Open RAN MoU progress update on maturity, security and energy efficiency

orange TIM Telefónica vodafone

Executive summary

As the momentum behind Open RAN continues to grow, it is natural that relevant experts and decision makers want to understand its progress and how the Open RAN industry has risen to the challenges, in particular relating to **maturity, security** and **energy efficiency**. Over the course of 2022, Open RAN MoU Operators encouraged an open dialogue about Open RAN and have taken steps to understand concerns and address valid questions. This paper represents a progress report that helps to showcase the gains and set the agenda for 2023. In summary:

Maturity

The technology gap between traditional RAN and Open RAN is closing. Considerable Open RAN deployments are already visible in markets such as the UK and North America, facilitated by government support. In Europe, small deployments (trials) are already in place, new pilots are announced for this year and larger scale deployments are expected from 2025. A key focus in 2023 will be around maturity of 5G for urban areas and minimising system integration overheads by maturing certification delivered through industry communities.

Security

Open RAN MoU Operators are strengthening cooperation with relevant national authorities to share information on security, implementation and management of Open RAN networks. Reports such as the EU NIS (Network & Information Systems) Co-operation Group's assessment of Open RAN security have helped develop strong security controls for specification, development, procurement, system integration, testing and operations. Open RAN MoU Operators have requested to formally include Open RAN as part of the GSMA (Groupe Speciale Mobile Association) NESAS (Network Equipment Security Assurance Scheme) and the EU´s 5G certification scheme defined by ENISA (European Union Agency for Cybersecurity).

Energy efficiency

The availability of energy-efficient hardware combined with sleep modes is helping Open RAN at least match the energy efficiency of traditional RAN. Open RAN MoU Operators collaborate with the industry to increase the energy efficiency of all the Open RAN building blocks, with particular focus on radio transmitters and cloud infrastructure. In addition, they are proposing a general framework for energy monitoring, focusing on tools and methodologies to measure power consumption at all possible levels of the Open RAN system. Such reporting of power metrics in real time, combined with the native intelligence offered by the Open RAN architecture will unleash fully automated management of the network energy efficiency. This will eventually allow Open RAN to outperform the traditional RAN.

1. Technical and ecosystem maturity and readiness

Message 1

The technological gaps between traditional RAN and Open RAN are melting away. Some areas such as non-complex macro RUs (e.g., single-band products, non mMIMO and low power products) and cloud platforms are already close to enabling large-scale deployments in various markets. Other areas such as complex macro radios (e.g., mMIMO, multi-band products, particular band combinations, etc.) may require deployment commitments to accelerate the enlargement of the range of product alternatives while RIC (RAN Intelligent Controller) platforms and the corresponding app ecosystem need further development.

Rationale/explanation

- Although performance optimisations are still monitored and discussed (e.g. mMIMO uplink performance in the mobility case), some products are maturing quickly and catching up with established vendors' products in different categories (e.g. virtualised baseband platforms, small cells, enterprise networks). Various macro network and enterprise deployments all over the world are proof points of that maturing process. Other areas still need to improve as a result of a lack of development, standards maturity or large-scale deployments.

- Radio units with specific band combinations only needed by some operators in certain geographical areas are still underrepresented in new vendors' portfolios. While traditional RAN vendors maintain a large family of radio variants for the various global regions, new vendors need to focus on products with high volume and revenue expectations. That excludes highly efficient multi-band radios with operator-specific band combinations, and those in combination with legacy radio access technologies (RATs) such as 2G.

- The RICs are entry points for small or medium enterprises (SMEs) or established companies from non-RAN areas and thus drive vendor diversity in the RAN area. Considerable advancements have taken place from technical and use-case perspectives in the area of non-real time (non-RT) and near-real time (near-RT) RIC. Nevertheless, open issues like conflict mitigation between applications or use cases which require both non-RT and near-RT RIC remain to be solved. Moreover, the relevance of use cases still needs to be quantified in field deployments, particularly for the near-RT RIC.

- Related to RIC interface standardisation, A1 and E2 interfaces are complete with example A1 type definitions and E2 service models. However, multi-vendor implementations based on standards compliant E2 and A1 interfaces have not yet shown up in the market. Standardisation of xApp and rApp APIs is still ongoing, thus a stable reference standard for onboarding third-party xApps and rApps on RIC platforms is still needed.

- From a standardisation perspective, the open fronthaul interface is the first that has been adopted by ETSI (ETSI TS 103 859) and implemented in commercial products (aiming at large scale deployments). This includes IOT test cases and conformance test specifications defined by O-RAN ALLIANCE.
- A lot of standardisation work is done for O-Cloud with many specifications for deployment scenarios and use case requirements. However, standardisation of the O2 interface is still not fully developed in terms of API data models and detailed information elements. The same applies to the acceleration abstraction layer (AAL) specs.

Message 2

Global deployments are now reaching thousands of sites but are mainly executed by new operators in greenfield deployments. Brownfield deployments lag due to the captive situation operators face (vendor lock-in) with modernisation cycles under current contracts and some missing key features. In Europe, small-scale deployments are already in place and major deployments are expected from 2025. Considerable Open RAN deployments are already visible in markets such as the UK and North America, facilitated by government support. Nevertheless, efficient deployments in brownfield operator environments require the support of both 4G and 5G in Cloud RAN, which would enable deployments of off-the-shelf HW, Cloud SW and related tooling for automation and life cycle management.

Rationale/explanation:

- Large-scale deployments involving Open RAN elements are present only outside Europe currently. In countries such as the USA, India or Japan, the Open RAN or partial Open RAN (vRAN) deployments are progressing, e.g. Verizon vRAN deployment (10000 sites deployed out of 20000 by 2025), Dish (>10000 5G Open RAN sites), NTT Docomo (10000 5G Open RAN sites) while an initial Open RAN deployment started in the UK. Other non-fully O-RAN compatible solutions are being deployed in high volumes by Rakuten in Japan.

- In Europe, the main factors delaying the Open RAN adoption (besides the closing, but still existing gap on maturity) in tier-1 operators' brownfield deployments are existing contractual obligations with regards to traditional network solutions and the challenging financial situation that operators and service providers are currently suffering from. The latter factor has the potential to restrict operators from planning additional investment in network renewal, and so delay Open RAN adoption at scale. New contracts for the next modernisation cycle will be the vehicle for the wide scale introduction of Open RAN in the second half of the decade in Europe.

- Despite initial delays in Europe, some operators have made some strong commitments towards Open RAN deployments, such as the one from Vodafone committing to have 30% of their network in Open RAN by 2030, or from Orange announcing progress with their European network upgrades, only featuring O-RAN compliant products from 2025.

Message 3

Industry communities are working together more collaboratively to ensure complementarity between certification frameworks. Still, the system integration challenge of Open RAN is not solved and communities, together with operators and vendors, need to make further joint progress on procedures to establish a strong universal certification system executed in open labs.

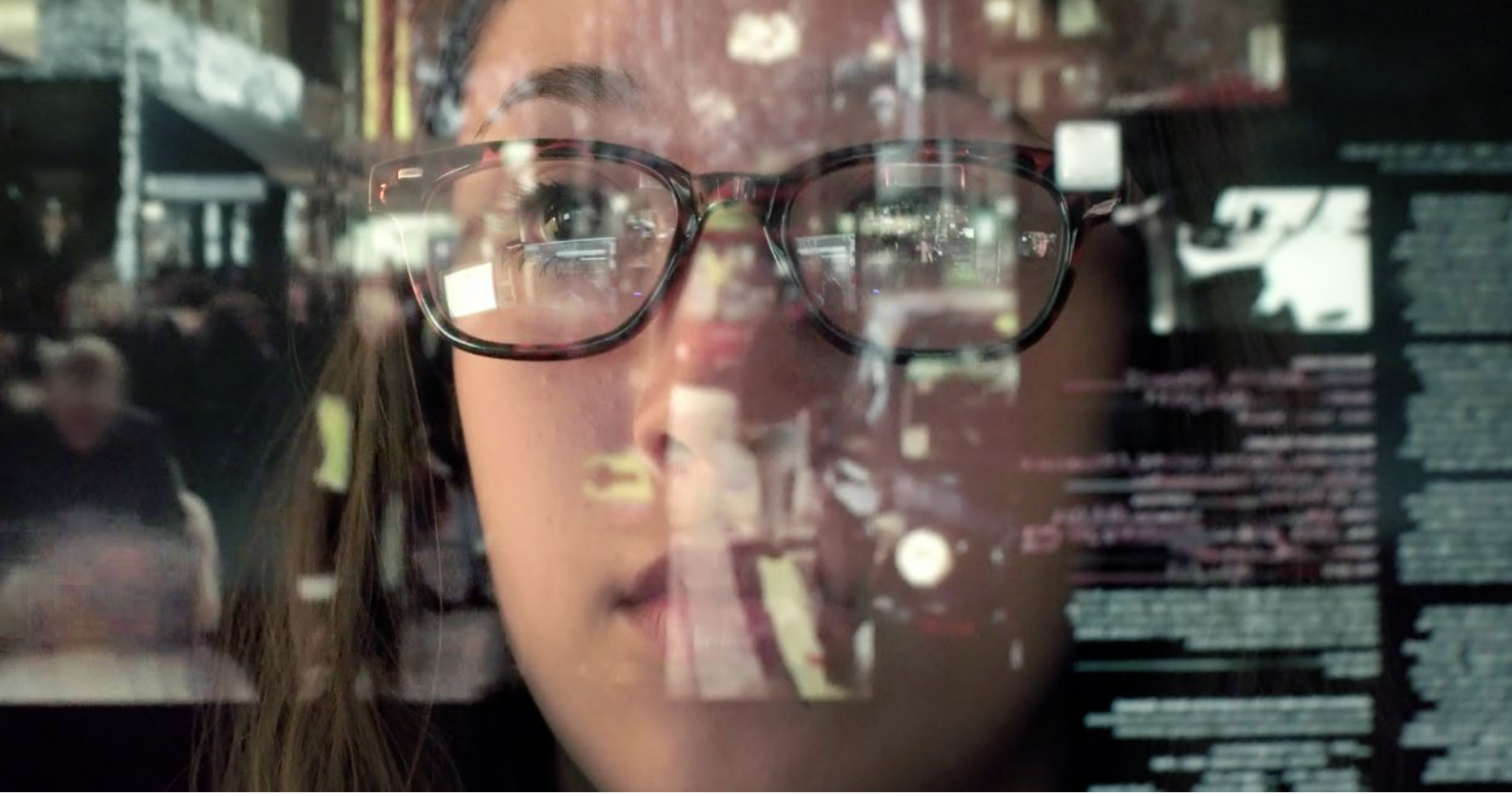
Rationale/explanation:

- The ultimate goal of Open RAN MoU operators is for certification to become sufficiently robust that any operator could request certificates as a prerequisite for taking part in RFP processes should it wish, promoting an efficient supply chain. Therefore, a well-working, scalable certification system for the compliance of interface conformance functional/non-functional features executed by leading open labs is a necessity to minimise the added system integration effort of a multi-vendor Open RAN solution. Certification and badging systems need to be maintained by organisations that are well supported by both operators and vendors, and independent from single companies or authorities.

- The O-RAN ALLIANCE is the undoubted authority on Open RAN interface standards in terms of their specification and certification. A validation framework around compliance of interface conformance and interoperability has been put in place by the test and integration task force (TIFG) while work groups (particularly work groups 4 and 5) published initial test specifications to enable early certification processes in open test and integration centres (OTICs). O-RAN ALLIANCE is an open organisation, coordinating healthy cooperation among vendors and operators, with the majority of major vendors and suppliers signed up as O-RAN ALLIANCE members and the rest of the industry encouraged to join.

- The Open RAN group of the Telecom Infra Project (TIP) is destined to become the authority on product and system functional/non-functional features certification. While a certification system framework has been put in place and is heavily supported by Open RAN MoU Operators, open issues exist in the areas of lifecycle management as well as scalability, and these need to be sorted out jointly. Furthermore, operators and vendors need to take a more active role in supporting TIP in developing and implementing relevant validation plans to enable certification prior to RFP shortlisting. Various major vendors still stay away from becoming TIP members. Reasons may be rooted in a more restrictive IPR (intellectual property rights) policy or the more centralised approach to certification. These hesitations should be overcome to enable worldwide acceptance of TIP certification and badging.

- Both organisations should be complementary in their scope. A major step towards that was made in 2022, when TIP and O-RAN ALLIANCE announced an agreement on mutual acceptance of certificates and badges within the own certification activities. However, detailed work on specific areas such as end-to-end system certification still needs to be conducted for both organisations to maximise complementarity.



- Open labs slowly pick up the Open RAN certification frameworks. While more and more labs around the globe open their doors, only few have executed certification tests on O-RAN ALLIANCE specs. No silver or gold badges have yet been issued based on TIP blueprints. Moreover, a methodology to gain trust between labs and operators still needs to be implemented. In a trustful environment, operators could acknowledge certificates to reduce cumbersome retesting even if they were issued by a lab the operators rarely deal with.

- Requirements and validation procedures to test against need to be globally organised in a transparent and maintainable way. In 2021, the Open RAN MoU group initiated a technical priorities workstream to prepare a list of important RAN requirements, and issued a second release in 2022. This set of requirements is intended to act as valuable input into TIP's Open RAN Release Framework, which could then be used as the basis of the certificates that operators need. After a selection process, those requirements can form a set of requirements as global basis for certificates. Validation procedures should be open sourced and test results made available to operators.

- The best work split between open and operator labs will evolve over time. A highly efficient Open RAN validation ecosystem could process the bulk of required tests in open labs and reduce operator tests to custom requirements. By differentiating between global base and regional specific requirements, the needs of different geographical areas can be considered in open lab testing. Common entry/exit criteria should be defined to drive a clear transfer process between vendor, open and operator labs.

- A process for lifecycle management of certificates is required to enable updates to existing certification requirements while technology advances. It creates the operational heartbeat around certification and enables less advanced vendors to certify against older versions of requirements if needed.

- Vendor-specific certification approaches are currently evolving to fill the existing gap for a global certification system. For the sake of highest efficiency, those proprietary certification systems should ideally end up in the global certification frameworks of relevant organisations as soon as those are mature.

2. Security

Open RAN MoU Operators are making significant progress towards more secure Open RAN deployments by implementing recommendations published by the NIS Cooperation Group in May 2022.

Message 1
Collaboration with national authorities

Open RAN MoU Operators are strengthening cooperation with relevant national authorities to share information on the security, implementation and management of Open RAN networks. Open RAN MoU Operators already collaborate with national authorities in countries such as the UK, Germany and Italy by providing information on the progress made in security specification and testing as well as on deployment plans, where relevant.

Rationale/explanation

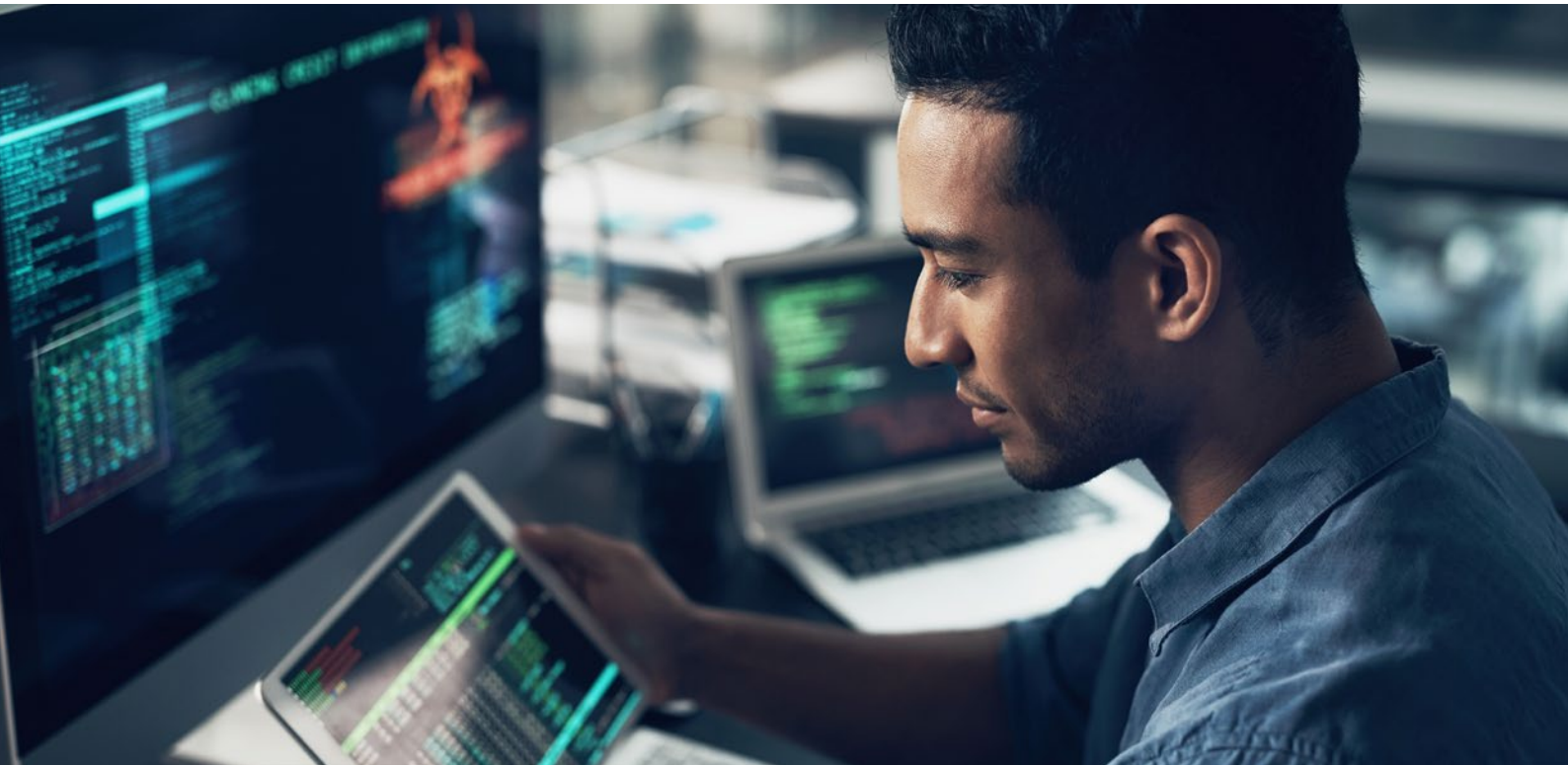
- Open RAN MoU Operators are strengthening collaboration with national authorities to ensure security baseline requirements are met and that the risk profile of vendors are correctly captured and assessed (EC NIS SM01-SM02).
- Open RAN MoU Operators are also collaborating with industry bodies such as GSMA and O-RAN ALLIANCE to provide Open RAN security testing specifications. These specifications from initial deployments are to be taken as input for the definition of a standard testing specification (EC NIS SA01-SA02-SA06).
- Open RAN MoU Operators commit to carrying out security hardening testing, considering but not limited to O-RAN ALLIANCE Release 3 and any future security assurance scheme requirements such as NESAS or 5G certification scheme that will incorporate Open RAN. O-RAN Security Test Specification 3.0 provides test specifications for common network security tests, e.g. network protocol fuzzing guideline, software composition analysis, Software Bill of Materials (SBOM) verification, Open Fronthaul Point-to-Point LAN Segment security verification based on 802.1x port-based network access control, and O1 interface Network Configuration Access Control (NACM) verification. Vendors and operators can use these tests to assess the security of their products and deployments.

Message 2
Introduction of a security controls

Open RAN MoU Operators are committed to strong security controls throughout the life cycle of Open RAN. This includes: specification, development, procurement, system integration, testing and operations. As a minimum, MoU Operators will apply all the mandatory controls defined by the O-RAN ALLIANCE and 3GPP security specifications. MoU Operators will also require the same security controls to be enforced across Open RAN supply chains.

Rationale/explanation

- The introduction of Open RAN will not be an exception to any mandatory cybersecurity policy requirements such as controls that prevent unauthorised access to the network (EC NIS TM03). To reinforce the software integrity, as well as update and patch management (EC NIS TM07), Open RAN MoU Operators will consider CI/CT/CD (continuous integration, continuous testing and continuous deployment) tools from multiple vendors. Requirements in this area will be requested as part of ongoing RFI/RFQ (request for information/request for quotes) activities on CT/CD solutions.
- Moreover, Open RAN MoU Operators will ensure suppliers commit to enforcing industry recognised security assurance standards in the software development phase. This will help to detect potential threats by malicious users especially on Open Fronthaul interface and rApps/xApps. Automation is also required for periodic vulnerability scanning.
- In addition to automated testing, manual penetration testing activities will be conducted, especially when new components and suppliers are introduced.



3 Message 3
Supplier assurance

Open RAN MoU Operators commit that their future Open RAN procurements and RFQs will ensure mandatory compliance by Open RAN suppliers (products and individual components) with security specifications. As a minimum, this would include, for example, O-RAN ALLIANCE specifications, as well as operator security policies and any requirements from national authorities.

Open RAN MoU Operators already follow a Zero Trust approach towards every vendor. Furthermore, in future the risk profile of suppliers (and third parties) will include an assessment against the criteria in the EU Coordinated Risk Assessment.

Rationale/explanation

- Any Open RAN suppliers that participate in individual MoU operator procurement and RFQ processes will be required, as a minimum, to comply with industry established standards and specifications such as 3GPP and O-RAN ALLIANCE, as well as any requirements from national authorities and operator security policies.
- Furthermore, Managed Service Providers (MSPs) will be evaluated in the same way as equipment suppliers (EC NIS SM04). MSP and third-party vendors will be required to comply with mandatory operator security controls, as well as new 5G certification schemes (ENISA), GSMA NESAS and industry badges e.g. TIP.

4 Message 4
Certification

Open RAN solutions must be as secure as traditional RAN and should be subject to the same official security assurance and certification processes. Open RAN MoU Operators have therefore requested that Open RAN should be part of both the 5G certification scheme being defined by ENISA and the next release of the GSMA NESAS security assurance scheme. Furthermore, through their participation in other industry fora (e.g. TIP/O-RAN ALLIANCE), Open RAN MoU Operators will work to support the inclusion of security features in any certification schemes.

Rationale/explanation

- From an early stage, there is an opportunity to introduce Open RAN as part of the ENISA 5G certification scheme and GSMA NESAS. These schemes are currently under definition so that all future Open RAN equipment has the same level of security assurance and certification as the conventional 5G equipment (EC NIS TM09-10 and SM01). Open RAN MoU Operators also commit to collaborate with the national authorities on O-RAN cloud implementation (EC NIS TM10).
- Furthermore, Open RAN MoU Operators will continue to collaborate, sharing best practices, looking to publish these where helpful, and defining additional requirements for potential inclusion by standard and certification bodies (EC NIS SA01).

Message 5
Secure by design

Open RAN MoU Operators are addressing outstanding gaps in security specifications through the O-RAN ALLIANCE. For example, Working Group 11 has introduced new security control mechanisms on A1(OAuth 2.0) and O2 (mTLS) interfaces defined in release 3.0 specifications. These were completed in November 2022 and will be published in February 2023. Open RAN MoU operators have also created a parallel Security Working Group that is creating a comprehensive set of security requirements as part of the Open RAN MoU Technical Priorities workstream.

Rationale/explanation

- Please refer to Annex 1 on security specifications progress.

Message 6
Vendor diversity and collaboration with European suppliers

Open RAN MoU Operators re-iterate their commitment to collaborate with a wide range of suppliers, including European incumbent suppliers and SMEs, to ensure a multi-vendor strategy.

Rationale/explanation

- Diversity will increase resilience and help develop a European ecosystem that will accelerate commercial readiness, increase competition and drive innovation. Open RAN MoU Operators will consider future funding opportunities such as the SNS Partnership Project for large-scale trials by consortiums of European players.
- Open RAN MoU Operators are independently assessing a wide range of suppliers to potentially supply the elements of every layer in the stack, strengthening the collaboration with European vendors (EC NIS SM03, SM05). To foster diversity and collaboration, the Open RAN MoU Operators encourage consideration of both new as well as incumbent suppliers (EC NIS SM08).

3. Energy efficiency

Energy efficiency of Open RAN systems is making progress, with the availability of energy-efficient hardware combined with mechanisms to activate sleep modes on both radio transmitters and cloud infrastructure. While the initial target is to at least match the energy efficiency of traditional RAN solutions, Open RAN will eventually be more energy efficient thanks to intelligence, with real-time monitoring, automated switch-on/off, adaptation to traffic, and native AI/ML (artificial intelligence/ machine learning).

Message 1

Progress is being made in the industry to increase the energy efficiency of all Open RAN building blocks, with particular focus on radio transmitters and cloud infrastructure.

Rationale/explanation

For radio transmitters:

- O-RUs contribute the greatest part of the total power consumption of the Radio Access Network (around 80%), so it is essential that Open RAN O-RUs are at least as energy efficient as in traditional RAN.
- It is worth mentioning that traditional O-RUs show a wide range of energy-efficiency performance between suppliers (up to 25-30%).
- Currently, Open RAN O-RUs' energy efficiency already falls within the typical range seen with traditional RAN, and they should further improve and reach best-in-class performance.
- Furthermore, enhancements are being considered in the O-RAN ALLIANCE to replicate the sleep mode features available with traditional vendors, allowing control of the O-RU shutdown modes by the O-DU through the Open Fronthaul interface. Several features are being considered for specification in the O-RAN ALLIANCE (e.g., shutdown with different granularity: symbol, channel, and carrier).
- Open RAN MoU Operators have defined energy-efficiency targets for O-RU in both loaded and unloaded conditions, as part of their technical priorities contribution to TIP's ongoing Release Framework, the output of which may be used for benchmarking with traditional RAN.

For cloud infrastructure:

- The baseline energy efficiency of cloud infrastructure is improving in the industry, thanks to progress in the efficiency of CPU (central processing unit) and accelerator technologies, but also cooling systems for servers.

- Recent progress has been made thanks to the latest evolution of chipset and accelerator technologies, with the introduction of in-line accelerators and more integrated chipsets natively optimised for lower power consumption.

- Progress is also being made thanks to cooperation between hardware and software providers of cloud infrastructure. Their activity aims to dynamically adapt the power consumption of servers depending on load, making use of CPU features to modify the voltage and frequency of processors, eventually switching-off unused CPUs thanks to reallocation of active workload to specific accelerators and/or CPUs.

- Open RAN MoU Operators have performed a complete review of all the cloud infrastructure hardware elements to be optimised, considering not only processors but also sub-components such as memory storage, NIC cards, fans, power supply. The objective of this review is to identify relevant monitoring and energy-saving features, and automation mechanisms.

Message 2

Open RAN MoU Operators are developing a general framework for energy monitoring. This framework focuses on tools and methodologies to measure power consumption at all possible levels of the Open RAN system, with the ability to differentiate consumption between network functions. Relying on a common API structure, a unified test methodology for rating energy consumption for different configurations, different loads, etc. should allow apple to apple comparisons of Open RAN solutions across vendors. Ultimately, this should enable energy efficiency of Open RAN to be benchmarked against traditional RAN. Open RAN MoU Operators intend to promote the resulting framework (standardised in ETSI for a harmonised methodology) for use across the whole industry.

Rationale/explanation

- Open RAN MoU Operators are promoting open APIs at all levels of the Open RAN system to monitor the power consumption of all possible hardware elements, based on an interoperable framework. In particular, operators are pushing for the monitoring of O-RUs and of most sub-components of the cloud infrastructure. While the O-RAN ALLIANCE has primarily focused on CPU optimisation, Open RAN MoU Operators wish to extend monitoring to a variety of server components including accelerators, memory storage, NIC cards, and fans, while also capitalising on open APIs made available by the IT industry.
- Open RAN MoU Operators have also prioritised the need for the O-Cloud to provide power, energy and environmental (PEE) parameters and measurement data at the workload level (e.g. pod, CNF, etc.)
- Open RAN MoU Operators have plans to carry out a comprehensive set of lab and field measurements of Open RAN systems during 2023.

Message 3

Intelligence will eventually allow Open RAN to be more energy efficient than traditional RAN, thanks to real-time monitoring, intelligent switch-off, adaptation to traffic, and native AI/ML offering more granularity in terms of managing energy of RAN elements.

Rationale/explanation

- Open RAN MoU Operators have prioritised four different use cases being considered by the O-RAN ALLIANCE, with the first specifications being published in Q2 2023.
  - Carrier and cell switch off/on
  - RF channel reconfiguration off/on
  - Advanced sleep modes
  - O-Cloud resource energy saving mode
- Open RAN MoU Operators are consolidating an AI/ML architecture framework (to be made publicly available) which would be capable of tackling the optimisation of energy efficiency.
- More specifically, Open RAN MoU Operators are also addressing the question of conflict management between RIC applications, allowing further operator control on the prioritisation of actions to reach the best trade off between energy efficiency and network performance

ANNEX 1 – Progress on security by design (specifications)

1. Where we were one year ago

The O-RAN ALLIANCE Security Work Group (WG11) continues developing O-RAN specifications that enable mobile network operators to operate an Open RAN that meets and exceeds industry expectations for an open, interoperable, and secure system.

https://www.o-ran.org/blog/the-o-ran-alliance-security-work-group-continues-defining-o-ran-security-solutions

The WG11 work is captured in four security specifications that are the pillars of the O-RAN security architecture. The WG11 specifications that were approved in 2021 are accessible on the O-RAN ALLIANCE web site at https://www.o-ran.org/specifications.

One year ago we had:

O-RAN Security Threat Modelling and Remediation Analysis 2.1

O-RAN WG11 conducted a risk-based security analysis in accordance with ISO 27005 to help define an effective O-RAN security architecture that manages and decreases risks to the overall O-RAN system.

O-RAN Security Requirements Specifications v2.0

Requirements address confidentiality, integrity, and availability protection by considering key controls such as authentication, authorisation, replay protection, least privilege access control, and zero-trust, among others.

O-RAN Security Protocols Specifications v3.0

This document specifies security protocols used by O-RAN compliant implementations. It defines implementation requirements for SSH, IPSec, DTLS, TLS 1.2, TLS 1.3 (compliant also with NIST) and NETCONF support over secure transport.

O-RAN Security Tests Specifications v1.0

This new specification document provides a description of the Security Tests which validate security functions, configurations and security protocols requirements and is the first step toward verifiability of O-RAN security requirements. It contains a set of tests to validate proper implementations of security protocols as defined in O-RAN Security Protocols Specifications (SSH, TLS, DTLS and IPSec). Tests for O-RAN components related to transversal requirements defined in O-RAN Security Requirements are specified for networks protocols and services, DDoS attack protection, password protection policies and vulnerability scanning.

2. Summary of O-RAN ALLIANCE progress last year

WG11's work is captured in four security specifications that form the pillars of O-RAN security. All WG11 updates to the specifications are publicly accessible on the O-RAN ALLIANCE web site.

O-RAN Security Threat Modeling and Remediation Analysis 4.0

Updates: the document now covers the O-Cloud and additional threats against the Open Fronthaul interface.

O-RAN Security Requirements Specifications 4.0

Updates:

- Non-RT RIC and rApps - added security requirements and controls
- Near-RT RIC and xApps - added security requirements and controls
- O-Cloud Software Package Protection - added security requirements and controls
- A1 Interface authentication and authorisation - added security controls
- Open Fronthaul CUS planes - added security requirements and controls
- Open Fronthaul LAN segment - extended security controls
- R1 interface - added security requirements and controls

O-RAN Security Protocols Specifications 4.0

Updates:

- Addition of DTLS and IPsec requirements, alignment of TLS 1.2 and TLS 1.3 profiles with 3GPP TS 33.210, update the O-RAN security protocols and specifications to include mandatory support for TLS 1.3

O-RAN Security Tests Specifications 3.0

Updates:

- Network protocol fuzzing, software bill of materials (SBOM), open fronthaul point-to-point LAN segment, O1 Interface Network Configuration Access Control Model (NACM) validation

Interface Security Controls

Table 1 shows the interface controls which are mandatory to support. Details can be found in O-RAN Security Requirements Specifications 4.0, O-RAN Security Protocols Specifications 4.0, and O-RAN Management Plane Specification 9.0.

Security control	A1	O1	O2	E2	Open Fronthaul			
					C-plane	U-plane	S-plane	M-plane
Authenticity	TLS	TLS	TLS	IPsec				TLS/SSH
Confidentiality	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH
Integrity	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH
Authorisation	OAuth	NACM	OAuth					NACM
Data origination	TLS	TLS	TLS	IPsec				TLS/SSH
Replay prevention	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH

Table 1 Mandatory O-RAN interface security controls

Authorisation for the E2 interface is being developed in collaboration with the near-real time RIC and E2 interface work group. PDCP requirements are specified by the 3GPP in TS 33.501.

Table 2 lists the optional security controls on the open fronthaul interfaces with details in O-RAN Security Requirements Specifications 4.0. All MOU Operators will make the support of IEEE 802.1X mandatory within their own networks and network equipment. WG11 is also currently working with other O-RAN work groups to mandate support of IEEE 802.1X, and all MoU Operators are also supporting the change from optional to mandatory in O-RAN ALLIANCE specifications.

Security control	Open Fronthaul		
	C-plane	U-plane	S-plane
Authenticity			
Confidentiality			
Integrity			
Authorisation	802.1X	802.1X	802.1X
Replay prevention			

Table 2 Optional open fronthaul interface security controls

Universal requirement

Universal requirements apply to all O-RAN elements and in some cases will make certain aspects of Open RAN more secure than traditional RAN deployments. Table 3 lists the mandatory O-RAN requirements for each category of universal requirements with details in O-RAN Security Requirements Specifications 4.0.

Category	Mandatory requirements
Application lifecycle management	• Application signature by vendor • Signature validation by SMO
Robust protocol implementation	• Handle unexpected inputs without functional compromise
Robustness of OS and application	• Known vulnerabilities in the OS and applications shall be documented by their providers
Password-based authentication	• Mitigate risks from password authentication attacks where password authentication is implemented
Software supply chain security	• Vendor signed, NTIA compliant with SBOM with every O-RAN software delivery

Table 3 Mandatory O-RAN security requirements

3. Requirements under development

The O-RAN ALLIANCE web site also has WG11 studies on the near real-time RIC and xApps, the non-real time RIC and the O-Cloud that are driving the development of security standards in these areas. Table 4 provides a quick reference of the new security work underway and how it will improve O-RAN security.

Category	Description
SMO	• Develop security requirements for SMO functions and internal SMO communications • Identify risks with external data sources and specify security requirements for external interfaces • Identify risks to SMO and O-Cloud via the O2 interface and specify security controls for the SMO, O-Cloud, and O2 interface
Non-RT RIC	• Already completed work to develop security requirements for the E2 interface • Define requirements for the secure on-boarding of rApps
Near-RT RIC and xApps	• Develop additional security requirements or the near-RT RIC and xApps • Specify authorisation requirements for E2 interface • Define requirements for the secure on-boarding of xApps • Identify risks to the Near-RT RIC platform via external interfaces for RAN analytics information exposure
Fronthaul C/U/S Planes	• Complete requirements to support IEEE 802.1X Supplicant function within the O-RU, O-DU, TNE, FHM, FHG, and O-Cloud • Complete requirements to support IEEE 802.1X Authenticator functions for the O-DU and O-Cloud • Complete optional requirements to support IEEE 802.1X Supplicant functions for the TNE, FHM, and FHG • Collaborate with ITU-T and IEEE on the possibility of using IEEE 1588 PTP integrated security to secure the S-Plane • Study MACsec requirements for improved security of the open fronthaul
O-Cloud	• Identify and assess risks to acceleration abstraction layer (AAL) and SMO components managing the O-Cloud through O2 interface using ISO 27005 and STRIDE methodologies • Derive security requirements for the O-Cloud
Automated Certificate Management for O-RAN	• Specify a comprehensive framework for automated X.509v3 certificate management based on CMPv2 and ACME
Security Log Management	• Specify a comprehensive framework for security log management across the O-RAN architecture
AI/ML Security	• Study the threats to machine learning • Develop controls to prevent attacks against the machine learning applications implemented within the non- and near-real time RIC
Application Life Cycle Management Security	• Create security requirements for development, testing, onboarding, operations, and maintenance of O-RAN applications
O-RU Centralised User Management	• Study centralised user management for O-RUs.

4. Cooperation with ETSI steps for ETSI PAS – as road to standardisation

In September 2022, ETSI and O-RAN ALLIANCE announced that ETSI had adopted the first O-RAN specification as ETSI TS103 859, namely 'O-RAN Fronthaul Control, User and Synchronization Plane Specification v7.02'.

The O-RAN Security Work Group (WG11) is starting to collaborate with ETSI on the transformation of the O-RAN security specifications into ETSI Technical Specifications (TS) or Technical Reports (TR) following the ETSI PAS (Publicly Available Specifications) process. As with other O-RAN technical specifications, the aim is to benefit from ETSI´s recognition as a European Standards Organisation, as well as from ETSI´s international reputation as a provider of standards for global use. Submitting a PAS to be published as an ETSI TS is a first step towards it becoming a European Standard. O-RAN security specifications are expected to go through the ETSI PAS process by the end of this year.

Reference to ETSI PAS: https://www.etsi.org/images/files/ETSI_PAS_Process_Guide.pdf