Open road to Open RAN: The challenges and solutions

Dublin, Ireland 2021

Author: Pádraig Ó Seighin

aspire Perfecting Networks

Table of Contents

Executive Summary

Technology adoption is often compared to taking a journey. Your starting point and your intended destination may be clear, but the road to be taken maybe less so.

Mobile network operators (MNOs) are considering the use of Open RAN (radio access networks) more seriously and this is causing significant change and disruption to the mobile network ecosystem. Many Open RAN trials have been completed and most MNOs have committed to using Open RAN at least in parts of their networks.

The journey to introducing Open RAN elements to an existing mobile network will present challenges to the MNO, from network planning to system verification, integration to operation and maintenance and from procurement to SLA management.

Aspire is very active in the Open RAN community. We contribute to the development of Open RAN, through our design, development, integration and benchmarking activities which are now centred in the Aspire Open RAN Lab. We aim to support MNOs to clear the road from many of the obstacles that can be found in the adoption of an Open RAN strategy.

Introduction

Mobile networks have become more complex as they have evolved from 1G in the 1980s to 4G and 5G today. It is clear that the predominantly manual, human-intensive, ways of deploying and operating networks are no longer fit-for-purpose. Mobile networks are now denser, more complicated and support more demanding applications. The successful deployment and operation of 5G (and beyond) needs networks that are robust and simple to deploy, orchestrate and operate. Only autonomous, artificial intelligence (AI)/machine learning (ML)-driven closed-loop RAN management of physical and virtualized RAN functions can deliver this. The industry still has some ground to cover to perfect it though.

Open RAN includes the disaggregation of hardware and software. This means the RAN is composed of software components from different vendors, running on commercial-off-the-shelf (COTS) hardware, communicating over truly open and interoperable interfaces. The key elements of Open RAN are that the networks are open, intelligent, virtualized and fully interoperable.

The standardization of RAN disaggregation started with the 3rd Generation Partnership Project (3GPP) which defined a number of logical splits to enable increased deployment flexibility. It is being further refined by the O-RAN Alliance to provide the open interfaces needed for even further disaggregation.

The O-RAN Alliance reference architecture in figure 1 shows fully open interfaces and a stable structure for vendors of all sizes to develop products in all areas, from xApps (and rApps) on the RAN intelligent controller (RIC) to RRUs.

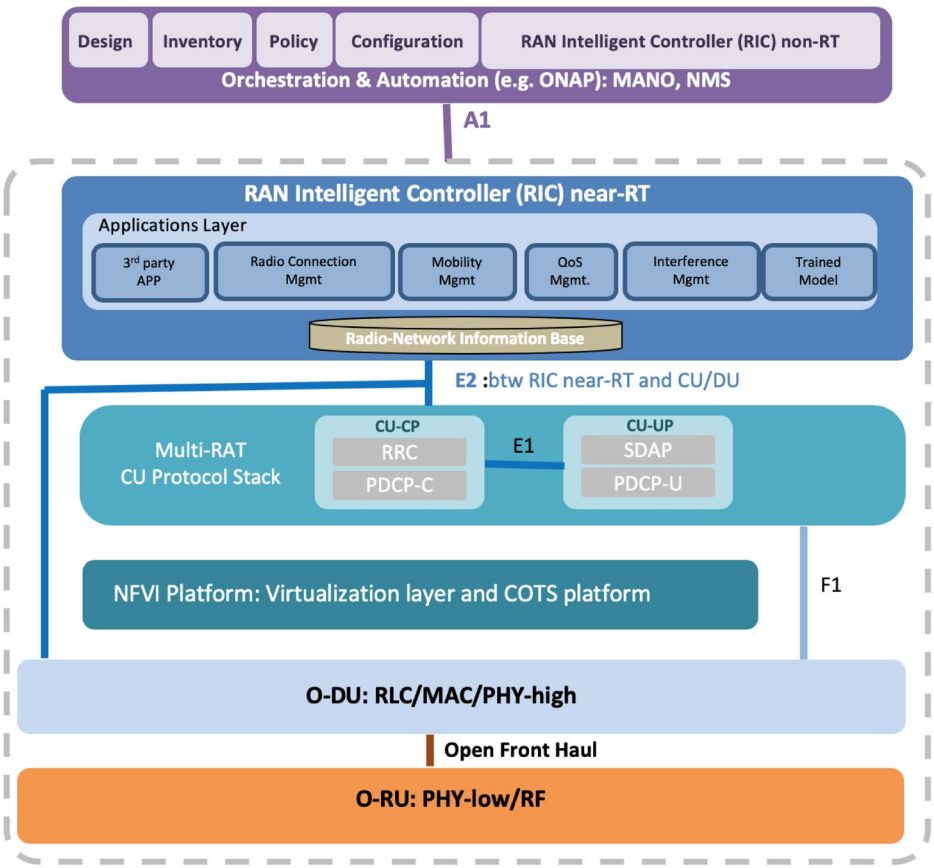

Figure 1: ORAN Reference Architecture From O-RAN Alliance

Challenges & Solutions

There are many stages in the successful development, deployment and operation of a RAN solution. Current ways of working are well understood by both vendors and MNOs but Open RAN adds complexity to those processes, from solution assessment and procurement to successful network deployment and operation.

Traditionally, vendors developed hardware and software solutions for each element of the radio access network, integrated the entire solution in-house and tested it. The MNOs understood that the entire solution was tested, would work with their operations tools and was ready for deployment. This one-stop-shop for a RAN solution had the advantage of a consistent roadmap and one point of contact when there were problems to resolve. Staff training was uncomplicated with a single vendor, institutional knowledge of the solution was easier to build up and development of operational processes was seemingly more straightforward.

With Open RAN solutions, this is no longer the case. Each vendor develops one or more network elements within the overall solution and the level of detail and clarity in the user documentation can vary significantly between the vendors. Integration is more complex and there is no institutional, legacy, knowledge of Open RAN platforms in the MNOs. In conjunction with the well-known and developed skills RAN engineers have used and perfected for decades, new skills are required – skills not traditionally associated with RAN testing and operations but more often used in IT roles such as system administration.

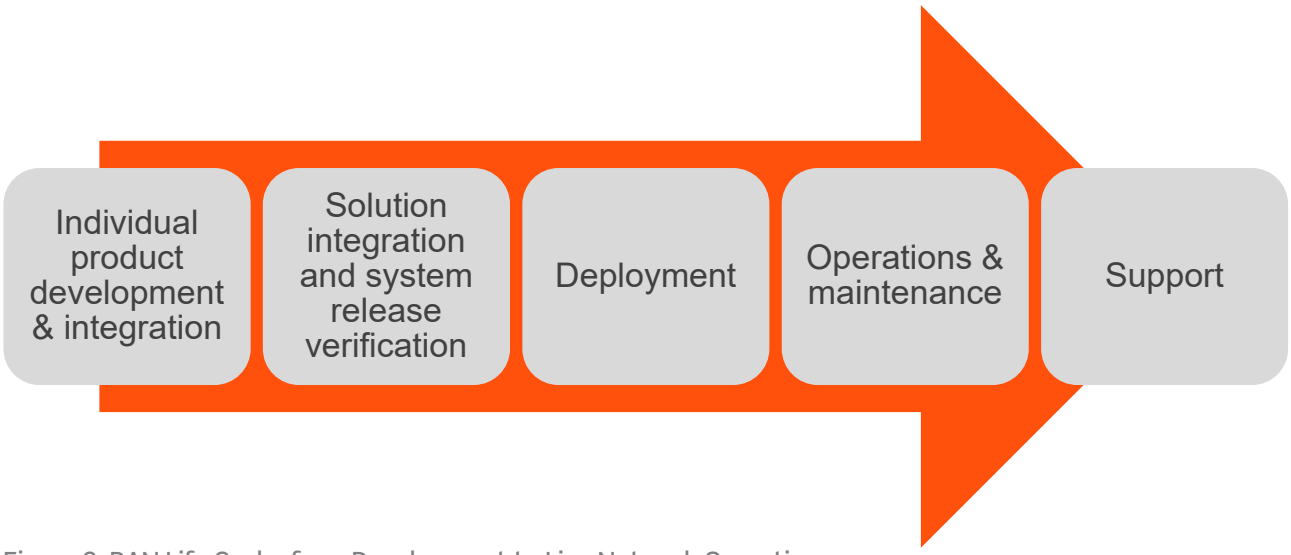

Figure 2: RAN Life Cycle, from Development to Live Network Operations

I. System Verification and Release Validation

Major legacy vendors have always conducted system release validation (SRV) before a major release. It is the integration and test of the whole RAN system, spans multiple product units of the vendor, is iterated with final development cycles and includes inter-radio access technology (RAT) inter-operability verification. There are hundreds of software developers, testers, integration and operations engineers involved in this process across multiple RATs (2G/3G/4G/5G) on a full-time basis. The process is iterative and is typically part of the vendor 's continuous integration development process. Component and system documentation is finalized in a similar process.

Once the vendor is satisfied that the RAN product is working properly – it has reached a suitable level of performance and stability, new functionality works as expected, legacy functionality works as before, system characteristics are within limits, inter-RAT behavior is within scope, system operations are as expected and documentation is complete – it is ready for release. Part of this documentation will be a detailed description of any performance deviations on a component and system level, relative to the previous solution release. The RAN solution is now ready for deployment.

Challenge

This process provides confidence in the new RAN release and MNOs assume this integration and testing has been done properly. In Open RAN, this SRV process, for the entire RAN solution, no longer happens.

Now MNOs will likely do their own testing of new releases. They will install the new RAN solution in a lab environment and run tests to verify the new software. However, these are usually functional in nature and do not verify system behavior under varied conditions, especially high loads, and do not involve verification of all inter-work with a service and management orchestration (SMO) – the MNO expects the vendor to have done all this.

So how do MNOs gain confidence in an Open RAN solution? This is a challenge facing MNOs and Open RAN component vendors – solving it is critical to wide-scale adoption of Open RAN solutions.

Open test and integration centre (OTIC) labs are operator-led initiatives that aim to facilitate the integration and testing of disaggregated RAN components. OTIC labs provide a very useful environment to integrate disaggregated components but, by definition, they do not address SRV.

Could it be that SRV, on which vendors expend a lot of resources, is an unnecessary step and cost? We do not believe it is – if it were, then legacy vendors could save a lot by simply removing the step from the development cycle.

The later in a software product development cycle that a fault is found, the more expensive it is to fix the fault. If it is not found before introducing software to a live network it can be very costly, as we saw in January 1990 when almost 50% of calls in AT&T's long-distance network were not connected for more than nine hours due to a single line of flawed code. At the time, that cost the MNO $60 million with an unknown amount of revenue lost by other businesses who relied on the telephone network (such as hotels, car rental agencies and airlines).

We do not believe MNOs can accept a lower level of confidence in an Open RAN solution. SRV is necessary but it doesn't seem realistic that each MNO will do it. It would lead to SRV duplication as different MNOs plan the use of the same combination of components.

Solution

SRV does not guarantee finding the type of bug that caused such disruption to the AT&T network. But it does mean that the code, hardware and interworking between components are all tested and stressed to higher levels than an integration test. Bugs, from serious software faults to small documentation discrepancies, are always found, and fixed, during SRV. Testing in general is a risk-mitigation exercise. Vendors are prepared to expend a lot of resources to reach a certain level of confidence in a product, and the vendors are primarily integrating and testing products they developed and in which they have deep knowledge, including platform, capabilities and feature interaction.

Though challenging to implement, we believe that a centralized, vendor-neutral approach to integrating and validating systems before they are deployed is an excellent alternative. This would need to be executed by expert independent entities, neither vendor nor MNO, who can coordinate between component vendors to verify the whole solution impartially. While not as exhaustive as currently executed by legacy vendors as part of a CI process, this approach will yield higher confidence levels in, and a greater understanding of, the overall solution.

High levels of automation will be required, as will a blend of traditional IT system administrator as well as RAN testing and troubleshooting skills. Test specifications, using O-RAN Alliance internet of things specifications as a starting point, would be developed and agreed with vendors and MNOs. Initial set-up costs would require a lot of investment, especially in server hardware, testing tools such as UE simulators, automation frameworks, test specifications, reporting structures and training in RAN and IT skills. How to share the cost of this activity, between vendors and MNOs, is just one of the challenges to be overcome.

Independent, end-to-end verification and validation across different vendors would fill this gap in the Open RAN ecosystem.

II. Deployment

With a traditional RAN, once the end-to-end solution has gone through the vendor's internal validation process, it is ready for general sale to MNOs and deployment in their networks. MNOs will do some testing, the scope of which can range from a limited test of a few functions to a more substantial test of a wider range of features and behaviors . However, this testing will never be as extensive as SRV, which covers areas such as features, characteristics, performance under load, operations and stability. The deployment will be done by the MNO, the vendor or by a specialist system integrator (SI), or a combination of these. The new solution is then optimized by a specialist optimization team to reach the radio and other performance targets.

Traditional RAN solution deployments are well understood and well documented thanks to very high levels of competence and experience built up over the years. Optimization of live RAN networks is equally well understood with many experienced optimizers working in legacy vendors, MNOs and service providers.

Challenge

The same levels of experience and competence do not exist for Open RAN solutions and there is no documentation for the entire solution. This leaves a steep learning curve within MNOs, system integrators and service providers and of course, there is no single vendor in Open RAN so the option of using the RAN vendor to do the deployment no longer exists.

Deployment and optimization are labor intensive, but with the deployment of a multi-vendor RAN, deep knowledge of each vendor's solution becomes more difficult to develop.

Solution

A centralized , independent, vendor-neutral approach to integrate and validate systems pre-deployment alternative to execute SRV would help ameliorate this situation. With a concentration of competence, as you would need with SRV, the independent entities executing SRV would become experts in Open RAN components integration and verification. This concentrated, independent, expertise could be leveraged to provide services to MNO and would be a valuable resource to MNOs for training and support, facilitating much more successful deployments.

Automation is crucial to deliver deployment and optimization of multi-vendor RAN solutions. rApps and xApps, deployed within the SMO, will be key to delivering this automation. They can be developed in-house by the MNO, by existing vendors or by independent third-party suppliers.

Though challenging to implement, we believe that a centralised, vendor-neutral approach to integrating and validating systems before they are deployed is an excellent alternative. This would need to be executed by expert independent entities, neither vendor nor MNO, who can coordinate between component vendors to verify the whole solution impartially.

III. Operations and Maintenance

Once a RAN has been deployed, the day-to-day management of it becomes critical for an MNO. The management of the traditional RAN deployments is typically done via a network management system (NMS) from the same RAN vendor. But when an MNO deploys multiple vendors in a RAN, they are probably deployed in separate geographical areas with separate toolsets to manage and operate each part of the network. In a two-vendor RAN, they are essentially two networks with separate, well developed O&M processes and they must be managed as such using O&M platforms that are propriety and vertically integrated, designed to work with one vendor's solution.

With the advent of disaggregated Open RAN deployments, with multiple hardware and software vendors, this is no longer feasible. The O-RAN Alliance has described (within their architecture) the SMO platform, which is a consolidation of a wide variety of management services and provides many network management functionalities, including those needed for RAN.

Challenge

Given the expected complexity of MNO Open RAN networks, due to multiple vendors and new 5G use cases such as network slicing, even a consolidated management system such as SMO would still require significant resources and upskilling to operate. For example, in addition to their radio knowledge, the O&M teams would require a high level of IT knowledge, given the shift from RAN software on propriety hardware to a full NFV system on COTS hardware. To avoid what in essence could be a doubling in O&M team size, there is a clear need for automation through AI/ML.

Solution

Within the SMO, the non-real time RAN intelligent controller (RIC) is a logical function that enables non-real-time control and optimization of the Open RAN elements and resources. The intelligence to enable the automation and orchestration by the SMO is encapsulated within applications which are deployed on the non-real time RIC. These applications, defined as rApps by the O-RAN Alliance, can be developed by the network element vendors, developed by the MNO themselves to achieve bespoke handling to their network, or by independent third-party suppliers who specialize in providing AI/ML solutions within our industry.

The non-real time RIC and the use of rApps will enable the path towards a highly automated O&M of an MNOs RAN, and will be a corner stone in the vision of a zero-touch management system which is being defined in ETSI.

IV. Support Model

While MNOs and Open RAN vendors are still focused on getting the solutions to work and the use cases to be tested and trialled, in some cases in production scenarios, concern about the support model is starting to arise.

Disaggregating the RAN brings a new set of challenges in achieving end-to-end support since the components are from different vendors most likely with separate SLAs and with more room to push responsibilities to any of the other integrated vendors.

Challenge

The challenge with the support model for Open RAN derives directly from the split of responsibilities across functions of the RAN as well the underlying IT infrastructure. Without a single point of contact and with multiple SLAs, how will the MNO manage the support contracts across multiple combinations of CU/DU/RU and IT infrastructure?

Currently, the CU/DU vendor is becoming a natural receiver for all RAN issues, however this brings the issue of independence regarding the root cause, not to mention the SLA management of different vendors will still have to be managed by the MNO.

On top of this, Open RAN vendors are currently focused on research and development and the support organizations are not prioritized, so they will need time to ramp-up.

Solution

The experience of dealing with multi-vendor environments in legacy RAN environments (one core, multiple RAN vendors), proved that the end-to-end support issues were already complicated to handle.

This is exacerbated with further multiplicity of vendors participating in the network, so the simplest solution is to involve an independent third-party that can consolidate the support function for all vendors.

This only works if the third-party has the competency to perform initial root cause analysis and determine which component is creating the fault or performance degradation. In more complex situations in which a patch is required, they must be able to get the vendor engineering involved.

This allows the vendor to have a one-stop-shop for support, while avoiding troubleshooting delays.

The service level agreement (SLA) can be also tied into this one centralized support, with a back-to-back contract which is simple for the MNO to manage, while the third-party deals individually with each participant in the Open RAN environment.

This centralized, vendor-neutral approach is also the solution to validate and integrate systems pre-deployment, including first node implementations of features, new hardware and software.

‘Disaggregating the RAN brings a new set of challenges in achieving end-to-end support since the components are from different vendors most likely with separate SLAs and with more room to push responsibilities to any of the other integrated vendors.’

Conclusion

Open RAN has come along to challenge to the established ways of working for MNOs and network vendors. However, as with any new technology, there is a big effort required to step out of the comfort zone and re-engineer the RAN concept, from selecting the best combination of vendors, to integrating and testing it, deploying and then maintaining, optimizing and supporting it. Attempts to push the old models into Open RAN will most likely result in less desirable outcomes. Across the network life cycle, Aspire has been involved from the very beginning, from research and development to field deployments, while preparing to centralize support. This unique experience, expertise and vendor independence will be crucial to solve the most important challenges of Open RAN adoption as MNOs engage in this new technology and take on the open road to Open RAN.

If you have any questions or would like to further discuss any of the points raised in this white paper, please contact Aspire Technology at solutions@aspiretechnology.com.

‘Across the network life cycle, Aspire has been involved from the very beginning, from research and development to field deployments, while preparing to centralize support. This unique experience, expertise and vendor independence will be crucial to solve the most important challenges of Open RAN adoption as MNOs engage in this new technology.’

Contact Us

111 Q-House,
76 Furze Road,
Sandyford Industrial Estate,
Dublin,
Ireland
Tel: +353 (1) 9022376
info@aspiretechnology.com
www.aspiretechnology.com