White Paper

O-RAN Testing: Challenges, and Recommendations

White Paper: February 2025

Contributors:

VIAVI Solutions
Tata Consultancy Services
Spirent
Digital Catapult
Univ. of New Hampshire – Interoperability Lab
Keysight
Rakuten Mobile
Peraton Labs
Mavenir
MITRE
Calnex
Iowa State University
Artiza Networks
Chunghwa Telecom
NEC

Disclaimer

Copyright

Executive summary

The O-RAN ALLIANCE has been supporting the testing and integration needs of its member companies for the past several years through the development of test specifications, specifying processes for certification and badging, establishment of Open Test and Integration Centers, and organizing Global PlugFests. A previous white paper has provided an overview of the certification and badging process and Open Test and Integration Centers. This white paper dives deeper into the O-RAN test specifications and other Open RAN laboratories that are contributing towards the proliferation of Open RAN. In addition, the paper contributors have outlined key challenges in Open RAN and recommendations on how to overcome several of these challenges.

Definition of terms, symbols and abbreviations

Terms

IOT: Interoperability Testing

O-CU: O-RAN Central Unit [O-RAN.WG1.OAD]

O-DU: O-RAN Distributed Unit [O-RAN.WG1.OAD]

O-RU: O-RAN Radio Unit [O-RAN.WG1.OAD]

O-Cloud: O-RAN Cloud Platform [O-RAN.WG1.OAD]

OTIC: Open Testing and Integration Centre

RAN: Radio Access Network. [O-RAN.WG1.OAD]

SUT: System Under Test

Abbreviations

For the purposes of the present document, the [following] abbreviations [given in i.1 and the following] apply:

AS	Application Server
CD	Continuous Deployment
CI	Continuous Integration
CN	Core Network
CT	Continuous Testing
IOT	Interoperability Testing

NFV	Network Function Virtualization
O-Cloud	O-RAN Cloud
O-CU	O-RAN Central Unit
O-DU	O-RAN Distributed Unit
O-RU	O-RAN Radio Unit
OTIC	Open Testing and Integration Centre
RAN	Radio Access Network
RRH	Remote Radio Head
RRU	Remote Radio Unit
SUT	System Under Test
UE	User Equipment
VNF	Virtual Network Function

Acknowledgements

[1]Special thanks to the following individuals who contributed to this White Paper:

Lead Editor: Ian Wong (VIAVI Solutions)

Co-editor and Contributors: Tulasi Babu Doppalapudi (Tata Consultancy Services), Chris Gu (Spirent), Xhafer Kransniqi (Digital Catapult), Lincoln Lavoie (Univ. of New Hampshire – Interoperability Lab), Jasper Li (Keysight), V. Lingasamy (Rakuten Mobile), Laurence Mailaender (Peraton Labs), Awn Muhammad (Rakuten Mobile), Eric Ortiz (Mavenir), Peter Pacheco (MITRE), Sunil Pandarlapalli (Rakuten Mobile), Stefano Ruffini (Calnex), Samir Kanta Satapathy (Tata Consultancy Services), Mohammed Soliman (Iowa State University), Shuhei Tokonami (Artiza Networks), Siddhartha Trivedi (Rakuten Mobile), Chloe/Jing-Chen Tu (Chunghwa Telecom), Neal/Sz-Hsien Wu (Chunghwa Telecom)

Major reviewers: Awn Muhammad (Rakuten Mobile Inc), Marko Babovic (NEC)

Table of contents

Introduction

Open RAN technology has evolved significantly since the very first O-RAN ALLIANCE specifications were released, and with it the complexity and challenges of O-RAN testing have likewise grown significantly. In this white paper, we summarize the status and progress to date in O-RAN test specifications and procedures and describe the current ecosystem of testing laboratories. We highlight the major challenges that O-RAN faces and provide recommendations to overcome these challenges.

1 O-RAN Test Specifications

The O-RAN ALLIANCE supports its ecosystem in testing and integrating O-RAN solutions through the development of test specifications, organizing global PlugFests, developing processes for certification and badging, and coordinating a global network of Open Testing and Integration Centres (OTICs). An overview of OTICs and the O-RAN certification and badging program can be found in a previously published white paper [1]. In this section, we provide an overview of the test specifications published by the O-RAN ALLIANCE. All published O-RAN specifications are available for download at https://specifications.o-ran.org/specifications.

The test specifications for O-RAN systems can be broadly categorized into: Conformance, Interoperability (IOT), End-to-End (E2E), and Security Test specifications.

1. Conformance Test

Conformance testing verifies that the interfaces of network equipment comply with O-RAN specifications. This type of testing assesses whether a vendor's equipment—such as a specific network element—adheres to the defined specifications for its designated exposed interfaces. As of the end of 2024, O-RAN ALLIANCE has published conformance test specifications on the A1, R1, E2, Open Fronthaul, and O-Cloud interfaces [2-6]. However, conformance testing alone does not guarantee correct inter-operation between elements from different vendors due to the large configuration space of these interfaces.

2. Interoperability Test

Interoperability testing (IOT) ensures that two network elements can work together seamlessly. Among the IOT specifications defined by the O-RAN ALLIANCE, a notable example is the WG4 interoperability test specifications [7] between O-RU and O-DU over the Open Fronthaul interface. In this scenario, both O-RU and O-DU are collectively treated as the System Under Test (SUT). The IOT tests between O-RU and O-DU cover various network planes—M/S/C/U-Planes—to validate that the combination of O-RU and O-DU meets O-RAN's requirements. IOT is integral to establishing a baseline for interoperability within the O-RAN ecosystem and addressing the limitations of conformance testing. As of the end of 2024, O-RAN ALLIANCE has published IOT specifications on A1, E2, F1, X2, Xn, O-Cloud interfaces/APIs and O-CU/O-DU Stack Interoperability [2,3,8,9,10].

3. End-to-end Test

E2E testing validates that all involved O-RAN network elements and interfaces of the whole O-RAN system, scoped as the SUT, can properly interoperate together, and an end-to-end (E2E) communication link can be established between the end-user device, i.e. User Equipment (UE), and the Application Server (AS) or another UE [11]. In E2E testing, the SUT is connected to the AS through 3GPP-compliant network elements, such as a Core Network (CN), to establish the complete E2E communication link. Key Performance Indicators (KPIs) for E2E testing are defined across the entire communication chain of network elements involved in the E2E link. These KPIs provide a comprehensive view of the SUT and ensure that the SUT meets the operators'/users' requirements for E2E functionality, performance, and reliability.

4. Security Test

Security testing is a category on its own, which validates security functions, configurations, and protocol requirements based on the risk analysis for O-RAN systems. The O-RAN Security Test Specification [12] is focused on validating the implementation of security requirements and protocols, emulating security attacks to measure the robustness of the O-RAN system and validating the effectiveness of the security mitigation methods.

2 Open RAN Testing Laboratories

Within the Open RAN community, several organizations have established testing resources focused on Open RAN technologies. These organizations range from mobile network operators, independent testing labs, universities or academic institutions, government agencies, and equipment manufacturers. Many of these laboratories are associated with specific industry groups that have established criteria or operational requirements for Open RAN testing. Table 1 below attempts to list the major organizations and government funded Open RAN testing / laboratory programs, which is by no means an exhaustive list.

Organization/Funding Source: Lab Name	Description
O-RAN ALLIANCE: Open Testing and Integration Centres (OTICs) https://www.o-ran.org/otic	The O-RAN ALLIANCE Open Testing and Integration Centres (OTIC) [1] provide an open, collaborative, vendor independent, and impartial working environment to support the progress of the O-RAN industry ecosystem, including: awarding O-RAN certificates and/or badges, hosting O-RAN PlugFests, and other testing activities. See https://www.o-ran.org/otic for the latest OTICs.
Telecom Infrastructure Project: TIP Community Labs & Authorized Labs https://telecominfraproject.com/clabs/	TIP (Telecom Infra Project) is an industry organization that helps accelerate the development, commercial adoption and deployment of open, standards-based, and disaggregated technology solutions, including O-RAN, for next-generation telecom networks. TIP's main activity is to design, build, test, and deploy network solutions at scale. TIP has established a community of labs providing testing services according to TIP project group documentation. TIP Authorized Lab extends the requirements and quality controls required of participating labs within the program. These Community and Authorized Labs are spaces where O-RAN vendors and other stakeholders can test and deploy O-RAN infrastructure. Though these Labs are not owned by TIP, they are sponsored by TIP participants. TIP has developed a badging program with a three-tier categorization: bronze, silver and gold; demonstrating the maturity and interoperability of products and solutions.
US NTIA[2] T&E: Open RAN Centre for Integration and Deployment (ORCID) https://www.orcid.us/home	Hosted by Boost Mobile (formerly Dish Wireless), this center, focusing on Open RAN integration and deployment, involves three major industry players, Fujitsu Network Communications, Mavenir Systems, and VMWare. This center is also supported by several technology partners, such as Analog Devices, ARM, Cisco, Dell, Intel, JMA, NVIDIA, Qualcomm, and Samsung.
US NTIA T&E: Acceleration of Compatibility and Commercialization of Open RAN Deployments (ACCoRD) https://accord-wif.org/	Hosted by AT&T and Verizon Wireless, this test and evaluation program is set in two different sites, in Dallas and Washington D.C., and is a consortium of US and foreign operators, universities and equipment vendors, that focuses on testing network performance, interoperability, security, and developing new testing methods.
US NTIA T&E: VIAVI Automated Lab-as-a-	Hosted by VIAVI Solutions, this test and evaluation program establishes a hybrid physical lab infrastructure and cloud-based testing lab-as-a-service (LaaS) for Open RAN. The idea of this

[2] https://www.ntia.gov/funding-programs/public-wireless-supply-chain-innovation-fund/innovation-fund-round-1-2023-research-and-development-testing-and-evaluation

Service for Open RAN (VALOR) https://www.viavisolutions.com/en-us/valor	T&E center is to create a fully automated, cooperative, open, and impartial testing-as-a-service (TaaS) for Open RAN interoperability, performance and security.
US Agency for International Development (USAID): Asia Open RAN Academy network of labs https://www.asiaopenranacademy.org/aora-programs/network-of-labs-for-rd	The Asia Open RAN Academy (AORA) is an initiative co-created with USAID funds as a part of the Indo-pacific economic framework. The academy is an alliance of academic, government, and Industry stakeholders in the Philippines and beyond. Incorporated as a nonprofit corporation in March 2023, AORA is built on principles of Partnerships, Open Education Resources, Curriculum Standards, and Community. The first O-RAN Laboratory is based in the University of the Philippines in Manila[3].
German Federal Ministry for Digital and Transport: i14y Lab https://www.i14y-lab.com/	The i14y Lab is based in Berlin Germany housed in the Deutsch Telecom campus. It is an open lab focused on interoperability and integration testing for disaggregated mobile & transport networking components. The lab is run by a consortium that has players from all areas needed to achieve this goal: operators, vendors, system integrators, and academia. The lab works together with providers and vendors of all sizes – from large companies to start-ups - and with a range of communities already active in network disaggregation.
Taiwan Government: ITRI (Industrial Technology Research Institute)	ITRI is a world-leading technology institute in Taiwan, focusing on applied technology research and development with a clear mission to use technology to drive industrial development, creates economic value, and improves social well-being. ITRI developed O-RAN testing capabilities within their Open Network Lab and collaborates closely with OTICs and other labs, such as SONIC, i14y Lab etc., to coordinate on O-RAN integration, testing, badging and certification.
UK Dept. of Science, Innovation and Technology: SONIC (SmartRAN Open Network Interoperability Centre) https://www.digicatapult.org.uk/programmes/programme/sonic-labs/	SONIC Labs, launched in 2021 to accelerate new open network solutions for the UK, is a part of the UK's national 5G Supply Chain Diversification Strategy. The programme is led by Digital Catapult and Ofcom; supported with the funding from the Department for Science, Innovation and Technology (DSIT). SONIC Labs built a commercially neutral environment for collaboration, enabling the telecoms ecosystem to test and explore the integration of multi-vendor architectures, their interoperability, and how they can develop open, disaggregated and software-centric network products, solutions and services.

In many cases, laboratories likely participate in more than one of the above programs to enable the sharing of knowledge and resources. Many of the labs have established similar operating approaches, based on the best practices known to the industry, such as:

1. Providing secure remote access to laboratory participants to configure, test, and troubleshoot equipment within the lab,.

[3] https://www.usaid.gov/philippines/press-releases/jun-05-2024-united-states-philippines-step-closer-launching-first-open-ran-laboratory-manila

2. Collaborating with regulatory authorities for experimental access to spectrum resources for testing or research purposes.
3. Maintaining confidentiality of results and measurement data for testing carried out in the lab.

Access to each of the testing laboratories, along with testing fees or funding models, is where more specificity begins to appear. For example, a testing lab operated by a specific mobile network operator may not charge fees to equipment vendors entering the lab but may only focus on areas of interest to that operator and only invite equipment suppliers with existing commercial relationships to the host operator. An independent testing laboratory might be open to any equipment vendor but charge fees according to reasonable and non-discriminatory practices.

Some laboratories may also follow, or be required to meet, specific accreditation processes, such as adherence to the ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories.

3 Open RAN Challenges

O-RAN represents a transformative approach in the telecom industry. By leveraging intelligence, openness, disaggregation, and virtualization, O-RAN breaks the closed nature of the previous RAN generations but that comes with several challenges.

3.1 Multi-vendor disaggregation

Establishing a multi-vendor disaggregated RAN comes with many challenges, including:

1. Interoperability: The O-RAN ecosystem offers a seemingly limitless combination of vendors and RAN functions and components, allowing operators to mix and match solutions from various suppliers. While this provides flexibility, competition, and choice, it creates interoperability challenges. Different vendors may implement their solutions differently, leading to compatibility issues and potential conflicts between components. Ensuring seamless interoperability becomes crucial for the success of O-RAN deployments. Disaggregation of RAN also introduces new challenges for life-cycle management because of version differences between O-RAN functions, platforms, and hardware. This means that there could be interoperability issues when different vendors update their products, especially software packages, and these changes have not been reflected across the system.

2. Integration complexity: Disaggregation and cloudification as the two key concepts of O-RAN require more system integration between O-RAN functions and components, which can lead to a more complex configuration and need for more technical resources. Furthermore, integration of O-RAN requires new skill assets that a large proportion of engineers and experts from the industry don't have yet.

3. CSP Confidence: Communication Service Providers (CSP) run critical infrastructure for provisioning different types of services with different requirements and priorities. Some of these services are very critical in nature, making the CSP very reluctant to take risks. This can be, in particular, very challenging to new entrants in the O-RAN space. As O-RAN seeks to diversify the supply chain from one or two vendors supplying most of the hardware and software to an ecosystem of seemingly endless possibilities, clear channels to present capability will need to be developed to ensure CSPs have the opportunity to select the best solution for their networks.

3.2 Virtualization and Cloudification

While virtualization and cloudification in O-RAN offer numerous benefits, including flexibility, scalability, and cost-efficiency, they also present significant challenges. Addressing these challenges requires an effort from industry stakeholders, including vendors, operators, and regulators, to ensure the successful deployment and operation of O-RAN networks.

1. Technical Challenges

- Performance and Latency: Virtualization can introduce additional latency due to the abstraction layers between hardware and software. For example, in a 5G network, achieving the ultra-low latency required for applications like autonomous driving or remote surgery can be difficult when using virtualized infrastructure. Especially software and hardware of a network element can be from different vendors in which case whether performance and functionality can meet QoS requirement of CSP is a question.

- Resource Management: Efficiently managing resources such as CPU, memory, and storage in a cloud environment is complex. For instance, dynamic resource allocation is necessary to handle varying network loads during peak hours, such as during major sports events or emergencies.

2. Security Challenges

- Data Privacy: Virtualized environments can be more vulnerable to data breaches. For example, a misconfigured virtual machine could expose sensitive user data. Ensuring robust encryption and secure data handling practices is essential to protect user data.
- Network Security: The distributed nature of cloudified RANs increases the attack surface. Implementing comprehensive security measures to protect against cyber threats is crucial. For instance, a DDoS attack on a cloud-based RAN could disrupt service across a wide area.
- Isolation: Ensuring proper isolation between different Virtual Network Functions (VNF) to prevent potential security breaches is a complex task. For example, a vulnerability in one VNF should not compromise the entire network.

3. Operational Challenges

- Complexity in Management: Managing a virtualized and cloudified O-RAN requires advanced orchestration and automation tools. The complexity of these systems can pose significant operational challenges. For instance, orchestrating the deployment and scaling of VNFs across multiple cloud environments requires sophisticated management platforms.
- Skill Gap: The shift to virtualized and cloudified O-RAN requires new skill sets for network operators and engineers. Training and upskilling the workforce to handle these new technologies are essential. For example, engineers need to be proficient in cloud-native technologies and Network Function Virtualization (NFV).
- Reliability and Availability: Ensuring high availability and reliability in a cloud environment can be challenging due to potential hardware failures, container corruption, and software bugs. For instance, a failure in the cloud infrastructure could lead to server outages if not properly managed.

4. Economic Challenges

- Cost: The initial investment in virtualization and cloud infrastructure can be high. Additionally, ongoing operational costs need to be managed effectively. For example, the cost of migrating legacy systems to a cloud-based O-RAN can be substantial, including expenses for new hardware, software licenses, and training.

3.3 Performance, Capacity, and Scale

To achieve wide acceptance in the marketplace, O-RAN network implementations must meet or exceed the performance of traditional RANs in capacity, latency, coverage, reliability, and security. To help ensure this, the O-RAN ALLAINCE's E2E Test Spec [11] defines a battery of 'Performance Tests' under a variety of conditions. This section identifies often-seen challenges in the design and implementation of such testing systems or solutions.

1. Basic capacity and KPI measurements: Performance tests begin by verifying that under near-ideal conditions, the O-RAN base station will achieve the maximum theoretical downlink and uplink throughput as defined in the relevant (4G, 5G, etc.) 3GPP technical specification. Such basic tests are similar to what is done for traditional monolithic RAN today. Complications will arise in test repeatability given the large configuration space for all the network components and UEs. If capacity appears to be limited it may be difficult to determine which specific network function or configuration file is responsible.

2. Handling multiple software versions across multiple network functions: Flexible RAN network topologies enabled by disaggregation of O-RAN introduce many possible architectural configurations that increase the number of test cases. The complexity of testing grows dramatically when multiple versions of software-builds of disaggregated RAN network functions, e.g. O-RU, O-DU, O-CU, etc. are considered.

3. Facilitation of SUT integration and test repetition: More integration time is also required for the system testing, including the setup of test equipment and configuration of the SUT, and there may be misinterpretation of O-RAN specifications on top of 3GPP specifications among vendors. More tests or repetition of the tests need to be analyzed due to the newly specified network interfaces, e.g. the M/S/C/U-plane of the Open Fronthaul.

3.4 Energy efficiency

Defining energy efficiency in wireless networks is far more complex than simply comparing data output to energy consumption. A truly comprehensive understanding of energy efficiency must consider additional factors, such as latency, availability, QoS, and the number of connected or actively serviced users. These factors are essential to maintaining network reliability, scalability, and responsiveness while optimizing energy use. Therefore, a holistic approach to energy efficiency in wireless communications balances reduced energy consumption with uninterrupted, high-quality services across diverse network conditions.

1. Complexity in Defining Energy Efficiency Across O-RAN: Evaluating energy efficiency across the entire O-RAN system—and even more so within specific network nodes like the O-RU—is inherently challenging due to numerous internal and external factors. For instance, the O-RU's energy efficiency is interdependent with other components, such as the O-DU, O-CU, and RIC platforms. Each of these elements impacts energy usage through features like energy-efficient scheduling and various power-saving functionalities, making isolated measurements difficult. Assessing cloudified network functions, such as the O-DU and O-CU, presents additional challenges. These functions often share resources with other virtualized functions in the cloud environment, complicating precise energy allocation. Energy consumption for each function can fluctuate based on network demand and orchestration policies, necessitating advanced monitoring and resource-sharing management techniques to ensure accurate energy attribution in real-time.

2. Dependencies on Network Management and Intelligent Apps: Implementing energy-saving strategies—such as cell and carrier switch on/off or dynamic channel reconfiguration—requires intelligent network management. This management is often facilitated by control equipment like the O-DU and O-CU, as well as intelligent applications such as xApps and rApps. Consequently, the overall energy efficiency of an O-RAN-based network heavily depends on the intelligent algorithms and control mechanisms provided by these applications.

3. Performance and energy efficiency Trade-Off: Implementing power-saving techniques like cell discontinuous transmission (Cell-DTX) can introduce latency, impacting applications that require real-time responsiveness. While Cell-DTX saves energy by allowing O-RU transmitters to lower down RF power during inactivity, transitioning between active and inactive states can cause delays on UE data, especially during high-traffic scenarios. Balancing energy efficiency with minimal latency necessitates intelligent network management and advanced algorithms. In such situations, validating performance while ensuring efficiency adds complexity to testing energy efficiency, as tests must assess both the energy savings and the maintenance of service quality under dynamic conditions.

4. Testing Challenges for O-Cloud Infrastructure: Testing energy efficiency in O-Cloud environments presents significant challenges due to the need to validate the cloud infrastructure's energy-saving features, such as optimized CPU states—dynamic frequency scaling, low-power modes—and shutting down idle servers. These hardware-level optimizations dynamically affect performance and resource availability, adding complexity to testing. Focusing on the O-Cloud, tests must ensure that these energy-saving mechanisms effectively reduce energy consumption without causing service degradation. This involves simulating real-time energy availability and dynamic network demand to assess how the O-Cloud handles variable workloads while maintaining performance metrics like latency and reliability. Ensuring compliance, interoperability, and optimal performance across all layers—hardware, virtualization, network functions, and orchestration—adds to the complexity. While the primary focus is on the cloud infrastructure, testing must also cover how orchestration mechanisms manage workload distribution in alignment with 3GPP and O-RAN standards. Developing comprehensive testing methodologies that encompass both the O-Cloud's energy-saving features and the orchestration processes is essential.

5. Vendor Interoperability in Energy-Saving Feature: Achieving energy efficiency across O-RAN's open ecosystem presents an additional challenge in terms of vendor interoperability. Energy-saving configurations may be implemented differently by various equipment providers, potentially hindering the effectiveness and integration of network-wide energy-saving strategies. Ensuring standardized, interoperable energy-efficient protocols is crucial for seamless operation across multi-vendor environments.

3.5 Resiliency/Robustness

Resiliency testing in O-RAN ecosystems involves addressing the complexities introduced by its disaggregated, cloud-native architecture. Multi-vendor coordination poses a significant challenge, as different vendor solutions must work seamlessly together to ensure interoperable failure recovery mechanisms. Standardized processes for fault management across vendors are essential, making multi-vendor testing critical. The distributed nature of O-RAN also increases the number of failure points across layers like RAN, cloud, and transport, making it vital to validate robust fault detection and recovery mechanisms. Cloud-

native focus further complicates testing, requiring verification of auto-scaling, auto-healing, and container orchestration during failures to ensure that these cloud-based mechanisms integrate well with fault recovery procedures. Key challenges include:

1. Testing the Distributed Nature of Open RAN: Resiliency testing must simulate diverse failure scenarios, including node and link failures, component crashes, and simultaneous failures across horizontal (O-RU, O-DU, O-CU, transport, core) and vertical (bare metal, firmware, CaaS, containerized software) domains. Comprehensive cross-domain testing is essential to validate failover mechanisms, real-time performance, and resource management, ensuring uninterrupted service during failures.

2. Defining Resiliency Metrics: Metrics such as packet loss, failover time, service restoration, and session continuity must be clearly defined and aligned with stringent latency requirements to accurately evaluate system recovery.

3. Resource-Intensive Testing: Extended high-load stability tests demand continuous oversight, with manual processes often straining resources and increasing the risk of lapses that could compromise test results.

3.6 Overload, Priority, Emergency Conditions

In real-world deployments, RAN equipment must withstand difficult heavy traffic conditions caused by disaster/emergency events (earthquakes, explosions/terrorism), equipment failures, or unusual traffic demand during, such as a sporting or political event. Such testing can assure the CSP community that O-RAN components are ready for service. The O-RAN E2E Test Spec [11] defines a special set of Load and Capacity tests that determine network performance under these heavily loaded conditions, which are:

- Emergency Call,
- Earthquake and Tsunami Warning System (ETWS), and
- Multimedia Priority Service (MPS) calls.

While these are similar to those in ordinary 3GPP networks, such tests are more difficult due to disaggregation, virtualization and cloudification as described in sections above, including: creating the overload/stressful conditions in realistic yet repeatable ways, and accounting for the variety of O-RAN configurations (aggregated vs distributed O-DU, O-CU) and the potential transport network latencies between them, and in properly configuring the core network and SMO.

3.7 Synchronization

Synchronization is a fundamental aspect in the operation of RANs, for example as a prerequisite to prevent interference when TDD (Time Division Duplex) radio technology is used. Several S-Plane specifications have been developed by the O-RAN ALLIANCE to meet the end-to-end synchronization requirements of O-RAN network implementations so that they meet 3GPP performance requirements. Multi-vendor disaggregation and virtualization have introduced new challenges for synchronization, making related testing an even more fundamental activity. Synchronization performance must be verified under ideal conditions (i.e., with no noise in the network) and in normal conditions (including effects from network rearrangements).

Relevant S-Plane testing details are provided as part of the WG4 Conformance Test Specification [5],which verifies that the O-RU and O-DU can support the various synchronization configurations defined in O-RAN, as part of the WG4 interoperability test specifications [7] between O-RU and O-DU, and as part of the WG9 Xhaul transport testing, where methodologies, parameters and limits for the various synchronization network technologies and architectures are provided [13].

3.8 RIC-enabled Use Case Testing

RIC-enabled use cases are scenarios that O-RAN defines to highlight novel network capabilities that feature the non-Real and near-Real Time RICs. Examples include Traffic Steering, Massive MIMO Beamforming Optimization, Energy Savings, and Filtered Measurements. However, given the novelty of O-RAN technologies, it turns out that testing these use cases can be quite challenging.

From specification development point of view, these RIC-enabled use cases are first defined at a high level by the Use Case Task Group, which then pass to detailed work groups responsible for defining test procedures for their specific interfaces utilizing Stage 2 and 3 specs. This may include the messages which pass over specific interfaces, or policies that alter RIC behavior via those interfaces. Designing a use case test is challenging because there are no minimum performance

requirements, and individually designed rApps/xApps may work according to different principles. This makes defining a test with clear pass-fail criteria that is broadly applicable impossible.

3.9 Operational/logistical challenges

The large number of laboratories around the world is a great asset for the O-RAN community but also comes with its challenges.

1. Entry & Expectation: The multiple types of labs in various regions of the world with different test capabilities lead to varying entry criteria and expectations. In the case of OTICs, many vendors start with PlugFest activities to mature their first level of interoperability and conformance. Then when vendors partner up (e.g. DU and RU vendors) the testing goes beyond the initial conformance and interoperability test, and can quickly move towards further validation, e.g. performance. Other labs will want proof of conformance and sharing of interface compliance prior to starting interoperability testing. Yet other types of labs may require more stringent full documentation and the vendor is kept outside the execution process and finally receives a report at the end of the cycle with much less visibility. In summary each lab has different entry and expectations, which can lead to vendor confusion, delayed execution or misalignment on expected results.

2. Quality Control: Since the various labs have different test capabilities, and while there are some common denominator elements – how those tests are executed and captured can have significant variability due to:

- Individual software versions when the test was executed by all products in the system (some might be development code and have certain features disabled, thus not triggering feature interaction)
- Level of simulators vs real world elements in an E2E test (depends on the SUT)
- Whether the environment is Over-the-Air or Cabled RF for products influenced by radio performance.

These variances and others create complexity when documenting results, and lead to new test challenges, e.g. test repeatability and consistency, when making results shared between labs and vendors inconsistent, leading to retests and delay in meeting product maturity in a timely manner. In summary, the dynamic testing landscape creates challenges on quality control.

4 Recommendations to Overcome Challenges

4.1 Interoperability Testing

The following recommendations address the IOT challenges described in the sections above:

1. Well defined interfaces: Well defined interfaces are fundamental to the interoperability between different components. It is recommended that O-RAN continue investing in improving the rigor and specifications around these interfaces and attempt to reduce the optionalities in order to facilitate interoperability.

2. Collaboration among vendors: Collaboration among vendors and system integrators is needed to validate solutions before deployment, which includes willingness to interoperate in e.g. plugfests, or be a part of continuous integration cohorts.

3. Automated testing: Automated testing is essential to identifying interoperability issues quickly and expedite the life cycle management of testing, verification and deployment

4.2 Continuous integration/deployment/testing (CI/CD/CT)

As described throughout section 4, O-RAN vendors likely have different release cycles of products, create a need for continuous integration (CI), continuous deployment (CD), and continuous testing (CT) processes. These CI/CD/CT operations are typically driven through automation systems, responsible for the integration and deployment of the new network function artifact, i.e. a new revision of a network component, into a test network or deployment, followed by the automated operation of testing cases and evaluation of metrics and KPI measurements. Review of these metrics and testing results should be used as a gate for the acceptance of the new artifact or component release.

O-RAN testing laboratories are encouraged to employ similar automation systems, to provide laboratory participants with ongoing testing services. Constructing testbeds and lab systems used to automatically run regression testing. Similarly, those systems can be utilized to support the open source communities, providing valuable feedback to upstream open source projects.

4.3 Capacity/Scale Testing

OTICs and other O-RAN testing labs that prepare for Conformance testing, Interoperability testing, and E2E testing should endeavour to:

1. Test and validate as closely to the real-world user experiences as possible by using network function emulation across the protocol stack and employ realistic traffic models to mimic real-world applications. An effort is now underway in TIFG to enhance the E2E test procedures to account for higher user densities, macro-micro cells, and network configuration (bandwidth, TDD pattern, etc), to incorporate various user traffic (Voice, Video, TCP) and mobility models, which will result in the definition of more realistic test plans.

The O-RAN test community must invest in test automation platforms and be prepared for multiple software releases for individual network functions and multiple component configurations to push capacity and performance testing of a SUT to its limits automatically and progressively, to cover overloading and priority testing scenarios described in sections above.

2. Given the complexity and flexibility of O-RAN performance and capacity testing, the test data logging and KPI analytic capabilities should be assessed by each test facility and ideally have a common data format that can be accessed more broadly.

4.4 Energy Efficiency Testing

The O-RAN ALLIANCE should facilitate the development of a unified testing framework that enables consistent and reliable comparison of energy efficiency across different vendors' equipment. This comprehensive framework should define standardized metrics, testing methodologies, and universally accepted benchmarks that account for the specific characteristics of various components, including O-RUs, cloudified network functions, CPUs, DPUs, and GPUs.

The Testing and Integration Focus Group (TIFG), in collaboration with relevant working groups, should develop specialized testing methodologies for these components. This involves creating component-specific benchmarks under realistic traffic workloads. Partnering with industry stakeholders—including equipment manufacturers, operators, standardization bodies, and standards development organizations—will provide access to necessary specifications and power management features.

By integrating software and hardware testing and standardizing procedures, this unified approach will enhance the accuracy and reliability of energy efficiency assessments. It empowers operators to make informed decisions when selecting vendors, fosters competition and innovation in the market, and promotes the adoption of energy-efficient technologies across the industry.

O-RAN working groups should define standardized testing and evaluation methodologies for O-RAN RIC-Enabled Use Cases. Develop detailed test methods for each component, focusing initially on high-priority, high-energy consumption areas such as O-RUs, O-DUs, O-CUs, and O-Cloud infrastructure. These methodologies should account for various operating conditions, traffic patterns, and deployment scenarios to ensure comprehensive evaluation.

4.5 Negative/Recovery Testing

Specific test procedures must be developed to verify resiliency/failure recovery of a complete network under various configurations. It should include at least the following aspects:

1. Message disruption: The testing solution should be able to offer testing engineers, under a tight security management means, the ability to revise/edit any information element (IE) of any interface of the SUT to disrupt the SUT with a specific error message pattern, e.g. F1 message editor to test the CU resiliency.

2. Container disruption: The testing solution should be able to stop and restart a container used by a network function, e.g. CU, to assess the capability of the SUT to recover from the container disruption as expected. KPIs related to the system resiliency against container disruption should be monitored and collected for system performance analysis.

3. Computer resource exhaustion: The testing solution should be able to offer means to manipulate the limit of computer resources, e.g. amount of memory, # of CPU cores, etc. available to O-RAN network functions, e.g. DU-L2. Testing engineers can assess the SUT resiliency and stability under specified negative operation conditions.

4.6 Lab Accreditation

The ORAN ALLIANCE produces test specifications for conformance, interoperability, performance, and security testing while defining criteria for awarding Certificates and/or Badges. In addition, the O-RAN ALLIANCE has defined criteria and guidelines for an Open Testing and Integration Centre (OTIC) as described in Section 3 above and [1].

On the other hand, the International Organization for Standardization (ISO) has defined ISO-17025, which is a standard that specifies the technical and management requirements for testing and calibration laboratories. Accreditation processes, such as ISO 17025, require laboratories to document and demonstrate detailed procedures and processes to protect the integrity and quality of results and measurements produced within the laboratory. To receive accreditation, those procedures and processes must be reviewed by an external accreditation body, typically organized within each country. Each accreditation identifies a specific scope, to which the accreditation applies. Generally, the owner of the testing program will provide and maintain documentation of that scope, such as requirements on how the validity of results is determined, specific laboratory tooling, or verification of that tooling, and other program-specific procedures or requirements.

Establishing ISO 17025 accreditation criteria for OTIC labs would establish consistent and repeatable test methodologies across all OTIC labs. The process of ISO 17025 Accreditation involves auditing laboratories to confirm they are complying to a set of criteria that includes lab facilities, management, and test methodologies. In this case, the ORAN ALLIANCE should establish the criteria for ISO 17025 accreditation of OTIC labs involved in ORAN ALLIANCE testing, like the process used by GSMA and NESAS testing.

With the ORAN Alliance establishing criteria for O-RAN OTIC accreditation and requiring ISO 17025 accreditation, all OTICs awarding ORAN Alliance badges/certificates become unified over the same test methodologies. This can bring consistency across all the OTICs, renounce credibility to OTIC testing. Members of the O-RAN ecosystem should seek ORAN Alliance badges/certificates with confidence that the test results are acceptable across the industry.

5 References

[1] “Overview of Open Test and Integration Centre (OTIC) and O-RAN Certification and Badging Program,” O-RAN White Paper, Apr. 2023 [available online: https://mediastorage.o-ran.org/white-papers/O-RAN.TIFG.Overview-of-OTIC-and-O-RAN-Certification-and-Badging-Program-white-paper%202024.pdf]

[2] O-RAN.WG2.A1TS-R004-v04.02, “O-RAN A1 interface: Test Specification,” Oct. 2024

[3] O-RAN.WG2.R1TS-R004-v01.00, “O-RAN R1 interface: Test Specification,” Oct. 2024

[4] O-RAN.WG3.E2TS-R003-v02.00, “O-RAN E2 Interface Test Specification,” Mar. 2023

[5] O-RAN.WG4.CONF.0-R004-v11.00, “O-RAN Working Group 4 (Fronthaul Working Group) Conformance Test Specification,” Oct. 2024

[6] O-RAN.WG6.O-CLOUD-INTF-CONF-R003-v04.00, “O-RAN O-Cloud Interface Conformance Test Specification,” Oct. 2024

[7] O-RAN.WG4.IOT.0-R004-v12.00, “O-RAN Fronthaul Interoperability Test Specification (IOT),” Oct. 2024

[8] O-RAN.WG5.IOT.0-R004-v11.00, “O-RAN Open F1/W1/E1/X2/Xn Interface Working Group Interoperability Test Specification (IOT),” Oct. 2024

[9] O-RAN.WG6.O-CLOUD-IOT-R003-v01.00, “O-RAN O-Cloud Interoperability Test (IOT) Specification,” Oct. 2024

[10] O-RAN.WG8.IOT.0-R004-v11.00, “O-RAN Stack Interoperability Test Specification,” Oct. 2024

[11] O-RAN.TIFG.E2E-Test.0-R003-v06.00, “O-RAN End-to-end Test Specification,” Jun. 2024

[12] O-RAN.WG11.Security-Test-Specifications.0-R004-v08.00, “O-RAN Security Test Specifications,” Oct. 2024

[13] O-RAN.WG9.XTRP-TST.0-R003-v04.00, “Xhaul transport testing”, June 2024