

© 2024 Spirent Communications, Inc. All of the company names and/or brand names and/or product names and/or logos referred to in this document, in particular the name "Spirent" and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice. Rev L | 02/24

spirent