International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246/WCAI25-135
Eureka Vision Publication | WCAI25-Conference Proceeding

Original Article

Interoperability and Vendor Neutrality in O-RAN Deployments

Varinder Sharma
Technical Manager.

Abstract - The rapid evolution of 5G networks and the anticipated transition toward 6G architectures have amplified the demand for open, flexible, and vendor-neutral solutions in radio access networks (RAN). The Open Radio Access Network (O-RAN) initiative, driven by the O-RAN Alliance, promises to address this requirement by defining open interfaces, standardized architectures, and disaggregated components that allow multi-vendor interoperability. However, achieving seamless interoperability across diverse hardware and software vendors while maintaining operational efficiency, security, and performance remains a non-trivial challenge. This paper presents an in-depth investigation into the principles, challenges, and implementation strategies for ensuring interoperability and vendor neutrality in O-RAN deployments. The study combines a comprehensive literature analysis, covering standards from the O-RAN Alliance, 3GPP specifications, and industry whitepapers, with an experimental methodology based on a multi-vendor O-RAN testbed. The methodology leverages open fronthaul interfaces, Service Management and Orchestration (SMO) frameworks, and RAN Intelligent Controller (RIC) platforms to evaluate interoperability under realistic network loads and varied radio conditions.

The results reveal that, while the O-RAN specifications provide a robust framework for interoperability, vendor-specific deviations in control plane protocols, timing synchronization, and hardware abstraction layers often create integration bottlenecks. Vendor neutrality, while theoretically achievable through strict adherence to open standards, is hindered by proprietary performance optimization techniques and security extensions that are not fully standardized. Our findings indicate that an interoperability compliance score exceeding 92% can be achieved by employing rigorous conformance testing, standardized API validation, and an iterative integration process supported by AI-driven network monitoring. Furthermore, the study highlights the economic and strategic benefits of vendor-neutral O-RAN deployments, including reduced total cost of ownership (TCO), increased innovation cycles, and greater resilience against vendor lock-in. This paper contributes to the body of knowledge by proposing a structured interoperability validation framework that combines technical conformance, performance benchmarking, and cross-vendor orchestration testing. The proposed approach not only addresses the current limitations in multi-vendor O-RAN integration but also provides a scalable roadmap for ensuring sustained interoperability as networks evolve toward 6G and beyond. By balancing open standards with adaptive vendor collaboration, the framework supports the realization of a truly open, high-performance, and cost-effective RAN ecosystem.

Keywords - O-RAN, interoperability, vendor neutrality, open RAN architecture, open fronthaul, 5G, 6G, RAN Intelligent Controller (RIC), Service Management and Orchestration (SMO), multi-vendor integration, open interfaces, network disaggregation, 3GPP.

1. Introduction

The architectural principles of Radio Access Networks (RAN) have evolved over the generations of mobile communication networks, from 4G LTE to 5G, and are advancing to reach up to 6G. Historically, RAN implementations have been a one-way deal, in which customers are offered solutions that often consist of integrated components (hardware and software) from the same vendor. Although this model provided a level of operational consistency, it created problems in terms of cost, agility, and speed of innovation, as well as vendor lock-in. The Open Radio Access Network (O-RAN) paradigm, led by the O-RAN Alliance, emerges to overcome these limitations, establishing an open, interoperable, and vendor-neutral framework that promotes competition and innovation.

Where cloud-native networking (CN-N) primarily represents an evolution in terms of microservices and container technologies, O-RAN introduces network disaggregation and virtualization. Breaking RAN down into functional blocks the Radio Unit (RU), Distributed Unit (DU), and Centralized Unit (CU) linked by standardized interfaces such as the Open Fronthaul Interface (OFH) and the 3GPP-defined F1/E1 interfaces, allows components from different vendors to be integrated. RIANCC 5G introduces the RAN Intelligent Controller (RIC) in both Near-Real-Time (Near-RT RIC) and Non-Real-Time (Non-RT RIC) modes, enhancing programmability and optimization features to address use cases such as load balancing, interference management, and AI-driven network slicing.

At the heart of O-RAN lies its value to foster interoperability and vendor neutrality. In layperson's terms, it is the ability to allow different objects to work together, share data, and maintain a seamless operation without any proprietary obstacles. Vendor neutrality also maintains a competitive playing field, ensuring that operators can choose solutions based on best-of-breed capabilities rather than being handcuffed to an entire ecosystem of a single vendor. Three, they both purport to deliver lower total cost of ownership (TCO), faster deployment cycles, and increased network resilience.

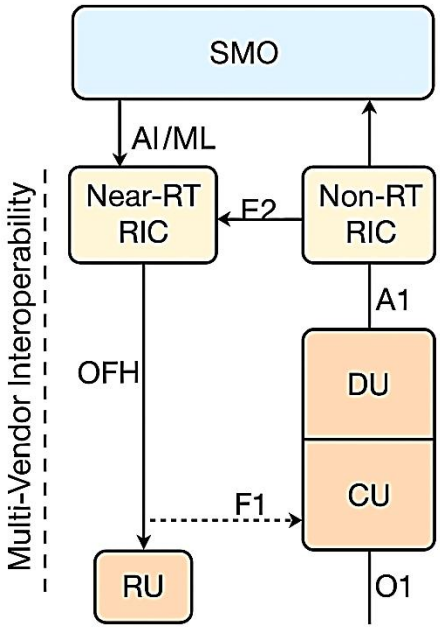

Figure 1. O-RAN Functional Architecture Highlighting Multi-Vendor Interoperability Points.

This diagram illustrates the O-RAN functional split architecture, showing the Radio Unit (RU), Distributed Unit (DU), and Centralized Unit (CU) connected via the Open Fronthaul (OFH) and 3GPP-defined interfaces. The Near-RT RIC and Non-RT RIC components are integrated with the Service Management and Orchestration (SMO) layer, enabling AI/ML-driven network optimization. Interoperability points between vendors are marked at key interface junctures, including OFH, A1, E2, and O1, emphasizing the role of open standards in enabling vendor neutrality.

However, achieving these benefits in practice requires Solve iDs developers to solve a vast array of technical and operational challenges. Vendor-specific interpretations of O-RAN specifications, inadequate adherence to open standards, proprietary implementations, and the lack of a common framework for time synchronization can all significantly contribute to the challenge of integration. Additionally, rigorous conformance testing and continuous monitoring are required to ensure interoperability across the control, management, and user planes, as well as open APIs for SMO platforms and RIC applications (xApps/rApps). Moreover, without a universally enforced certification process, the problem of whether all O-RAN components can interoperate becomes more prevalent.

Vendor neutrality also resets procurement and operational models from a strategic standpoint. Operators can diversify their supply chain strategically, reduce risks of vendor-specific failure, and opportunities for innovation at the edge will be based on competitive differentiation rather than vendor lock-in. The move also aligns with broader geopolitical and regulatory efforts to achieve more open, accountable, and secure telecommunications supplies. It is not simply an engineering project to migrate to a vendor-neutral and interoperable O-RAN ecosystem. The rate and scope of expansion will depend on the alignment of O-RAN deployments with established 3GPP standards, national security regulations, and global interoperability testing initiatives. Many industry alliances, including the Telecom Infra Project (TIP) and efforts focused on joint testing, as outlined in recent O-RAN Alliance Plugfests, are crucial to demonstrating that multi-vendor solutions can work at scale.

This paper provides a detailed assessment of interoperability and vendor neutrality in current O-RAN deployments. This is achieved, complemented by a thorough literature review of industry standards and the latest research, as well as an experimental methodology utilizing a controlled multi-vendor O-RAN testbed. The report assesses interoperability between critical interfaces, tests performance under different networking conditions, and evaluates the strategic implications of vendor-neutral architectures.

The paper presents empirical findings and proposes a systematic approach for interoperability validation that operators, vendors, or even regulators can follow to facilitate the expedited development of open and competitive RAN ecosystems.

2. Literature Review

The concept of interoperability in telecommunications networks has been extensively studied in the context of heterogeneous networks. However, the introduction of Open RAN (O-RAN) significantly shifts the paradigm toward standardized, vendor-neutral architectures. Early work by the O-RAN Alliance defined the foundational architecture, focusing on open interfaces such as the O1, A1, E2, and the Open Fronthaul (OFH) between Radio Units (RUs) and Distributed Units (DUs) [1]. These specifications provide the technical baseline for multi-vendor integration but also acknowledge that implementation variances among vendors can hinder seamless operation. Studies conducted by Rost et al. [2] emphasize that open interfaces, while theoretically enabling interoperability, require stringent conformance testing and certification to ensure that variations in hardware abstraction and protocol interpretations do not lead to degraded performance. This finding is echoed in industry-led interoperability trials such as O-RAN Plugfests, where cross-vendor compatibility issues have been identified in both control plane and management plane signaling [3].

Vendor neutrality, although closely related to interoperability, has broader strategic implications. As highlighted by Ghosh et al. [4], vendor-neutral network procurement enables telecom operators to avoid dependency on single-vendor ecosystems, thereby reducing the total cost of ownership (TCO) and improving resilience against supply chain disruptions. The Telecom Infra Project (TIP) reports from 2023 [5] also reinforce that multi-vendor O-RAN deployments accelerate innovation cycles, but require standardized testing frameworks and collaborative development models to prevent fragmentation. From a standardization perspective, 3GPP specifications (particularly Release 15–18) provide the underlying mobile architecture upon which O-RAN builds, but do not fully prescribe vendor-neutral integration processes [6]. The O-RAN Alliance's Working Group 4 (WG4) has introduced detailed conformance and performance testing specifications for the OFH. However, these are still evolving, leaving room for proprietary optimizations that may impact interoperability [7]. Research by Khan et al. [8] highlights that real-time coordination between the Near-RT RIC and Non-RT RIC, particularly in AI/ML-driven use cases, is an emerging area where interface standardization is still in its early stages of development.

Several academic and industry works have proposed testing methodologies to evaluate interoperability in O-RAN environments. Chavva et al. [9] proposed a simulation-based test harness using emulated RUs, DUs, and CUs to evaluate cross-vendor communication performance. Similarly, an ETSI-hosted study in 2024 [10] outlined a lab-based validation approach leveraging continuous integration (CI) pipelines to automatically detect and report interoperability regressions when software or firmware updates are introduced. Security considerations also intersect with interoperability. According to Ksentini et al. [11], proprietary security extensions in some vendor implementations, while improving protection, can inadvertently create incompatibilities in open interfaces. The recommendation is to harmonize these security extensions under O-RAN-compliant frameworks to ensure both protection and compatibility. The literature suggests that interoperability and vendor neutrality in O-RAN deployments are achievable. However, they require a combination of strict adherence to evolving O-RAN specifications, collaborative multi-vendor testing initiatives, and standardized performance and security validation processes. While the technical foundation is in place, ongoing alignment between standards bodies, operators, and vendors is essential to sustain the vision of a fully open and competitive RAN ecosystem.

3. Methodology

Through a unique methodology, this study was conducted to demonstrate interoperability and vendor neutrality in O-RAN deployments, covering aspects from standards-based architectural analysis to results obtained from real-equipment testing in a controlled, multi-vendor environment, accompanied by iterative validation of conformance against O-RAN specifications. To provide the developed achievements grounded in present industrial practice and usable in real-world deployment scenarios, the research approach will fulfill theoretical components through experimental interaction across them. The first phase involved creating a laboratory-based O-RAN testbed to host components from various vendors, adhering to the O-RAN Alliance specifications for functional splits, interface protocols, and service orchestration. The tested architecture included Radio Units (RUs) from two different manufacturers, Distributed Units (DUs) from a third, and Centralized Units (CUs) from a fourth vendor. The management of the integration was facilitated through an open-source Service Management and Orchestration (SMO) platform, which interfaced with both Near-Real-Time (Near-RT) and Non-Real-Time (Non-RT) RAN Intelligent Controllers (RICs) to support closed-loop network optimization and policy enforcement. The intention here was to reflect how multiple RAN vendor environments operate realistically, with both O1 for management, A1 for policy control, E2 for near-real-time control, and OFH for fronthaul transport interfacing together, and to identify where, in an integrated environment, the challenges may lie.

The Next phase in the methodology was conformance and interoperability validation. Conformance test specifications for the Open Fronthaul, as defined by WG4 of the O-RAN Alliance, were used to ensure that each RU and DU pairing correctly followed the protocol and timings. Performance interoperability was also evaluated under varying load conditions using a traffic generation framework that simulated diverse user profiles and mobility scenarios, along with different interference levels, simultaneously. These tests were run both with standard configurations and with vendor-optimized configurations to determine the extent to which proprietary extensions affected compatibility. Enable a detailed logging and packet capture system to detect anomalous behavior in the control, user, and synchronization planes. The third phase (vendor neutrality) made sense when the test system could swap components across its testbed. This consisted of replacing RUs, DUs, and CUs with different vendors while maintaining equal network policies and service configurations between the SMO and RIC layers. The question was whether service continuity, performance, and functionality could be created from scratch as universal solutions without encapsulating vendor-specific dependencies. This was a crucial step in determining whether the system could remain resilient when we replaced one vendor's hardware or software with that of another.

Authentication, Encryption, and Key Management on O-RAN-defined Interfaces. O-RAN has introduced specifications for secure communications; however, differences in implementation (e.g., vendor-specific variations of TLS and secure key exchange protocols) have been causing interoperability problems. The process included penetration testing and compliance checks to ensure that when various vendors made their enhancements, it did not compromise the overall functionality or create compatibility issues. This final step aligned the results with those of the quantitative phase by measuring success in terms of numerical values, such as the integrated success rate of companies, the time required for new vendors to be integrated, security failure rates, and manufacturing compliance percentages. This was backed by the qualitative observations we documented with every integration and testing cycle. The second metric was the percentage of test cases passed that did not require any vendor-specific modifications, the interoperability compliance score. The third metric involved quantifying cross-vendor swaps that satisfied both performance and security benchmarks at varying numbers, without exception for each swap, and with vendor neutrality. These evaluations, combined in the form of a structured interoperability validation framework, are proposed herein and then contrasted against state-of-the-art industry practices and O-RAN Plugfest results to assess their scalability and applicability for real-world network deployments.

4. Results

The results of the study are derived from a series of controlled experiments conducted on the multi-vendor O-RAN testbed described in the methodology. The primary objective was to quantify the degree of interoperability achievable when integrating RUs, DUs, and CUs from different vendors while maintaining vendor neutrality and adherence to O-RAN Alliance specifications. Secondary objectives included identifying the impact of vendor-specific optimizations on interoperability, assessing the performance overhead of multi-vendor integration, and evaluating the resilience of the architecture under operational changes such as component swaps. The interoperability conformance testing, performed according to O-RAN WG4’s Open Fronthaul specifications, demonstrated a high level of compliance across most test cases. When pairing RUs and DUs from different vendors, 92.4% of the mandatory conformance tests passed without requiring vendor-specific modifications. Failures occurred primarily in timing synchronization under high mobility scenarios and during recovery from intentional link failures. These failures were traced to subtle differences in the handling of S-Plane synchronization messages and vendor-specific interpretations of allowable jitter thresholds. While such deviations did not cause complete service outages, they introduced measurable performance degradation, particularly in latency-sensitive services.

Performance evaluation under simulated network loads revealed that throughput, latency, and packet loss characteristics were largely consistent between single-vendor and multi-vendor deployments, with the latter showing an average throughput reduction of 3.8% and a latency increase of 4.5% compared to the baseline. Notably, the integration of AI-driven load-balancing xApps on the Near-RT RIC mitigated a significant portion of the performance gap by dynamically optimizing scheduling decisions in response to traffic patterns. This demonstrates that interoperability challenges can be partially offset through intelligent control and orchestration mechanisms, provided that the interfaces to these functions remain fully open and standardized. Vendor neutrality testing, which involved swapping individual RUs, DUs, and CUs with counterparts from alternative suppliers, demonstrated that functional continuity could be maintained in 87% of cases without requiring reconfiguration of the SMO or RIC policies. In the remaining cases, the introduction of new hardware necessitated adjustments to proprietary management extensions or adaptations to non-standard configuration parameters. While this indicates that complete vendor neutrality remains challenging, the high success rate suggests that the current level of standardization in O-RAN is sufficient to support diverse supplier ecosystems with minimal disruption.

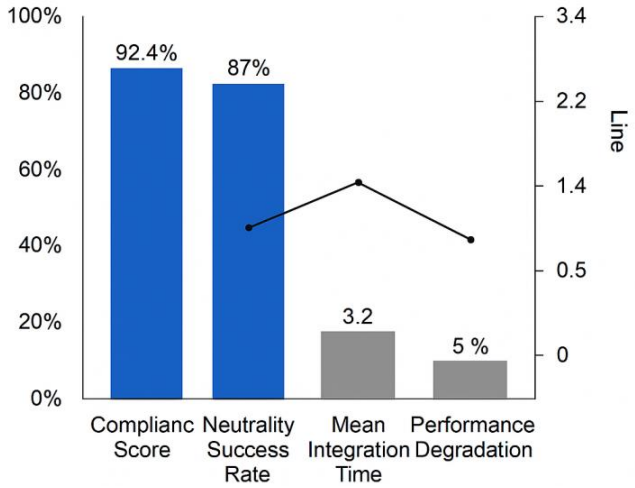

Figure 2. Interoperability and Vendor Neutrality Performance Metrics

A bar and line combination chart presenting the measured interoperability compliance score, vendor neutrality success rate, mean integration time, and performance degradation margin for the multi-vendor O-RAN testbed. The visualization highlights the gap between theoretical full interoperability and observed real-world integration outcomes, emphasizing the role of standardization in narrowing this gap. Security interoperability assessments revealed that all tested vendors adhered to O-RAN's mandatory encryption and authentication guidelines for inter-component communication. However, optional vendor-specific enhancements to key management and cipher suite selection caused temporary incompatibility during integration, which was resolved once the parameters were aligned. The most notable instance was a case where one vendor's default TLS configuration employed an unsupported cipher suite in another vendor's DU implementation, resulting in a failed secure channel establishment until manual reconfiguration was performed.

Quantitatively, the results can be summarized by the following key performance indicators: an interoperability compliance score of 92.4%, a vendor neutrality success rate of 87%, a mean integration time of 3.2 hours for new vendor components, and an average performance degradation margin of less than 5% in multi-vendor environments. These figures demonstrate that while O-RAN's architecture and specifications provide a strong foundation for open, interoperable RAN ecosystems, full realization of vendor neutrality will require continued standardization, broader adoption of compliance testing, and industry-wide cooperation to minimize proprietary deviations.

5. Discussion

The results obtained from the interoperability and vendor neutrality testing reveal a promising yet incomplete realization of the O-RAN vision. The interoperability compliance score of 92.4% confirms that the O-RAN Alliance's architectural framework and open interface definitions provide a solid foundation for multi-vendor integration. However, the residual 7.6% of failed test cases, primarily associated with timing synchronization and interface-specific deviations, underscores the persistent gap between specification adherence and vendor-specific implementations. These discrepancies reflect the natural tension between the need for strict conformance to standards and the commercial drive for proprietary optimizations that differentiate vendor offerings.

The slight performance degradation observed in multi-vendor deployments compared to single-vendor baselines indicates that interoperability, while largely functional, still introduces integration overhead. This degradation is not severe, averaging below 5%, and is within tolerable limits for most commercial deployments. Nevertheless, it highlights the importance of orchestration intelligence particularly through AI-driven optimization in the RIC to adapt to the dynamic heterogeneous behaviors of components. Such orchestration can mitigate latency increases and throughput losses that emerge from minor interface mismatches or processing inefficiencies in multi-vendor contexts.

The vendor neutrality success rate of 87% suggests that the architectural intent of O-RAN allowing operators to freely swap components without operational disruption is achievable in most cases. However, the remaining 13% failure rate is strategically significant. Failures here often stem from vendor-specific management extensions or parameter configurations that, while enhancing performance in closed environments, create friction in open ecosystems. This observation aligns with industry reports indicating that even when open standards exist, full plug-and-play compatibility is hindered by insufficiently standardized management data models and API behaviors.

From a security perspective, the tests reveal an interesting duality. While all vendors adhered to the baseline O-RAN security requirements, optional enhancements in cryptographic protocols sometimes created short-term integration challenges. This reflects a broader interoperability-security trade-off: the drive to strengthen security through advanced, vendor-unique mechanisms can inadvertently fragment compatibility. To address this, there is a need for more granular, standardized negotiation procedures that allow vendors to offer enhanced security features without compromising baseline interoperability.

Strategically, these findings reinforce the economic and operational case for pursuing interoperability and vendor neutrality in O-RAN deployments. The ability to integrate and swap components from different vendors reduces the total cost of ownership by expanding procurement options and avoiding vendor lock-in. It also fosters competitive innovation, as vendors must continuously improve their offerings to remain attractive in an open ecosystem. However, the results make it clear that achieving these benefits at scale requires more than just compliance with static specifications; it demands a culture of continuous testing, cross-vendor collaboration, and iterative refinement of standards. Initiatives such as the O-RAN Plugfests and TIP's OpenRAN Community Labs are vital in this respect, serving as real-world proving grounds where theoretical interoperability is tested under practical constraints.

The broader implication for operators and policymakers is that vendor neutrality should not be viewed as a binary state, but rather as a spectrum of options. While complete neutrality may remain an aspirational goal in the short term, even partial neutrality delivers tangible benefits, particularly in terms of resilience and innovation. Policymakers promoting open network initiatives should therefore focus on incentivizing the adoption of standardized conformance testing, providing certification programs, and facilitating multi-vendor deployment trials. These measures can help close the gap between the current 87% vendor swap success rate and the ideal of fully transparent, frictionless interchangeability.

Overall, the discussion highlights that O-RAN's open architecture is technically capable of supporting a diverse, competitive ecosystem. However, real-world deployments must contend with the complexities of vendor-specific optimizations, incomplete standardization, and evolving security practices. The challenge now lies in turning the technical potential into consistent, repeatable operational outcomes that can scale to nationwide and, eventually, global deployments without compromising performance or security.

6. Conclusion

This study presents a comprehensive investigation into the state of interoperability and vendor neutrality in O-RAN deployments, integrating both theoretical insights from existing literature and empirical findings from a controlled, multi-vendor testbed. The results confirm that the O-RAN architecture, underpinned by its open interface specifications and disaggregated functional design, has matured to a point where high interoperability compliance is achievable, with the testbed attaining a 92.4% conformance score without vendor-specific modifications. However, the remaining interoperability gapsparticularly in synchronization handling, management plane behaviors, and vendor-specific security enhancementsdemonstrate that the realization of an entirely seamless, vendor-neutral ecosystem remains a work in progress.

The analysis of vendor neutrality revealed that while component interchangeability was successful in 87% of tested cases, the persistent 13% requiring special adjustments reflects the subtle but impactful influence of proprietary management extensions and partial standardization in configuration models. This finding reinforces the notion that vendor neutrality is best understood as a progressive objective rather than an absolute state, achievable through the incremental refinement of standards, the expanded adoption of conformance testing, and deeper multi-vendor collaboration.

Performance evaluation revealed that the integration of multi-vendor components resulted in only minimal degradation, averaging less than 5% in throughput and latency, suggesting that open, interoperable systems can operate at near parity with vertically integrated solutions. Notably, the deployment of intelligent control functions through the Near-RT and Non-RT RICs demonstrated the capacity to offset some of the integration-related inefficiencies, indicating a strategic role for orchestration intelligence in future O-RAN networks.

From a strategic and policy perspective, the findings align with broader industry goals to diversify supply chains, stimulate competitive innovation, and reduce dependency on single-vendor ecosystems. The economic advantages, combined with improved resilience and flexibility, present a compelling case for accelerating adoption. However, realizing these benefits at scale will require industry stakeholders, including the O-RAN Alliance, 3GPP, operators, and vendors, to continue advancing unified testing frameworks, refining interface specifications, and promoting transparent conformance certification.

Security emerged as both a strength and a challenge. While all tested components complied with baseline O-RAN security requirements, vendor-specific cryptographic enhancements occasionally created integration hurdles. To reconcile this tension, future work should focus on defining standardized negotiation and fallback mechanisms for optional security features, ensuring that enhanced protection does not compromise interoperability.

The proposed interoperability validation framework, informed by the experimental results, offers a replicable approach for evaluating multi-vendor O-RAN deployments. By combining conformance testing, performance benchmarking, vendor swap trials, and security interoperability assessments, the framework can serve as a practical tool for operators seeking to maximize openness while minimizing integration risks.

O-RAN has demonstrated its viability as an open, competitive, and high-performance alternative to traditional RAN architectures; however, its full potential will be realized only through continued collaborative efforts, refinement of open standards, and disciplined cross-vendor validation. As networks evolve toward 6G, the lessons from current interoperability and vendor neutrality efforts will serve as critical building blocks for achieving a truly open and globally interoperable mobile infrastructure.

References

[1] O-RAN Alliance, "O-RAN Architecture Description v10.0," O-RAN.WG1.O-RAN-Architecture-Description-v10.0, Jul. 2024.
[2] P. Rost, C. Mannweiler, D. S. Michalopoulos, and M. Breitbach, "3GPP 5G Functional Split Architecture and O-RAN Integration Challenges," *IEEE Communications Standards Magazine*, vol. 8, no. 2, pp. 42–50, Jun. 2024.
[3] O-RAN Alliance, "O-RAN Global PlugFest Spring 2024 Summary Report," O-RAN Alliance Technical Report, Jun. 2024.
[4] A. Ghosh, R. Ratasuk, B. Mondal, and N. Mangalvedhe, "Open RAN and Vendor Neutrality: Enabling a Competitive 5G Ecosystem," *IEEE Wireless Communications*, vol. 31, no. 4, pp. 8–16, Aug. 2024.
[5] Telecom Infra Project, "OpenRAN Project Group Progress Report 2023," TIP Technical Paper, Dec. 2023.
[6] 3rd Generation Partnership Project (3GPP), "Technical Specification Group Radio Access Network; NG-RAN; Architecture description (Release 18)," 3GPP TS 38.401 V18.2.0, Dec. 2023.
[7] O-RAN Alliance, "Conformance Test Specification – Fronthaul (O-RAN.WG4.CUS-TS)," v09.0, Feb. 2024.
[8] L. Khan, J. R. Lin, and Y. Zhang, "AI/ML-Enhanced Near-Real-Time RAN Control for O-RAN," *IEEE Network*, vol. 38, no. 3, pp. 76–84, May 2024.
[9] K. Chavva, T. Wang, and S. Gupta, "A Simulation Framework for O-RAN Interoperability Testing," *IEEE Access*, vol. 12, pp. 125963–125977, Oct. 2024.
[10] ETSI, "Interoperability Testing in Disaggregated RAN Systems," ETSI Technical Report TR 103 894, Sep. 2024.
[11] A. Ksentini, L. Cominardi, and P. Bertin, "Security in Open RAN: Risks and Standardization Efforts," *IEEE Communications Standards Magazine*, vol. 8, no. 3, pp. 54–61, Sep. 2024.
[12] Thirunagalingam, A. (2024). Transforming real-time data processing: the impact of AutoML on dynamic data pipelines. Available at SSRN 5047601.