NTIA Technical Memorandum 23-568

5G Challenge Preliminary Event: Evaluating Modular, Interoperable, Multi-Vendor, Open RAN Solutions

Margaret H. Pinson, Mark Poletti, Julie Kub, Jeremy Glenn, Tim Thompson, Robert Kupsh, Naser Areqat, Okmar Dharmadhikari, Annie George, T. Lauriston Hardin, Cory Johnson, Spiros Kapoulas, Sundar Sriram

Technical Memorandum

NTIA Memorandum 23-568

5G Challenge Preliminary Event: Evaluating Modular, Interoperable, Multi-Vendor, Open RAN Solutions

Margaret H. Pinson, Mark Poletti, Julie Kub, Jeremy Glenn, Tim Thompson, Robert Kupsh, Naser Areqat, Okmar Dharmadhikari, Annie George, T. Lauriston Hardin, Cory Johnson, Spiros Kapoulas, Sundar Sriram

U.S. DEPARTMENT OF COMMERCE

Alan Davidson
Assistant Secretary of Commerce for Communications and Information
National Telecommunications and Information Administration

May 2023

DISCLAIMER

Certain commercial equipment, materials, and/or programs are identified in this report to describe aspects of the ways that Open RAN solutions are being introduced at present or may be introduced in the future. In no case does such identification imply endorsement, approval, recommendation, or prediction of success by the National Telecommunications and Information Administration, nor does it imply that the equipment, materials, and/or programs identified are necessarily the best available for achieving an open, modular, interoperable 5G market. The mention of any commercial equipment, material, or program should not be construed as that they are in any way superior to or more noteworthy than similar ones not mentioned.

CONTENTS

FIGURES

GLOSSARY OF TERMS

3GPP	3rd Generation Partnership Project
ARPANET	Advanced Research Projects Agency Network
CD	continuous delivery
CI	continuous integration
COTS	commercial-off-the-shelf
CT	continuous testing
CU	Central Unit
DDOS	distributed denial of service
DOCSIS	Data Over Cable Service Interface Specification
DoD	Department of Defense
DU	Distributed Unit
E2E	end-to-end
EO	Executive Order
FCC	Federal Communications Commission
FDD	frequency division duplex
FTP	File Transfer Protocol
gNB	gNodeB, refers to 5G Next Generation Node B
ICMP	Internet Control Message Protocol
IE	Information Element
IT	information technology
ITS	Institute for Telecommunication Sciences
IoT	Internet of Things
IOT	interoperability test
KPI	key performance indicator
L1	layer 1 (physical layer)
L2	layer 2 (data link layer)
L3	layer 3 (network layer)
MAC	Medium Access Control
MNO	mobile network operator
MSSP	Managed Security Service Provider
NOI	Notice of Inquiry
NTIA	National Telecommunications and Information Administration
O-CU	Open RAN central units
O-DU	Open RAN distributed units
O-RAN	Open Radio Access Network; *O-RAN* refers to the O-RAN ALLIANCE and the group's specifications for open interfaces in the RAN
O-RU	Open RAN radio units

OTIC	Open Test and Integration Center
OUSD	Office of the Under Secretary of Defense
PDCP	Packet Data Convergence Protocol
PHY	physical layer
RAN	Radio Access Network
radalt	radar altimeter
RIC	Radio Intelligent Controller
RLC	Radio Link Control
R&E	Research and Engineering
RF	radio frequency
RRC	Radio Resource Control
RTP	Real-time Transport Protocol
RU	Radio Unit
SA	standalone
SBOM	Software Bill of Materials
SDAP	Service Data Adaptation Protocol
SDN	software defined network
SUPI	Security Permanent Identifier
TCP	Transmission Control Protocol
TDD	time division duplex
TS	Technical Specification
UE	user equipment
µTP	Micro Transport Protocol (sometimes also uTP)
UX	user experience
VEX	Vulnerability Exploitability eXchange
vRAN	virtualized radio access networks

5G CHALLENGE PRELIMINARY EVENT: EVALUATING MODULAR, INTEROPERABLE, MULTI-VENDOR, OPEN RAN SOLUTIONS

Margaret H. Pinson,[1] Mark Poletti,[2] Julie Kub,[1] Jeremy Glenn,[1] Tim Thompson,[1] Robert Kupsh,[1] Naser Areqat,[1] Okmar Dharmadhikari,[2] Annie George,[3] T. Lauriston Hardin,[1] Cory Johnson,[1] Spiros Kapoulas,[2] and Sundar Sriram[2]

Today's mobile wireless networks comprise many proprietary solutions with custom, closed-source software and hardware. Changes to these proprietary elements require complex and meticulous verification of the entire network. This dynamic increases costs, slows innovation, reduces competition, and makes security issues difficult to detect and fix. Our vision is to accelerate adoption of 5G open interfaces, interoperable components, and multi-vendor solutions by fostering a large, vibrant, and growing vendor community dedicated to advancing 5G interoperability towards true plug-and-play operation. This memo describes the "5G Challenge Preliminary Event: RAN Subsystem Interoperability" conducted by the U.S. in 2022. Contestants submitted Open RAN radio units (O-RU), distributed units (O-DU), and central units (O-CU). We evaluated each subsystem individually in an emulated environment. Our tight testing timeline consisted of one week of preparation and two weeks of emulated wraparound testing. We then integrated subsystems from multiple vendors to create an end-to-end network. In true plug-and-play fashion, contestants approached network integration with no prior experience interoperating with their fellow contestants' subsystems. The 5G Challenge provided a rigorous five-week schedule for end-to-end integration and testing. Contestants worked through diverse issues, from software options to discrepant hardware. This successful event demonstrated end-to-end data communication sessions using multiple protocols across a multi-vendor, interoperable, Open RAN architecture.

Keywords: 5G, interoperability, network testing, SBOM, open interfaces, Open RAN

1. INTRODUCTION

Today, mobile networks typically consist of proprietary software integrated into customized hardware designed by a single mobile network supplier. Network upgrades or fixes require systematic deployment and validation to each of the network subsystem functions and, in some cases, lead to an entire network overhaul. Mobile operators are locked into the development, release pace, and schedule of the network supplier, which can significantly impact network

[1] These authors are with the Institute for Telecommunication Sciences, National Telecommunications and Information Administration, U.S. Department of Commerce, Boulder, CO 80305.
[2] These authors are with CableLabs, Louisville, CO 80027.
[3] This author is with Kyrio, Louisville, CO 80027.

operation, offered services, and deployment plans. This industry dynamic increases costs, slows innovation, and reduces competition.

The industry is attempting to change this single vendor paradigm ("vendor lock") by developing industry standards to disaggregate proprietary software from the hardware and open proprietary interfaces between network subsystems and functions to allow for network supplier interoperability.

In response, the National Telecommunications and Information Administration's Institute for Telecommunication Sciences (NTIA/ITS), in collaboration with U.S. Department of Defense's (DoD) Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) deployed the 5G Challenge to accelerate the adoption of open interfaces, interoperable components, and multi-vendor solutions—specifically focused on the Radio Access Network (RAN). NTIA/ITS, the U.S. government's spectrum and communications lab, works to realize the full potential of telecommunications to drive a new era of innovation, development, and productivity. OUSD(R&E) serves as the primary advisor to DOD leadership on all matters pertaining to the Department's Research and Engineering (R&E) enterprise, technology development and transition, developmental prototyping, experimentation, and administration of testing ranges and activities.

CableLabs, the host lab for the *5G Challenge Preliminary Event*, is the leading innovation and R&D lab for the cable industry. CableLabs creates global impact through its member companies around the world. With a state-of-the-art research facility and collaborative ecosystem with thousands of vendors, CableLabs delivers impactful network technologies for the entire industry. CableLabs has experience working with diverse Wi-Fi vendors to achieve interoperability and harden the Data Over Cable Service Interface Specification (DOCSIS). The 5G Challenge builds on CableLabs' experience as an independent arbitrator and host of industry interoperability events.

In the envisioned future 5G market, Open RAN interfaces reflect clear-cut requirements, enabling true plug-and-play operation. Modular 5G elements let network operators quickly and easily reconfigure, update, or replace components as needed. External scrutiny of open interfaces allows vulnerabilities to be identified and patched. This open, modular, interoperable environment attracts and incentivizes new vendors. A diversified marketplace delivers targeted innovation and drives down costs. International allies and partners can establish secure, trusted supply chains. Beneficiaries of this future 5G market include DoD, international allies and partners, network operators, businesses, and consumers.

The 5G Challenge is a two phase, multi-year prize challenge. This memo describes phase one—the *5G Challenge Preliminary Event: RAN Interoperability Event* in 2022—during which NTIA/ITS offered a $3,000,000 prize purse to contestants who successfully integrated hardware and/or software solutions for one or more of these 5G network subsystems: Central Unit (CU), Distributed Unit (DU), or Radio Unit (RU). The second phase, the *5G Challenge Final Event*, began in 2023.

The *5G Challenge Preliminary Event* had three stages. In Stage One, competitors submitted white paper applications to participate in the competition and were required to have one or more

5G Open RAN subsystems that adhere to the 3GPP standards and O-RAN ALLIANCE specifications. In Stage Two, each contestant's Open RAN subsystem was evaluated separately in an emulated environment. In stage three, multiple vendors integrated their Open RAN subsystems into an end-to-end (E2E) network. Each winning contestant submitted a Software Bill of Materials (SBOM), and a prize was awarded for the best SBOM.

In true plug-and-play fashion, contestants approached network integration with no prior experience interoperating with their fellow contestants' Open RAN subsystems. The 5G Challenge's integration stage provided a rigorous five-week schedule for contestants to work through diverse issues, from configuration options to discrepant hardware.

2. BACKGROUND

2.1 Single Versus Multi-vendor Solutions

2.1.1 Historical Dynamics Between Mobile Operators and Network Suppliers

The pre-5G wireless industry converged around monolithic, E2E solutions from one-stop vendors. This market consolidated into a small number of major infrastructure vendors. Although 3GPP standards include interface specifications, little to no interoperability existed between equipment from different vendors. Tier 1 mobile network operators (MNO) deployed a single vendor's equipment throughout large geographic regions. MNOs treated these proprietary solutions as black boxes. Older network equipment tended to be proprietary, function-specific hardware built with custom manufactured chip sets. Replacing or updating network equipment was expensive and time consuming, involving 6 to 12 months of pre-deployment testing to avoid user experience (UX) problems. This increased costs and limited network flexibility for specialized use cases.

The single-vendor model suited Tier 1 MNO customers. The single-vendor model simplified procurement, deployment, E2E integration, and troubleshooting—one source to blame and one vendor to troubleshoot.

Let's fast-forward to today. Computer systems in general have experienced cost reductions and improved security due to advances in virtualization, softwarization, continuous integration / continuous delivery / continuous testing (CI/CD/CT), Agile software development, and other modern software development lifecycle practices. Vendor equipment is adopting some of these advances—particularly virtualized radio access networks (vRAN)—but lags in other areas (e.g., CI/CD/CT).

Governments around the globe have made available vast new quantities of spectrum in multiple frequency bands. This has led to new spectrum owners and new ownership categories (e.g., mining, utilities, public safety, and manufacturing), each with novel and distinct use cases and requirements (e.g., higher throughput, lower latency, higher security, and many endpoint connections). These scenarios do not align with purchasing from a single, E2E infrastructure vendor because no single vendor can specialize in everything. This next generation of network operators requires a more diverse ecosystem of vendors to meet their new use case requirements. Many of these network operators would like to replace older solutions that poorly serve their needs. Many of the new operators support a paradigm shift to multi-vendor, disaggregated 5G solutions—as do some of the Tier 1 MNOs.

Other Tier 1 MNOs are interested in multi-vendor solutions but require confirmation—like demonstrated interoperability, scaled deployment, vendor longevity assurance, measured energy savings, load balancing, spectrum efficiency, or new service offerings. Also, most Tier 1 MNOs must solve the brownfield problem (i.e., how to integrate multi-vendor 5G equipment with pre-existing, single-vendor networks). There are many "flavors" of 5G, and their brownfield equipment may not strictly adhere to 3GPP interface specifications (e.g., due to the implementation of options available within the specification). The 5G Challenge tackles a critical

first step towards addressing these concerns for multi-vendor RAN solutions, by requiring compliance with 3GPP interface standards and O-RAN ALLIANCE specifications and by demonstrating E2E, multi-vendor integration.

2.1.2 A New Model with 5G

The 3GPP reference architecture for 5G defines multiple discrete and interoperable core functions and their interfaces. 3GPP releases 14 and 15 [1] introduce the concept of decomposing the gNB into CU, DU, and RU. The RAN is the final link in the wireless network between the network and the handset (aka user equipment (UE)). The Open RAN decomposes into the RU, DU, and CU.

The RU converts radio signals sent to and from the antenna into a digital signal for transmission (handling the front end and parts of the physical layer as well as digital beamforming functionality). RU development requires specialized skills around issues such as antenna design, radio frequency (RF) filter design, interference, and propagation. For example, the introduction of 5G systems in the U.S. between 3700 and 3980 MHz has raised concerns about electromagnetic compatibility with airborne radar altimeter (radalt) receivers operating between 4200 and 4400 MHz [2]. As a result, most presently available RUs include function-specific hardware.

The CU and DU can be deployed on commercial-off-the-shelf (COTS) servers. When compared to the RU, COTS deployment simplifies the engineering skill sets needed for development and maintenance (e.g., computer programming and information technology (IT)). The DU is typically deployed on a COTS server that likely has hardware-based accelerators. The DU is responsible for real-time layer 1 (L1, physical layer) and lower layer 2 (L2, Radio Link Control (RLC) and Medium Access Control (MAC)), which contains the data link layer and scheduling function. The CU is responsible for non-real-time, higher L2 and L3 (network layer) functions (i.e., Radio Resource Control (RRC), Service Data Adaptation Protocol (SDAP), and Packet Data Convergence Protocol (PDCP) protocol stack functions).

However, for the RU, 3GPP defines a RAN functional split architecture and leaves it to the global vendors to differentiate themselves and decide how layer 1 and 2 functionality should be "split" between the RU and the CU/DU. As shown in Figure 1 [3], vendors have multiple functional split options. Vendors can therefore create CU/DU and RU split options that apportion protocol layers differently, in response to specific customer use cases and deployment scenarios (e.g., delay and throughput requirements and fronthaul bandwidth availability). This "option 2" split appeals to MNOs because it enables innovation around transmitters and receivers (e.g., to lower power consumption) with minimal impact on the rest of the network.

To standardize the Open Front Haul interface (between the DU and RU), the O-RAN ALLIANCE proposes a version of the split 7.2 (called 7.2x) that splits the physical layer (PHY) into a high-PHY and low-PHY. The O-RAN ALLIANCE's 7.2x split provides a balance between functionality, time-to-market, and deployment cost. The 7.2x split option objectives are explained in detail by Dell Technologies [4]. O-RAN ALLIANCE also specified two variant splits (7.2a and 7.2b) generically based on where precoding occurs.

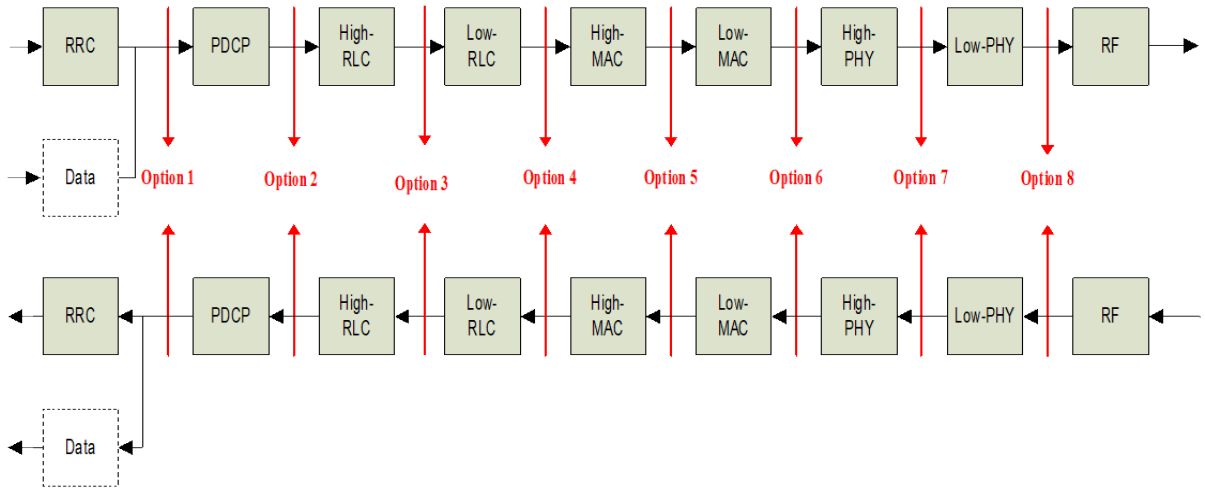

Figure 1. 5G RAN Functional split between central and distributed units
(see also 3GPP TR 38.801, Figure 11.1.1-1)

2.2 O-RAN ALLIANCE Specifications

3GPP Release 14 outlines and Release 15 clearly defines the DU and CU as well as the F1, E1, Xn, and NG interfaces between them and the core network [5] but neither Release defines the service management framework and interfaces for the RAN to operate within an orchestrated and automated cloud environment (see Figure 2). For the RAN, note that if the interfaces between the CU, DU, and RU are not open,[4] the RAN itself is not open (leading to vendor lock) [6]. The O-RAN ALLIANCE's mission is to re-shape the RAN industry towards more intelligent, open, virtualized and fully interoperable mobile networks. O-RAN ALLIANCE specifications enable a more competitive and vibrant RAN supplier ecosystem with faster innovation to improve user experience [7].

Open RAN is based on years of research on open and programmable networks (based on software-defined networking transformation) [8]. Open RAN deployments are based on disaggregated, virtualized, and software-based components, connected through open and standardized interfaces, and interoperable across different vendors [9]. The Open RAN vision driven by the O-RAN ALLIANCE [10] starts with the disaggregated RAN.

The four foundational principles for O-RAN ALLIANCE specifications include disaggregation; intelligent, data-driven control with the RAN Intelligent Controllers (RIC); virtualization; and open interfaces [9]. Disaggregation splits the base station into different functional units per 3GPP standards for the 5G Next Generation Node B's (gNBs) [6]. Near–Real-Time and Non–Real-Time RICs and Closed-Loop Control allow near–real-time and non–real-time data-driven, closed-loop control over RAN optimization and orchestration [11]. The RICs enable finer grain control of radio resource management and virtual/physical network functions (e.g., for policy

[4] We use "open" here to mean a well-defined, standardized interface with specific information exchange that enables multi-vendor communication.

applications for scheduling, handover, RAN slicing, and load balancing based on network load and/or resource utilization). O-RAN virtualization extends software defined network (SDN) concepts [12], decoupling hardware and software components to enable automated deployment of RAN functionalities on COTS hardware.

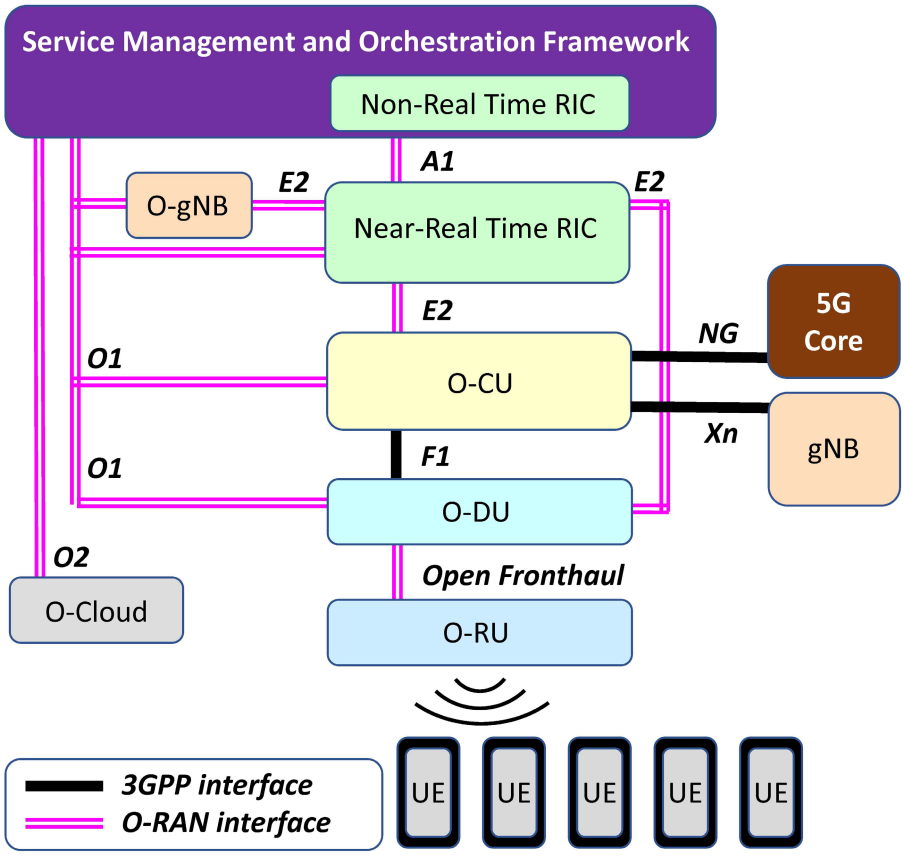

Figure 2. O-RAN logical architecture (see also O-RAN Architecture Description 7.0 [13])

The O-RAN ALLIANCE specification, beyond 3GPP, further disaggregates the RAN functionality by defining three open interface specifications between the three RAN elements. These open interfaces include:

- Open Fronthaul, connecting the RU and DU
- Midhaul, also called F1 as defined by 3GPP, connecting the DU and CU
- Backhaul, also called NG as defined by 3GPP, between the RAN and the Core

Disaggregating the RAN elements (RU, DU, and CU) into interoperable components connected by open interfaces further allows network operators to use equipment from multiple vendors and still ensure interoperability. O-RAN decouples hardware and software into three layers: the COTS hardware, a software abstraction layer, and an application layer where the RAN functions

reside. O-RAN ALLIANCE has specified a list of requirements for a cloud platform that supports the execution of O-RAN network functions. This is referred to as the O-RAN Cloud Platform, or O-Cloud.

2.3 Plugfests

O-RAN ALLIANCE plugfests (currently with over 80 participants worldwide) focus on topics such as multi-vendor interoperability using O-RAN's open interfaces, RAN virtualization, and RICs. During the plugfest, participants showcase such aspects of their products as interoperability with another vendor's subsystem, conformity to a standard, or interoperability with respect to a specific use case or use cases. Plugfest participants know who they will be working with well in advance. Participants may work jointly for several months prior to the plugfest and then for another few months during the plugfest [14]. Plugfests typically do not involve E2E testing.

The 5G Challenge's goal differs from typical plugfests because the 5G Challenge tests "cold" vendor groupings (i.e., unknown partners). This supports more of a plug-and-play architecture versus a pre-prepared use case demonstration created solely for the plugfest.[5] Additionally, the 5G Challenge focuses first on testing individual components with wraparound (or bracket) testing, then exposed interfaces, and finally E2E testing. At the 5G Challenge, vendors are assigned to interoperate with other vendors without any prior knowledge of the other vendors' equipment or of the interoperability test plan. Competitors need to work together to win the challenge. This builds camaraderie among vendors, as each is motivated to assist the others in order that all may succeed.

2.4 Security

2.4.1 Importance of 5G Security

Cybersecurity is especially important in 5G networks because of a vastly increased routing attack surface and continued Internet of Things (IoT) device vulnerabilities. Dynamic cloud-based routing infrastructure is replacing traditional hardware-based routing. Previously, security controls could focus on a limited number of routing devices. Now, routing is occurring in a vast array of virtualized routers spread throughout the network. Future 5G networks are expected to integrate billions of small IoT devices throughout their networks and throughout every facet of our lives: the grocery store, emergency room, and even the battlefield. While there are now robust IoT security standards, there will always be unpatched and extremely vulnerable devices [15].

2.4.2 Security Gaps and Exposures

Upgrading networks from 4G/LTE to the new 5G standard will provide revolutionary improvements in all facets of the security triad: confidentiality, integrity, and availability. At the

[5] From private communications with Ian Wong, Viavi.

core of this advance is the ability to shift from legacy technology to virtual, distributed, cloud-based networks, which enable a host of critical defense-in-depth and virtualization security techniques.

One of those advantages is distributed denial of service (DDOS) protection and mitigation on the edge of networks to prevent larger outages. When attempting to provide high levels of availability to a wireless customer, service providers are vulnerable to motivated and well-resourced attackers using DDOS techniques that could quickly spread through large parts of a network. 5G allows such attacks to be identified and stopped at the network edge without causing more catastrophic outages [16]. Another important advantage of 5G is the use of stronger encryption schemes for the Security Permanent Identifier (SUPI) and over-the-air interface.

Legacy network communication security has long been plagued by a necessary level of trust between different network components. Some of the original packet-switched networks like the Advanced Research Projects Agency Network (ARPANET) relied on complete trust between every communication node, and we have been playing catch-up from that paradigm ever since. More recent network security models utilized a hardened perimeter, but trust was implied within the internal network. That 5G relies on the "zero trust" networking model is thus an important security upgrade. In this model, no information received is trusted unless it can first be verified.

2.4.3 O-RAN Potential for Improved Security

O-RAN seeks to build on the security strengths of 5G by offering more visibility to network operators throughout the network stack [17]. Modern professional enterprise security organizations use a powerful suite of tools and techniques that are best served by an open flow of information and access and are hindered by proprietary protocols and interfaces. For example, a vendor may be unfamiliar with alerts generated by non–O-RAN devices. Threat hunting is frequently outsourced to Managed Security Service Providers (MSSPs).

Within the security community there is a longstanding debate about the value of "security by obscurity." If an attacker is unfamiliar with a system's configuration or cannot find it, there are certain security advantages. The opposing viewpoint is that open interfaces enhance the ability of automated tools and community development to find and fix vulnerabilities.

One major objection to O-RAN is that standardized interfaces and protocols remove a defender's ability to use obscurity to their advantage. A provider can no longer leverage the advantages offered by proprietary, black-box infrastructure configurations. This is a valid concern. However, from a security perspective, the numerous potential advantages offered by O-RAN (discussed in Sections 2.2 and 2.4.2) vastly outweigh the potential disadvantages.

The FCC *List of Equipment and Services Covered by Section 2 of the Secure Networks Act* [18] identifies equipment and services that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons. In response, numerous entities have replaced (or seek to replace) their telecommunications equipment and services. The 5G Challenge is motivated in part by the desire to facilitate improved security from future telecommunications equipment and services. However, standalone (SA) 5G equipment

was in the very early stages of development when the *5G Challenge Preliminary Event* was designed and launched. Therefore, our lab tests focused on interface compliance and basic operational capability. Separate projects will be needed to assess compliance with O-RAN ALLIANCE security protocols and to test various aspects of network security.

3. SOFTWARE BILL OF MATERIALS

3.1 What is the SBOM?

The concept of the SBOM is that all components and dependencies of a software program must be recorded in a single, easily accessible format that can be audited for security risk and vulnerabilities [19], [20]. NTIA's SBOM initiative was incorporated into the Biden administration's May 12, 2021, Executive Order (EO) 14028, Improving the Nation's Cybersecurity [21]. This EO was in part a response to the 2020 SolarWinds cyberattack, which was reported to have compromised many high-level U.S. Federal Government agencies for extended periods of time. The EO directed NTIA to "publish minimum elements for an SBOM" within 60 days (July 11, 2021) of the EO's release.

The minimum elements of the SBOM are the essential pieces that support basic SBOM functionality and will serve as the foundation for an evolving approach to software transparency. These minimum elements comprise three broad, interrelated areas:

- **Data Fields:** Documenting baseline information about each component that should be tracked
- **Automation Support:** Allowing for scaling across the software ecosystem through automatic generation and machine-readability
- **Practices and Processes:** Defining the operations of SBOM requests, generation, and use

Open RAN subsystems distributed with SBOMs allow operators to better protect their network ecosystems and hold third-party suppliers accountable for the quality and security of their products. Specifically, the SBOM focuses on identifying vulnerabilities and dependencies; understanding integration and integrity; verifying sourcing and authenticity; and managing risk through a more targeted security analysis [22].

3.2 Why We Chose SBOM as the Security Component of the 5G Challenge Preliminary Event

SBOMs level the playing field between attackers and defenders. The intended audience are people who can use the data constructively—particularly customers who operate the software. SBOMs are not necessarily made public, though [23] notes that attackers do not need SBOMs due to their asymmetrical advantages (e.g., mass indiscriminate attacks and tools to identify software components). SBOMs empower software operators to identify potentially vulnerable components, plan for end-of-life components, comply with license obligations, evaluate whether they will be affected by new attacks, and avoid blacklisted components [22]. Without the SBOM, operators must consult and rely on the supplier for these tasks. SBOMs are well established in banking and are gaining traction in health care [23], defense, and other industries that depend on critical infrastructure.

The SBOM was chosen as the security component of the *5G Challenge Preliminary Event* because it is a natural fit with the President's cybersecurity goals outlined in EO 14028 [21] and the Secure 5G and Beyond Act of 2020 [25]. At the highest levels, the U.S. Government has issued policy directives providing frameworks to intelligently advance policy objectives in the technological sphere. In this case, providing incentives for 5G Challenge competitors to submit an SBOM fosters the development of industry knowledge and expertise. It's a small step towards growing the SBOM ecosystem with the goal of helping industry reach a critical mass, in which SBOMs become a routine component of every software project.

3.2.1 Vulnerability Exploitability eXchange

An SBOM must be used in conjunction with other tools or resources. Knowing what components and versions of those components are used in a software program does not independently provide any insight into the security of that program. Those components must be checked against current vulnerability databases. A mature security ecosystem will have programs that interface with SBOMs to validate that no critical security vulnerabilities are present. Several submissions recognized the weakness of merely having access to SBOMs without any supplementary documentation. Although it was not explicitly required, they included vulnerability assessment reports for all their components.

The Vulnerability Exploitability eXchange (VEX) [26],[27] provides vulnerability information for SBOMs. VEXs are not limited to use with SBOMs or even always a necessary component of SBOM projects.

Large software projects may have hundreds or thousands of SBOM-documented components, dozens of which may be affected by different vulnerabilities. Often these vulnerabilities are low, or zero-risk and the software developer is aware of them and has implemented mitigations. In this case, the developer can notify the user by issuing a VEX, which is an assertion about specific components. The four VEX status categories are: [27]

- **Not affected**: No remediation is required regarding this vulnerability
- **Affected:** Actions are recommended to remediate or address this vulnerability
- **Fixed:** Represents that these product versions contain a fix for the vulnerability
- **Under Investigation:** It is not yet known whether these product versions are affected by the vulnerability. An update will be provided in a later release

Including a VEX along with the SBOM is a useful addition to understanding the security posture of software projects. Requiring SBOMs in this stage of the challenge helped support various high-level policy objectives. Adding VEX is a natural next stop for supporting those efforts and providing useful data to evaluate the submissions and for our test lab, so it has information about vulnerabilities being introduced to its test environment.

3.2.2 Observations and Lessons Learned

For every project, additional requirements create increased costs, friction, time to produce, and perhaps even a decision not to complete the project. Following the completion of the *5G Challenge Preliminary Event*, we assessed whether including the SBOM requirement was a worthwhile additional requirement. Ultimately, we decided that it was. There was some minor resistance, but no indication that anyone chose not to participate because of the requirement.

4. EMULATED TESTING

The goal of Stage Two Emulated Testing was to (1) determine participant RAN subsystem (i.e., O-CU, O-DU and O-RU) compliance with O-RAN ALLIANCE specifications and 3GPP standards and (2) evaluate its integration and performance capability as a standalone unit.

ITS selected CableLabs as the host lab to operate the 5G test bed, design and manage 5G Challenge events, provide technical oversight, conduct contestant testing, analyze test data, and deliver final event reports. The host lab provided 5G RAN emulators into which competing contestants integrated their RAN subsystems. For emulated testing, the 5G test bed supported 5G SA Core and 5G RAN system specifications, as defined by 3GPP Release 15. The 5G Challenge focused on testing only 5G SA configurations.

4.1 Lab Setup, Tests

During emulated testing, CableLabs evaluated each selected contestant's O-RAN subsystem using a wraparound RAN subsystem emulator. As shown in Figure 3, CableLabs used wraparound emulators (i.e., O-CU tester, O-DU tester, O-RU tester) to test the distinct interfaces of each RAN subsystem (i.e., N2, N3, F1 and Open Fronthaul). The contestants provided an appropriate level of technical expertise and resources to ensure interoperability with the RAN emulator.

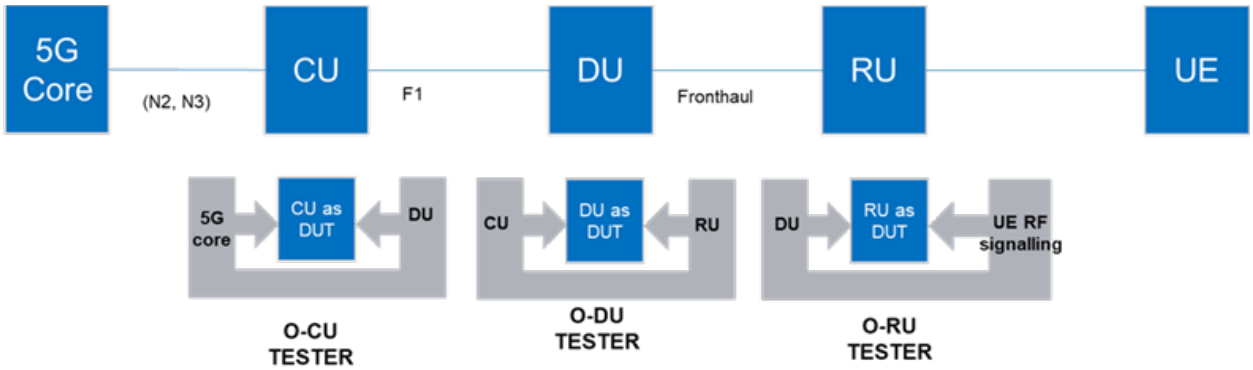

Figure 3. 5G Challenge test setup.

Test cases assessed contestant RAN subsystem capabilities at an increasing level of complexity using 3GPP and O-RAN ALLIANCE standards as a reference. RAN subsystems that complied with more complex test cases provided an indication of their state of development against the industry standards and their likelihood of a successful multi-vendor integration (in Stage Three of the competition).

Emulated test cases included four levels:

- **Level 0, Integration:** The objective was to demonstrate successful integration into the test environment

- **Level 1, Interface:** The objective was to demonstrate successful setup of its distinct interfaces with the wraparound test emulator (including basic message exchange)

- **Level 2, Functional:** The objective was to perform O-RAN conformance, limited interoperability test (IOT), and basic functionality tests

- **Level 3, Performance:** The objective was to demonstrate throughput and loading performance with the wraparound tester emulating E2E network traffic flow

4.2 Observations and Lessons Learned from Emulated Testing

Nine contestant RAN subsystems passed Stage One (the application process) and moved on to Stage Two (two RUs, three DUs, and four CUs). Of the initial nine contestants, only six were tested in the lab. Three did not pass due to insufficient contestant subsystem "readiness" in the allocated test time frame or contestant withdrawal from the test event. Our testing process allocated each contestant subsystem one week of preparation and two weeks of testing.

The overall results of Contestant Pass Rate by Test Level for the Stage Two event (of contestants presented for testing) show that all six contestants passed all Level 0 tests and half of the contestants (three) passed all Level 1 test cases. Additionally, one-third of the contestants (two) passed all Level 2 and Level 3 test cases. The 5G Challenge required each contestant to complete all test cases at each Level before moving to the next Level of test cases.

Because none of the contestant DUs had passed Level 1 after two weeks of testing, we offered extra lab time (on an equal basis) to all DUs that passed Level 0. Only one DU contestant accepted the extra time and subsequently passed Level 1. The above statistics reflect four weeks of testing for one DU and two weeks of testing for all other subsystems.

Highlights of additional results are summarized below:

- The remaining contestants that did not pass all Level 1 tests completed an average of 46% of the Level 1 tests

- The remaining contestants that did not pass all Level 2 tests completed an average of 17% of the Level 2 test

- Two contestants' RAN subsystems completed all four levels of test cases

Based on the test results, several observations are summarized below.

4.2.1 Test Level Completion Varied per Contestant O-RAN Subsystem

Contestant CUs reached the farthest level of integration and performance, including two contestant CUs successfully completing all four levels of test cases. Contestant RUs had a modest level of completion, while contestant DUs had the lowest rate of completion. The level of test completion may correlate to the complexity of RAN subsystem functionality and interface

requirements, with the CU the least complex and the DU the most complex. This was reflected in the time it took to integrate and establish connectivity with the RAN subsystem and the wraparound testers (i.e., CU being least complex, and DU being most complex).

Two weeks seemed to be sufficient time for wraparound emulation testing of a CU. However, due to the RU and DU integration complexity, allocating the RU four weeks of testing and the DU six would have improved the process.

4.2.2 Configuration Differences were a Common Problem

Contestants spent much of their test time resolving configuration issues between their subsystems and the wraparound tester/emulator. 3GPP standards and O-RAN ALLIANCE specifications offer hundreds of configuration parameters depending on unique operator needs. Competitors spent extensive time capturing and reviewing log files and configuration settings to ensure successful integration, messaging, and data session establishment met industry standards. Contestants with coupled solutions (i.e., CU+DU) used for commercial deployments had to take time to re-configure and separate their CU and DU subsystems to integrate with a wraparound tester to comply with O-RAN standards.

4.2.3 Compliance with 3GPP and O-RAN was a Common Problem

Contestants spent much of their test time resolving compliance mismatches of 3GPP standards and O-RAN ALLIANCE specifications, mostly centered around implementation of different release versions, inclusion of optional features or requirements, and differing interpretation of a specific requirement. For example, there were several instances where a contestant RAN subsystem implemented a different 3GPP standard release version than the wraparound tester (e.g., TS 38.413 v15.3 vs v15.6, and TS 38.473 v15.6 vs 15.9). Handling the implementation of requirements and features of varying 3GPP Release versions can yield different results that are functional in isolation, yet incompatible when combined. In some cases, this required either the contestant or the wraparound tester vendor to adjust their software. In some instances, hard-coded emulator/tester equipment parameters required contestants to change their software to properly integrate, causing additional time delays. Additionally, some contestants had baselined their O-RAN subsystem for specific commercial deployments and had to modify their O-RAN subsystem to integrate with a wraparound tester.

4.2.4 Messaging in the Control Plane was a Common Problem

In general, establishing E2E messaging in the control plane was a common challenge resulting from configuration and industry standard compliance misalignments or other challenges. For example, an optional Information Element (IE) parameter not expected or recognized (but sent by one subsystem) caused challenges, as did mismatching port configurations and F1 setup issues. Establishing downlink and uplink messaging was equally challenging.

5. NETWORK INTEGRATION

The goal of Stage Three network testing was to establish a data session across a multi-vendor RAN with an emulated UE and a commercial 5G SA core and then to characterize the performance of the fully integrated E2E network under non-stressed and stressed conditions.

5.1 Lab Setup and Tests

From the pool of contestants who passed the Level 1 test cases in Stage Two Emulated Testing, three contestants were selected for Stage Three. Stage Three established a complete RAN subsystem consisting of CU, DU, and RU subsystems from different contestants. During Stage Three integration, each contestant provided one O-RAN subsystem (RU, CU, or DU) and the host lab provided the remainder of the 5G system (i.e., UE emulator and 5G SA core), as shown in Figure 4. The contestants provided the appropriate level of technical expertise and resources to ensure interoperability with the UE emulator and 5G SA core. Actual UEs were occasionally used for debugging, in addition to the UE emulator.

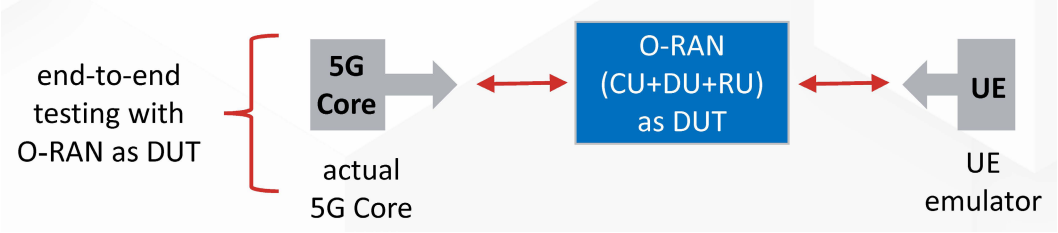

Figure 4. Stage Three test setup.

The 5G Challenge Rules allowed for an alternate configuration, where up to six contestants could have participated in Stage Three. In this configuration, two contestants would have provided O-RAN subsystems and the host lab would have provided the third O-RAN subsystem (e.g., contestant CU, host lab DU, and contestant RU). This would have allowed for three E2E integration tasks to operate in parallel, with different sets of contestants.

Several problems prevented this option from being implemented. First, only one DU passed Stage Two testing, creating a DU bottleneck. Second, one contestant submitted a frequency division duplex (FDD) RU, but the other contestant and host lab O-RAN subsystems were time division duplex (TDD). This FDD RU could not be evaluated in Stage Three, which created an RU bottleneck. Third, some E2E paths were eliminated due to fairness or compliance problems (e.g., the same vendor's equipment appeared as both a contestant subsystem and a host lab component). Therefore, Stage Three consisted of a single E2E configuration.

Stage Three contestants had five weeks to establish E2E network integration. Stage Three test cases were similar to those in Stage Two. The goal was to assess RAN subsystem capability in increasing levels of complexity using 3GPP standards and O-RAN ALLIANCE specifications and test cases as a reference. The four levels of test cases included integration, functional, performance, and stress as described below.

- **Level 0, Integration:** Objective was, via test cases, to validate the ability of the contestants' RAN subsystems to successfully integrate with the E2E setup that consisted of a UE emulator, non-emulated 5G SA core, and other contestants' subsystems (i.e., CU, DU, and RU)

- **Level 1, Functional:** Objective was to verify the contestant subsystem's compliance with protocol conformance and baseline functionality of O-RAN ALLIANCE and 3GPP specifications to establish a successful E2E data transmission across a 5G network

- **Level 2, Performance:** Objective was to verify the contestant subsystem's performance across different KPIs, including throughput, latency, and jitter, for optimal RF conditions for a single UE

- **Level 3, Stress:** Objective was to verify the contestant subsystem's performance across different KPIs, including throughput, latency, and jitter, for cell edge and loading conditions with multiple UEs

5.2 Lab Testing Results

Three contestant RAN subsystems participated in Stage Three (one CU, one DU and one RU). Results show that, collectively, all contestants passed all Level 0, Level 1, and Level 2 tests. The grouped contestants did not test Level 3 test cases, due to time limitations.

Stage Three network test cases demonstrated successful E2E bi-directional data sessions with multiple protocols (μTP, TCP, RTP, FTP and ICMP) across a multi-vendor RAN (with limited prior integration experience) with a commercial 5G core and UE emulator.

The 5G Challenge demonstrated a multi-vendor RAN that both complied with O-RAN standards and achieved interoperability with a commercial 5G SA core and a UE emulator within five weeks. This fast-paced integration had not previously been accomplished.

5.3 Observations and Lessons Learned from Integrated Testing

Highlights of key qualities that enabled the success of Stage Three:

- Close collaboration and openness to revise software between contestant O-RAN subsystem, test vendor, commercial 5G core vendor, and host lab

- Contestant RAN subsystem developer expertise

- Test vendor developer expertise

- Commercial core vendor expertise

- Host lab system integration expertise

Of these lessons learned, we would like to stress the importance of collaboration among diverse vendors. The 5G Challenge design was informed in part by [28], which identifies potential obstacles to 5G open architecture deployment. Collaborative efforts between contestant vendors, host lab, and test equipment vendor resolved three of six potential obstacles: (1) complexity of integration and deployment; (2) complicated maintenance, including fault finding and remediation, during operation; and (3) lack of end-to-end coordination for optimization and upgrades. The other potential obstacles reflect uncertainties associated with this relative newness of 5G open architectures: (4) piecemeal growth; (5) potential for slower development; and (6) latency and scalability.

The 5G Challenge confirmed the importance of easily accessible 5G testbeds. Our analysis of 51 responses to a public Notice of Inquiry (NOI) [28] indicated that new market participants need to test interoperability without waiting for a plugfest or partnering with a large company. This need is specifically for 5G testbeds that enable hands-on engineering research (i.e., connecting actual devices to explore the impact of both physics and mechanics). University testbeds focus on science research, which does not fill this industry need. The 5G Challenge contestants valued and requested more time "in the lab" at CableLabs, which serves this niche as a not-for-profit company and the only Open Test and Integration Center (OTIC lab) in North America. To advance the industry, we need more open, transparent labs that are recognized as unbiased, trusted agents in which to conduct 5G multi-vendor interoperability research.

The test software played a critical role in the success of the 5G Challenge. The NOI analysis [28] expressed support for an open-source test suite, but later investigations indicated an insufficient level of community support. The test suite used by the 5G Challenge was intended to support development, not compliance testing. This design goal mismatch was exacerbated by our aggressive schedule. Certain elements of the O-RAN ALLIANCE specifications were newly released, being revised, or under development when the 5G Challenge launched in April 2022. In addition to the test suite identifying problems with contestant subsystems, the wraparound emulation and interoperability testing encountered typical growing pains with the test suite. Such issues inevitably arise when conducting engineering research that pushes the envelope.

6. CONCLUSIONS

The mobile industry is undergoing a transition from a closed, proprietary RAN architecture to an open, disaggregated RAN architecture. A blueprint of this open RAN architecture is defined in 3GPP standards and O-RAN ALLIANCE specifications, which allows for greater flexibility in design and network deployment. This presents many advantages to mobile operators by improving deployment flexibility, network performance, cost reduction, and the ability to customize service delivery. This also introduces advantages to the overall mobile network ecosystem by increasing competition, promoting innovation, and driving multi-vendor plug-and-play capability.

The NTIA/ITS introduced a 5G Challenge event to characterize the state of the open RAN ecosystem and to drive multi-vendor interoperability. The 5G Challenge was designed to (1) demonstrate the level of RAN subsystem compliance with industry specifications and (2) establish E2E bi-directional data sessions with multiple protocols (μTP, TCP, RTP, FTP and ICMP) across a multi-vendor RAN (with limited prior integration experience of contestants) with a commercial 5G core and UE emulator in the allocated five-week time frame.

Results of the test event showed that standalone CUs reached the farthest level of integration and performance, demonstrating the most compliance with industry specifications. Contestant RUs attained a modest level of completion, while contestant DUs attained only the lowest level of completion. In addition to design maturity, it was observed that the level of test completion may correlate to the complexity of RAN subsystem functionality and interface requirements, with the CU the least complex and the DU the most complex. This suggests that standalone RAN subsystems are still working towards industry standard compliance.

Results of the test events also demonstrated successful interoperability across a multi-vendor O-RAN using E2E bi-directional data sessions with multiple protocols with a commercial 5G core and UE emulator in the allocated five-week time frame. This suggests that the industry ecosystem is capable of true multi-vendor interoperability with open RAN.

To help drive the industry towards open RAN, key findings for success include: (1) a well-established baseline set of E2E industry requirements and O-RAN subsystem configurations in advance of test event; (2) advanced planning for the testing of different spectrum usage techniques; (3) specialized expert O-RAN developers available during the test event to support troubleshooting efforts; (4) unbiased host lab with expertise in system integration and advanced test equipment; (5) sufficient test time for preparation and integration activities; and (6) commitment to multi-vendor collaboration during troubleshooting and fault remediation.

7. REFERENCES

[1] "NG-RAN; Architecture Description," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.401, May 2019, version 15.5.0. https://www.3gpp.org/ftp//Specs/archive/38_series/38.401/38401-f50.zip.

[2] Frank H. Sanders; Kenneth R. Calahan; Geoffrey A. Sanders; Savio Tran, *Measurements of 5G New Radio Spectral and Spatial Power Emissions for Radar Altimeter Interference Analysis*, U.S. Department of Commerce, National Telecommunications and Information Administration, NTIA Technical Report TR-22-562, Oct. 2022. https://its.ntia.gov/publications/3289.aspx

[3] "5G functional splits," White Paper, parallelwireless.com: Parallel Wireless. https://www.parallelwireless.com/wp-content/uploads/5G-Functional-Splits_092721.pdf.

[4] "Split option 7.2x," *Dell Technologies, VMware, and Mavenir 5G O-RAN Reference Architecture Guide*. https://infohub.delltechnologies.com/l/dell-technologies-vmware-and-mavenir-5g-o-ran-reference-architecture-guide/split-option-7-2x-5 .

[5] 3rd Generation Partnership Project (3GPP), *Specifications & Technologies / Releases*. https://www.3gpp.org/specifications-technologies/releases.

[6] "NG-RAN; Architecture Description," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 38.401, Apr. 2022, version 17.0.0. https://www.3gpp.org/ftp/Specs/archive/38_series/38.401/38401-h00.zip

[7] O-RAN ALLIANCE, "About O-RAN Alliance." https://www.o-ran.org/about.

[8] Michele Polese, Leonardo Bonati, Salvatore D'Oro, Stefano Basagni, and Tommaso Melodia, "Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges," submitted to IEEE, version 2 from Sep. 1, 2022. https://arxiv.org/abs/2202.01032

[9] O-RAN ALLIANCE, "ORAN. WG1.O-RAN-Architecture-Description-v05.00," Technical Specification, Jul. 2021. https://orandownloadsweb.azurewebsites.net/specifications

[10] O-RAN ALLIANCE, "Who we are." https://www.o-ran.org/who-we-are.

[11] Leonardo Bonati, Salvatore D'Oro, Michele Polese, Stefan Basagni, and Tommaso Melodia, "Intelligence and Learning in O-RAN for Data-driven NextG Cellular Networks," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 21–27, Oct. 2021, doi: 10.1109/MCOM.101.2001120.

[12] Raj Jain and Subharthi Paul, "Network virtualization and software defined networking for cloud computing: a survey," *IEEE Communications Magazine*, vol. 51, no. 11, pp. 24–31, Nov. 2013, doi: 10.1109/MCOM.2013.6658648.

[13] O-RAN ALLIANCE, "O-RAN.WG1.O-RAN-Architecture-Description-v07.00," Technical Specification, Oct. 2022. https://orandownloadsweb.azurewebsites.net/specifications

[14] O-RAN ALLIANCE, "O-RAN Global Plugfest 2022." https://plugfestvirtualshowcase.o-ran.org/

[15] Ashutosh Dutta and Eman Hammad, "5G security challenges and opportunities: a system approach," *2020 IEEE 3rd 5G World Forum (5GWF)*, 2020, pp. 109–114, doi:10.1109/5GWF49715.2020.9221122.

[16] Chih-Ting Shen *et al*., "Security Threat Analysis and Treatment Strategy for ORAN," *2022 24th International Conference on Advanced Communication Technology (ICACT)*, 2022, pp. 417–422, doi: 10.23919/ICACT53585.2022.9728862.

[17] Open RAN Policy Coalition, "Open RAN Security in 5G," Apr. 2021. https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf

[18] Federal Communications Commission, Public Safety and Homeland Security Bureau, "List of Equipment and Services Covered by Section 2 of the Secure Networks Act," updated Sept. 20, 2022. https://www.fcc.gov/supplychain/coveredlist.

[19] Xinxing Ding, Feng Zhao, Lijuan Yan and Xiaodong Shao, "The Method of Building SBOM Based on Enterprise Big Data," *2019 3rd International Conference on Electronic Information Technology and Computer Engineering (EITCE)*, 2019, pp. 1224–1228, doi: 10.1109/EITCE47263.2019.9094817.

[20] U.S. Department of Commerce, National Telecommunications and Information Administration, NTIA Multistakeholder Process on Software Component Transparency, Framing Working Group, *Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)*, Second Edition, Oct. 21, 2021. https://www.ntia.gov/sites/default/files/publications/ntia_sbom_framing_2nd_edition_20211021_0.pdf.

[21] Executive Office of the President, Executive Order 14028: Improving the Nation's Cybersecurity, May 12, 2021, *Code of Federal Regulation,* 86 FR 26633. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[22] U.S. Department of Commerce, National Telecommunications and Information Administration, NTIA Multistakeholder Process on Software Component Transparency, Use Cases and State of Practice Working Group, *Roles and Benefits for SBOM Across the Supply Chain*. https://www.ntia.gov/sites/default/files/publications/ntia_sbom_use_cases_roles_benefits-nov2019_0.pdf.

[23] U.S. Department of Commerce, National Telecommunications and Information Administration, NTIA Multistakeholder Process on Software Component Transparency,

SBOM Myths vs. Facts, Nov. 2021. https://www.ntia.gov/sites/default/files/publications/sbom_myths_vs_facts_nov2021_0.pdf

[24] Seth Carmody et al., "Building resilient medical technology supply chains with a software bill of materials," Nature Partner Journal (*npj) Digit. Med.,* vol. 4, no. 34, 2021. doi: 10.1038/s41746-021-00403-w.

[25] Secure 5G and Beyond Act of 2020, Public Law 116-129, 116th Cong. (Mar. 23, 2020), 134. https://www.govinfo.gov/app/details/PLAW-116publ129.

[26] L. Jean Camp and Vafa Andalibi, "SBoM Vulnerability Assessment & Corresponding Requirements," *Comments on Software Bill of Materials Elements and Considerations*, Bloomington, IN: Luddy School of Informatics, Computing, & Engineering. https://www.ntia.doc.gov/files/ntia/publications/camp_andalibi_-_2021.06.16.pdf

[27] U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, *Vulnerability Exploitability eXchange (VEX) — Use Cases*, Apr. 2022. https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf

[28] U.S. Department of Commerce, National Telecommunications and Information Administration, Institute for Telecommunication Sciences, "*5G Prize Challenge Notice of Inquiry Analysis*," NTIA Special Publication SP-21-554, Sept. 2021https://its.ntia.gov/publications/3274.aspx.

ACKNOWLEDGMENTS

The authors would like to thank the Department of Defense representatives Dolores Shaffer and T. K. Woodward for their technical contributions. The authors would also like to thank the many 5G experts from industry, academia, government, and standards-developing organizations who took the time talk with us about 5G technology.

NTIA FORM 29
(4-80)

U.S. DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION NO.	2. Government Accession No.	3. Recipient's Accession No.
TM-23-568		

4. TITLE AND SUBTITLE	5. Publication Date
5G Challenge Preliminary Event: Evaluating Modular, Interoperable, Multi-Vendor, Open RAN Solutions	May 27, 2023
	6. Performing Organization Code

7. AUTHOR(S)	9. Project/Task/Work Unit No.
Margaret H. Pinson, Mark Poletti, Julie Kub, Jeremy Glenn, Tim Thompson, Robert Kupsh, Naser Areqat, Okmar Dharmadhikari, Annie George, T. Lauriston Hardin, P.E., Cory Johnson, Spiros Kapoulas, Sundar Sriram	08 6925 000 300
8. PERFORMING ORGANIZATION NAME AND ADDRESS Institute for Telecommunication Sciences National Telecommunications & Information Administration U.S. Department of Commerce 325 Broadway Boulder, CO 80305	10. Contract/Grant Number.

11. Sponsoring Organization Name and Address	12. Type of Report and Period Covered
Office of the Secretary of Defense for Research and Engineering The Pentagon Washington, DC 20301	

14. SUPPLEMENTARY NOTES

15. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)

Today's mobile wireless networks comprise many proprietary solutions with custom, closed-source software and hardware. Changes to these proprietary elements require complex and meticulous verification of the entire network. This dynamic increases costs, slows innovation, reduces competition, and makes security issues difficult to detect and fix. Our vision is to accelerate adoption of 5G open interfaces, interoperable components, and multi-vendor solutions by fostering a large, vibrant, and growing vendor community dedicated to advancing 5G interoperability towards true plug-and-play operation. This memo describes the "5G Challenge Preliminary Event: RAN Subsystem Interoperability" conducted by the U.S. in 2022. Contestants submitted Open RAN radio units (O-RU), distributed units (O-DU), and central units (O-CU). We evaluated each subsystem individually in an emulated environment. Our tight testing timeline consisted of one week of preparation and two weeks of emulated wraparound testing. We then integrated subsystems from multiple vendors to create an end-to-end network. In true plug-and-play fashion, contestants approached network integration with no prior experience interoperating with their fellow contestants' subsystems. The 5G Challenge provided a rigorous five-week schedule for end-to-end integration and testing. Contestants worked through diverse issues, from software options to discrepant hardware. This successful event demonstrated end-to-end data communication sessions using multiple protocols across a multi-vendor, interoperable, Open RAN architecture.

16. Key Words (Alphabetical order, separated by semicolons)

5G; interoperability; network testing; SBOM; open interfaces; Open RAN

17. AVAILABILITY STATEMENT	18. Security Class. (This report)	20. Number of pages
☒ UNLIMITED.	Unclassified	34
☐ FOR OFFICIAL DISTRIBUTION.	19. Security Class. (This page)	21. Price:
	Unclassified	N/A

NTIA FORMAL PUBLICATION SERIES

NTIA MONOGRAPH (MG)

A scholarly, professionally oriented publication dealing with state-of-the-art research or an authoritative treatment of a broad area. Expected to have long-lasting value.

NTIA SPECIAL PUBLICATION (SP)

Conference proceedings, bibliographies, selected speeches, course and instructional materials, directories, and major studies mandated by Congress.

NTIA REPORT (TR)

Important contributions to existing knowledge of less breadth than a monograph, such as results of completed projects and major activities.

JOINT NTIA/OTHER-AGENCY REPORT (JR)

This report receives both local NTIA and other agency review. Both agencies' logos and report series numbering appear on the cover.

NTIA SOFTWARE & DATA PRODUCTS (SD)

Software such as programs, test data, and sound/video files. This series can be used to transfer technology to U.S. industry.

NTIA HANDBOOK (HB)

Information pertaining to technical procedures, reference and data guides, and formal user's manuals that are expected to be pertinent for a long time.

NTIA TECHNICAL MEMORANDUM (TM)

Technical information typically of less breadth than an NTIA Report. The series includes data, preliminary project results, and information for a specific, limited audience.

For information about NTIA publications, contact the NTIA/ITS Technical Publications Office at 325 Broadway, Boulder, CO, 80305 Tel. (303) 497-3572 or e-mail ITSinfo@ntia.gov.