IORS 2024: Notes from Interactive Workshop Sessions

For action items, main discussion points, and points of agreement

Interactive Workshop—Topics for Test Collaboration

Discussions led by Discussion led by Paul Sludden (Digital Catapult/SONIC Labs UK), assisted by Maggie Chao (ITRI)

Breakout Session #1—What labs are already collaborating? What are their collaboration goals?

Led by Maggie Chao (ITRI)

1. The collaboration in labs should help the document/define test procedure to reduce variability of results
    a. Still need to have the calibration, the baseline, etc…
2. Identify strong points of each lab
    a. What are the topics the labs would want to collaborate with
3. Base on the collaboration within ITRI, SONIC Labs and i14y Lab, would like to extend this collaboration with new labs from different regions such as Latin America

Breakout Session #2—What types of tests should we conduct in multiple labs worldwide, to evaluate consistency and repeatability?

Led by Vijay K. Shah (North Carolina State University)

[Insert notes here]

4. **Whether we want two types of test specifications?**
    a. Shareable across the world - O-RAN compliant
    b. Operator-additional requirements - Operator-compliant

5. Protocol compliance, interface compliance, conformance -
6. **Minimum viable test profile**
    a. Interoperability/Conformance
    b. Functionality
    c. Security
7. **Common test suite for MVP profile**
8. Best practises/
9. **Collaboration between different test vendors**
    a. Same test scripts - significant overhead
10. Common test passing/failing criteria across labs
11. **Automated testing framework** - automated execution of common test suites across various labs worldwide.
12. Follow 3GPP and other standard parameters for OTIC badging
13. **Identical testbed configurations/Network emulation** - Except DUT, keep rest of the testbed, network emulation, environment, load, UE behavior similar across different labs (with certain customization for specific countries)
14. **OTIC can serve as system integrator (as an independent entity) for specific operator and vendors**
15. Share test cases, setup, logs, which labs, data format, on a central repository
16. Standardize FCAPS, automation, orchestration, O&M test cases
    a. O&M best practises
17. Establish a baseline performance metric from one lab and use it as a reference for all other labs
18. **Review meetings across OTIC labs**, and who leads, manages and funds it?

Breakout Session #3—How can we progress consistent and repeatable testing by dividing the effort among multiple labs?

Led by N. K. Shankaranarayanan (Rutgers University)

We had a small group which led to a great discussion. Good representation from industry, industry labs and forums, academia, government

1. Dividing the effort: What does it mean?

- Implies some common set of tasks which can be divided. There are different types of labs: OTIC labs, TIP Labs, NTIA T&E Labs, university labs.
- Assumption for Repeatable and Consistent:
    - Test plans and specs needs to be explicit. Cannot have a wide area of interpretation

    - Validating capability of test equipment is important.
- Comment: Establish consistent and repeatable so that you do not have to repeat, and can then focus on dividing tasks in test
- Repeatable v complementary
    - Repeatable: Lab 1 runs same test in same condition as Lab 1 and gets same result
    - Complementary: Lab 1 run different set of tasks or scenarios as Lab 2 to achieve complementary objective
- "Divide the effort" interpretation
    - First achieve repeatability and then divide by sharing tasks in the test plan. Goal is "not to have to repeat"
    - Split set of tasks in test plan to share the burden
    - Co-operation between labs: eg RIC/SMO in one lab and RU in another lab
    - Testing of apps needs reliable, usable RAN, Digital Twin etc. - another way of dividing the effort

Action: Need to get Test Specs and Plans to be mature enough to achieve consistent and repeatable.

2. Leveraging capabilities of test labs

Test Labs will have common and differentiating capabilities

- Geography - access to location for different stakeholders
- Set of equipment available (component, test equip, emulators)
- Test scenarios (indoor/outdoor, people
- Synergy with other projects
- Matrix of test areas: badging, performance, commercialization, innovation areas (OTIC capabilities from TIFG)

Repeatable => Suppress differences to have common, equivalent setup
Complementary => Leveraging differentiating capabilities

Consensus: There will always be differences. It is worthwhile trying to find a way to leverage the differentiating advantages. This will follow the commercial model/needs to do so.

- Different RAN scenarios: indoor/outdoor/urban/OTA frequencies
- UE Emulator capabilities
- Availability of advanced RU
- Availability of software capabilities - RIC, apps platforms
- Test cases involving use of more than one lab at the same time

Action: Need a forum and discussion to establish consensus that it is worthwhile to leverage different advantages of labs. Then we map different test areas and have a process for labs to find suitable roles and participate in complementary tests.

3. Collaboration Dynamics

- Do we need a forum for labs to collaborate? What is the driver to invest time/energy?

Comments:
OTICs have been set up as independent. Not enough validation of the OTICs.
TIP has set up CL under a central authority.
Sharing information can be a constraint.

Breakout Session #4—How can existing labs provide training and workforce development to new labs?

Led by Michele Polese (Northeastern University)

- It is impractical for existing labs to train new labs, for business/competitiveness reasons
    - Test vendors provide training for their equipment for lab bring-up
- Workforce development is practical, in multiple steps/stages
    - Academic programs (masters)
        - Need to align curricula to new developments offering a combination of
            - Wireless/RF/hardware/embedded engineering
            - System engineering
            - Cybersecurity/IT/operations/networking
            - AI/ML
            - Software engineering
            - QA
        - *And* provide cross-functional training on the specific applied science domain (Open RAN/Open RAN testing)
    - Industry certification (or re-certification)
    - Hands-on training
- More details: https://photos.app.goo.gl/xd4Y7GBgpa8vmJgMA

Breakout Session #5—What are labs willing to share (e.g., open source code and data)?

Led by Tracy Van Brakle (AT&T)

1. Cloudified federated testbeds to serve as open 5G/NextG lab (both US-based and Global)

    a. Build upon O-RAN OTIC concept as foundational but not sufficient as-is to meet the needs of MNOs
    b. Build upon NSF PAWR initiative (especially wrt outdoor testbeds)
    c. Build upon FCC Innovation Zone
2. Open source / open industry standards
    a. To develop IM/DM common core (80%) that supports proprietary extensions (20%)
    b. Protocol
    c. Code
    d. Reference designs
3. Network data
4. Proprietary data
    a. FM/PM (KPIs) to train models & etc.
    b. Test results (anonymized? aggregated?)
5. Expertise
6. Reservation system for costly lab resources and/or access to complex indoor/outdoor testbeds with specialized UEs

Breakout Session #6—Security collaboration: current progress and next steps

Led by Syed Hussain (Pennsylvania State University) and Arup Bhuyan (INL)

Notes:

1. For what components of O-RAN do we need to perform security testing? E.g., RIC, NR-RIC, xAPPs, rApps, protocols, standard and non-standard interfaces, crypto testing
    a. Component level testing
    b. Compositional testing
    c. Lab scale testing
    d. Deployment setting testing, e.g., testing in cloud settings
2. How to obtain software quality/security assurance to get a minimum viable security profile?
3. What are the security benchmarks and safe programming principles for O-RAN?
4. What are the ways to run software security testing for RU, DU, CU, RIC, and NR-RIC?
5. How to address vendor diversity in security testing?
6. What are the ways to ensure secure spectrum sharing?
7. What are the ways to perform physical layer security testing?
8. How do we ensure zero-trust in security testing?

9. What are the certification processes?
    a. Need different certification for different use cases, e.g., regular traffic vs. security sensitive traffic, normal operations vs. DoD operations
10. What will happen if the vendor doesn't support security features?
11. How can we perform supply chain security testing?
12. Is the conformance test provided by Open RAN and 3GPP enough? Standard only provides positive testing, but for security, we need more negative testing and red teaming efforts.
13.

Interactive Workshop—Consistent, Repeatable, International Testing

Discussions led by Discussion led by Julie Kub (NTIA/ITS), assisted by Aloizio Da Silva (Commonwealth Cyber Initiative Virginia Tech)

Beginning of session:
[Insert overall themes here]

- Breakout Accuracy:
- Transparency of the configuration, create more concrete standards, disclosure of data testing, report is not standardized
- Consistency test: the same interface, same test case, selection of test cases
- What is the cost of transparency?
- Different types of data, how to classify different types of data?
- Test case data and test system data
- OTIC Internal exercise: Quality control, lab comparison, calibration,
- SONIC Lab: RIC application requires a lot of data to execute specific tasks, emulated data and real data to feed the Apps. The Plugfest is a good mechanism to get the labs to collaborate.
- Test control measurement
- TIP: test case should be attached to a blueprint and should be connected to a solution.
- How to define the use cases requirements?
- Accreditation cost? OTIC Quality assurance

- Knowledge database
- How to run the test cases?
- Adding test control also increases the cost.
- Cost should not be discussed in an open forum.
- Each test vendor should implement the same test case.
- Open-source test method validation

Conclusion of session:
[Insert overall themes here]

- Breakout section #2
    - 2 MNOs from ACCoRD Project #2
    - How to MNO define performance metrics: Parity with RAN, throughput Dl, UL
    - What testing is more important MNO: Iterops M-Plane, Security,
    - What are the use case: NTN, NSA, DSS, Slicing, MTC, TCO (Total Cost of Ownership), RAN Sharing,
    - What testing MNO will do in their own lab: SW roll out and upgrade; IOT with core; loading testing; feature testing; conflict avoidance testing in cluster of multiple apps; KPI, performance field testing;
    - Actions: Augment test plan; define stability testing; define channel model that reflect field environment.

- Breakout section #3
    - Consistency across different location
    - Missing well-defined testing environment
    - Explanability of test case
    - Peer-review across the labs
    - The lowerbound and upperbound is associated with use cases per si.
- Breakout section #4
    - Accuracy on the testing input configuration; testing result accuracy; accuracy is different from different use cases;
    - Declaration of conformance or not, it is related to the use case
    - A testing program (innovation testing and innovation lab)
    - Develop a quality control program for certification, SDO can play a role on set the stage for the program; specify the delta.
- Breakout section #5
    - High quality test cases are needed;
    - Where to automate?, specific test cases are not automated
    - Usage of AI/ML for testing automation
    - Flexibility is needed for the test framework
    - How to bring field conditions to the lab?
    - Produce evidence as part of the testing execution and results
    - Automated cause analysis is important for the testing automation.
- Breakout section #6

- IP license consensus
- What kind of data and format is needed for different use case
- Public repository for data sharing
-

Breakout Session #1—How do we do resilience testing?

Led by Joe Constantine (Ericsson)

Possible questions:

- How does the network respond when things go bad?
- How do we model the network problems?
- How do we test the network's resilience to these problems?
- How does this testing become standardized?

Additional items added by Joe:

- Testing "interoperability" of an open interface.
- Over an agreed upon IOT (Interoperability Testing) profile.
- Consideration for complexity and cost.
    - Merely adhering to an IOT profile doesn't guarantee interoperability.
    - Agreement on YANG modules, NETCONF capabilities, and other aspects of systemization needed before a first successful call, even under ideal conditions.
- Robust specification of IOT profiles is key to consistent and repeatable testing.
- Limit the number of IOT profiles per open interface (e.g., <= 4 for open fronthaul).
- Is resilience testing in the lab environment required for testing an open interface?
    - Operators typically will do field test (FOA) anyway.
    - Is resiliency really required for the IOT of an interface?

[Insert overall decisions here]

Breakout Session #2—What testing do MNOs want (e.g., performance parity, use cases)?

Led by Farook Hussan (Verizon)

To	antoine.a.soyoh.ctr@mail.milPerson Person Person
Cc	Person

Bcc	Person
Subject	IORS

Possible Questions:
- How do MNOs define performance parity?
- Which use cases and at what point in time?
- What types of testing are most important right now (e.g., functional testing, performance testing, stability testing, resilience testing)?
- What is the scope of testing: network functions, E2E, interfaces, security, architectural components, etc.?
- What parts of testing will MNOs do in their own lab and what can be done in a test lab? What parts of testing will be common vs different worldwide?

[Insert overall decisions here]

Breakout Session #3—How can we achieve and demonstrate consistent, repeatable testing?

Led by Andreas Gladisch (DT/i14y Lab) - supported by Monika & Carsten

Part 1: Consistent, repeatable testing: Observation of status - 20 Min
- What is your understanding of consistent, repeatable testing
- Where do we stand regarding consistent, repeatable testing (on a scale 1 - 10)
- What have you seen in the past concerning repeatable testing (in a lab, between labs)

Part 2: Areas of improvement - 30 Min
- What does the industry need to get consistent, repeatable testing
- How can we achieve consistent, repeatable testing | how and where to improve
- Key challenges - activities - collect answers

Part 3: Demonstrate repeatable testing in the next quarters - 25 Min

- How can we demonstrate consistent testing?
- Who is volunteering to work on this
- Wrap up of the key aspects | learnings of the session

Definition of "consistent, repeatable testing"

- Ability to gain identical results from running the same test cases with the same system under test (SUT)
- Consistency across location (different labs), time (different runs), and test beds (different test equipment) as long as test spec and SUT configuration are identical
- Consistency and repeatability are closely related terms and can probably be interchanged.

Observations - state of the ecosystem

- Attendees reviewing the repeatability of testing today (on a scale from 1=none to 10=perfect):
  Unit Conformance around 2-4, end-to-end and RIC testing not repeatable yet
- Environment definitions, calibration rules, and test specs are not yet well enough specified, so labs have a hard time
- Operator use case requirements are not ubiquitously agreed (ATIS talk: Minimum viable profile defined for some use cases in North America?)
- There is a limit to repeatability:
    - Error margins for performance tests
    - Low-level test case definitions (cable lengths etc.) which are extremely detailed, and are part of the basic skill set of the lab to compensate for
- Why is repeatability important?
    - Avoid false positives
    - Create dependable results that can be consumed with trust

Potential areas of improvement

- **Try out peer review** to validate where we are in this industry with regard to the reproducibility of results. Or are the detailed test specs enough?
    - What happens as a next steps if labs have different results? Would there be consequences, or would labs "agree to disagree"? Lab rating system by a "neutral" instance?
    - Sources of non-repeatability across lab execution:
        - Imprecise test spec: Must be resolved by SDOs
        - Different test bed configuration by misunderstanding or lack of experience: can be resolved by peer review
        - Negligence: Can be resolved by spotchecks (happens only from time to time)
        - Gross negligence: Must be avoided by accreditation
        - Intentional gaming: Must be protected against by certification authorities
    - Automation will eliminate some of these sources of human errors

- *Improve TIP MoU requirements or other MVP requirements*
- **Standardize of test tool configuratio**n (but conflict of interest with test tool vendors?)
- Could we work on the **exchangeability of config files?**
- Individual test tool vendor initiative to create standard scripts for their tools: Industry solution or sales tool for the test vendor? -> needs to be repeatable across tools in the end, ideally including open source tools to prevent tool vendor lock-in

How to demonstrate that in the next months?

- Define pass/fail criteria, including margins where needed
- Margins will differ per deployment scenario, ask operators to define deployment scenario requirements, raise technical requirements for certification (MVP) with help from operator requirements
- Run a trial of certifying a few reference solutions by multiple labs
- Create governance (like a Certification authority) in the O-RAN Alliance similar to TIP Test & Verification Committee (TVC)
- Define a peer review process between labs and do one exercise, including feedback loop to test specification editors

Possible questions (provided by NTIA):

- *What are the differences and commonalities in testing based on geographical location (e.g., frequency settings, security, frequency sharing)?*
- *How do we achieve the interoperability of multi-vendor components?*
- *How to replicate the same conditions and same environment in the lab? Lower/Upper bound to reach consistency?*
- *How do we add supportability testing, e.g., managing deployed network functions, scalability, resiliency, robustness?*
- *Is there a need for lab accreditation or result certification by an independent body?*
- *The first step is to repeat the same test at multiple labs. What comes next?*
- *What standard metrics and KPIs?*

Breakout Session #4—How accurate do tests need to be, and how large of differences are significant?

Led by Doug Montgomery (NIST)

Possible questions:

- What standard deviation is acceptable if there are difference is testing between testing in different labs in the world if the same test setup and environment is used?
- What are the attributes or measurements of uncertainty?
- We need a way to explain the differences (e.g., errors in testing process vs explainable differences between labs)

• Who should be responsible for creating the metrics (e.g., ATIS-MVP, O-RAN ALLIANCE, universities)?

[Insert overall decisions here]

- **Composition of Breakout Group**
  - Test system vendor
  - USG research, standards, and mission agencies
  - Academic
- **Key Questions To Address**
  - Accuracy of what?
  - For what purpose?
    - What are the categories of purposes?
- **Key Observations**
  - The accuracy question breaks down in questions about the accuracy of
    - Inputs - test specifications, test methods, test input data, IUT capabilities, IUT configuration
    - Test exectuion - test execution, metrics and measurements of certainty.
    - Test results - accuracy of the test results for specific usecases.
  - Accuracy is different for specific usecases
    - Test program accreditation and calibration
      - Synthetic - curated data sets designed to address laboratory quality control - profiincy tests, test method validation, results determination.
    - Standards Conformance
      - Base standards and community profiles.
      - Base performance, resilience tests. Defined by SDOs.
    - Specific user / usecases testing
      - Defined by user groups / use cases.
      - Specific profiles of functionality, test inputs, KPIs and result
      - MNO usecases, specific users groups (Goverments), specific use cases.
- **Plans to Make Progress**
  - Walk before we run ….
  - Begin to embrace that there are multiple use cases for testing
    - And possibly different classes of test users / processes
      - Innovation testing,
      - demonstration testing,
      - product certification testing,
      - system integration and performance testing.
  - Begin to develop a quality control program for the product certification labs.
    - Basic unit tests for test method validation, proficiency testing, inter-laboratory comparisons, regression testing of test program.

        - Determine who / how large scale systems integration testing will be conducted.
            - User / usecase driven.
-

Breakout Session #5—What test frameworks and automation are needed?

Led by Eng Wei Koo (Keysight)

Possible questions:

- What are the challenges and needs for enhanced test automation?
- What level of test automation is needed?
- What are the key challenges for automating test cases?
- How prescriptive and how precise do the test cases need to be (e.g., some conditions are not specified)?
- What is the present state of automation?
- What area is the most impactful for automation?
- What constitutes a framework (e.g., blueprints)?
- Who disseminates and maintains this information?
- How are these answers impacted by differences between test vendors?

[Insert overall decisions here]

1. Test automation framework requirements enabling consistent, repeatable testing for conformance, interoperability - functional, performance, security, capacity, stability, robustness, resiliency among others
    a. **Test cases (high) quality** – clear documentation of input parameters, pre-conditions, test configuration, test scenarios (channel conditions, traffic models, subscribers models inc. mobility - velocity), procedures and outputs
        i. On the input parameters for e.g. the TDD UL/DL slots allocation, carrier bandwidth etc matter a lot for throughput testing and benchmarking for eg
        ii. Some of the test cases are written with parameters embedded in descriptive texts which makes it difficult to identify them
        iii. Test cases modularity - some test cases are difficult to modify for e.g to increase the number of UEs but keeping the rest of the test cases the same.
    b. **Test cases automation readiness** – the way the test cases are written may make sense for manual testing but not easily automatable with test scripts
    c. **Test cases automation where it makes sense** – some test cases are not automatable or fully automatable (automate as much as possible)
        i. e.g. inserting a USB drive into the server as one of the 3GPP security test cases

d. **Test cases automation needs to be further studied for RIC AI/ML enabled use cases** taking into consideration the AI/ML models lifecycle management including training, testing and validation.
    i. Suggest to consider starting a study
e. **Test automation needing reliable and consistent test cases selection**
    i. Smart selection required to avoid re-running all the test cases considering that testing time will be required to re-run all the test cases for every single change esp. Considering that there are multiple vendors involved.
    ii. AI/ML can be considered to be used for smart test cases selection (later)
f. **Test automation scripts needing to be validated** to ensure accuracy, consistency and repeatability
    i. Reference datasets and traffic models can be used here
g. **Test automation to include establishing the pre conditions of the test cases** and a **built in sanity check before executing the test cases**
h. **Test automation requires support of DUT configurability and observability**
    i. For e.g. DU configurability for fronthaul conformance require standards O1 support and if not available then need proprietary implementation
    ii. For e.g. Interfaces like WG4 fronthaul M plane may be encrypted and therefore logs may be required from the DUTs which will be vendor specific accesses and formats.
i. **Test automation scripts flexibilities in terms of varying test scenarios, cases, KPIs and KPIs values**
    i. **e.g. operators have more stringent criteria as compared to standardized test cases** such as availability, reliability, retainability values as compared to general test results.
    ii. **Performance tests will require guidance from blueprints (deployments, products capabilities)** as DUTs are designed for different deployment scenarios and therefore performance targets.
    iii. Capacity and soak testing performed in the operators labs prior to field deployments.
j. **Additional observability for soak tests**
    i. for e.g. where memory consumption can be recorded and analyzed to detect potential memory leaks which may result in outages in the deployments when operating for durations in the field greater than the lab test durations.
k. **Explore test automation to include field to lab so that field issues can be reproduced in the labs** to complete the CI/CD/CT lifecycle management.
l. **Automating security test cases** for e.g. vulnerabilities detection can be sent to the end users for self validation and reports generation with potential recommendations on the possible solutions.
m. **Test report generation**
    i. **Considerations to be compliant to ISO-17025 requirements** to ensure that the evidences are recorded for the required traceability

        ii. **recording additional information on the device under test** e.g. DU tested with or without specific **accelerators**
        iii. **machine readability of test reports** – test results, and summary reports are straight forward but the detailed reports with pictures/graphs/freeform texts are less straightforward and need to be reviewed if advanced technologies such as image recognition can help.
    n. **Automated root cause analysis** esp. important for stability, long term, soak tests in the lab and extended to field deployments
        i. Using AI/ML assisted techniques
    o. Diversity of the test automation framework implementation
        i. Suggestion for O-RAN ALLIANCE to specify the test automation framework which can outline the components and interfaces of the test automation framework that can be implemented as one more components

1. Test automation applications
    a. Useful for pre-testing in the vendors lab prior to testing in the OTICs for certification and badging for e.g.

Breakout Session #6—How can we gather, sanitize, and maintain test data? (input and output)

Led by Binbin Chen (Singapore SUTD Associate Professor and Deputy Director of Future Communication R&D Program)

Possible questions:

- What results should be shared and with whom (confidentiality concerns)?
- How do we share and maintain executed test results?
- How much and what type of meta data is important for repeatability?
- What techniques are appropriate are needed for validation and cleaning?
- What is important for training data? Where do we get it and who makes sure it is realistic?
- Who hosts and maintains test data?
- Can we create realistic simulated data, to enable AI/ML models?
- How do we compare and contrast simulated datasets?

Notes:

- Potential concerns in sharing data
    - NDA with device vendors

        - Testing labs are very careful in publishing data associated with vendors, regarding potentially sensitive information such as energy efficiency / performance / security issues.
        - This is different from the publication / sharing of test results for consumer / off-the-shelf devices (e.g., performance benchmarking by PCMag)
    - MNO data – user privacy, regulation, business interest, lack of incentive
    - IP / licensing issues – e.g., test scripts from testing solution vendors, joint IP developed through collaboration
    - Whether proper / sufficient sanitization has been applied to the data before sharing
- Potential leverage / low hanging fruits
    - Data based on open source projects: Easier to share packet traces / logs generated based on open-source O-DU/O-CU or other open-source tools.
    - Dataset contributed by academia
    - Sample test data
- Action items / next steps:
    - Compile lists for the various data that are useful.
        - What kind of data (metadata) needed, in what format
        - The scale needed
        - Potential use case?
    - Compile list of data that are already available and may be useful
        - E.g., for some countries, their cell site locations are in public domain.
        - Mobility traces (taxi, metro) are available in public domain for some big cities
        - Application-layer traffic data / statistics
        - Measurement data collected from research testbeds
        - Compose different types of data to meet the wishlist (see point above) and assess the quality —- may not be as realistic as real-world multidimensional data from MNO, but could already be a good starting point.
    - How to design mechanisms to give credit and incentive to organizations who share data.
        - In several academic conferences rigorous artifact reviews are conducted to make sure the experiment results can be reproduced independently by reviewers based on the submitted artifact (easier for software-only projects)
    - Mechanisms to share
        - If the data can be shared in public domain, may be easiest to share via the organization's own website / public repository (github / Kaggle) — full control, easier to update based on feedbacks, some may be directly through downloadable link, some can be upon request by email (so access control can be applied).

- If the data are mainly to be shared among O-RAN ALLIANCE members, may use O-RAN wiki, which has both confidential pages (mainly voting results) and non-confidential pages.
- Pair-wise sharing — governed by the NDA / other agreements by the two parties

Interactive Workshop—Policymakers

Discussions led by Discussion led by Jaisha Wray (NTIA/OIA)

[Insert notes here]

Breakout Session #1—Investments: Financial Support for Open RAN

Led by Ean Hundley (DFC)

[Insert notes here]

Breakout Session #2—Policy: Government Role to Enable Telecommunications Supplier Diversity

Led by Alex Botting (ORPC)

[Insert notes here]

Breakout Session #3—R&D and Testing: How Policymakers Can Best Support R&D Efforts

Led by Tom Rumbelow (UK DSIT)

- What are the different roles played by the different stakeholders in R&D and testing and how can those roles be optimized to promote consistent, repeatable, international testing?
- There are plenty of government supported (or aligned) testing laboratories, how can these laboratories best engage with independent or university-affiliated laboratories?
- The technical track is discussing how best to collaborate to ensure consistent, repeatable, international testing. How can the policy folks support the technical goals for consistent, repeatable, international testing? One example of this could be establishing an exchange program between technical folks and policy folks across governments to incentivize ongoing collaboration across countries.
- How can Open Testing Integration Center's be utilized to expedite testing and certification processes? Is there a standard approach to testing that OTICs might be able to facilitate and simplify for vendors and Mobile Network Operators?
- How do we ensure that R&D conducted by smaller vendors filters through to networks?
- How can independent labs and their outputs be trusted by MNOs?
- How can we engage in international R&D more effectively to leverage complementary strengths?
- How can researchers ensure that their work is feeding through into patents and standardisation processes?

Breakout Session #4—International Cooperation: Next Steps in Practical Cooperation Between Like Minded Governments

Led by Brian Larkin (NTIA)

[Insert notes here]

Interactive Workshop—Confounding Issues that Impact Testing

Discussion led by David Debrect (CableLabs) and Mark Poletti (CableLabs)

- Key issue from TIFG - quality of OTIC issuing certificates and badges. Working on this. Are lab certifications required?
- Key question, how to accredit OTICs and what services are available? IS this an O-RAN Alliance need or does industry need to figure it out?
- OTICs - are there more than the market can bear?
- What next after the testing in OTICs? Are RFP asking for certificates and badges? Not seen yet. Does this testing have value more than once? Can we create the further process moving to equipment acceptance and deployment/
- OTICs serve two functions - certification and badging - plugfests (to push the industry forward) - needs more organization, needs more application of the testing to equipment sales/deployment
- OTICS are a good environment for doing multi-vendor testing and quality of capabilities is improving. We have not seen operator demand in RFPs requiring OTIC certs yet, this will be a major step in the success on OTICs and Open RAN.
- Sustainability of the work in the labs and the labs themselves verses the “one-off” of plugfest.
- Policy side - can entities (governmental, other) promote policies that move the consumers (MNOs) to prefer testing results (e.g. certificates, badges)
- We need to get to a spot where OTICs certify and operators have a limited amount of testing beyond that to make it network ready.
- AT&T is very supportive of OTICs. Specifications are still “underspecified” and OTICs are still spinning up their capabilities
- Question of the value of certificates - do they reach/enable plug and play? Only 24 certificates total from 19 OTICs.
- RFP question - what can the ORAN community bring the industry to a point where ORAN and associated certifications are gating elements in such RFQs?
- Certification is not innovation. It can delay the process. It can present a baseline.
- Is lab federation an option?
- We should start by limiting what OTICs are focused on and not try to boil the ocean at each and every OTIC.
- Need to look at what areas need to be covered and figure out how to decide where to start and where to go, split up which lab does which thing, need to find focus for each OTICs

- Should be focus on system level certification - perhaps using “blueprints” based on regional MVPs and other similar documents. Similar issues are beginning to be addressed in the Optical industry.
- Also need to include the other areas that are important to operators such as 3GPP standards or specific features/functions - moving to a comprehensive view of testing required by MNOs. Formed in productized solutions.
- How do we continue to raise the competence of the labs - can this be accelerated by specialization of various labs.
- Open Source - can serve smaller vertical markets for both operation and testing. Is there a space in the middle of the market that can be supported by OS software.
- Different parts of the industry (markets segmentation) may have different needs, ie. tier 1 – enterprise – verticals – etc.
- Plugfests need to move to limiting the number of participants and move to deeper testing/demonstrations/test cases
- End-to-end appears in the marketplace to be the more critical issue as compared to OFH certification.
- Value of plugfests for smaller vendors is the access to specific equipment and a deeply trained staff support.
- Has the listing of present testing capabilities contained in one place (a follow on to the work completed by National Spectrum Consortium)? A central repository would be useful.
- We need to have more discussion around BSS functions when talking about other features, it is missing right now, might end up with many different vendor specific deployments.

Breakout Session #1—Do small lab-to-lab differences produce large differences in results?

Led by Lincoln Lavoie (University of New Hampshire, InterOperability Laboratory)

Group approached the question from the concept of a “root cause” analysis to determine the source of the differences between labs.

1. Test plans that do not fully specify the test environment, configuration setup:
    a. RF / Channel Models
    b. Configuration parameters
    c. Test plans should define confidence intervals (i.e. ensuring individual test cases are repeatable within the lab).
2. Reporting guidelines to standardize output and “proof” of testing
    a. Exact definitions of KPIs
    b. Ensuring specific parameters or configuration of equipment is captured.

    c. Ensure any additional steps required, such as performance tuning of the system, DUT, etc. are documented within the results.
3. Different integration options from the specifications
    a. Not fully solved through things like the IOT profiles.
4. Test tools
    a. Methods of implementation (i.e. mapping of test plan procedures to tool specific procedures). This requires input from the tool providers.
    b. Definition of calibration processes, to ensure test setup or approach is accurate prior to the start of testing.
5. Lab Accreditation (ISO17025)
    a. Won't improve the lab testing or quality beyond what is described in the test plan, if the test plan is ambiguous, the accreditation just ensures the lab follows that test plan, ambiguities and all.

Breakout Session #2—What factors matter the most?

Led by Tim O'Shea (DeepSig)

[Insert notes here]

Breakout Session #3—What factors can be ignored?

Led by Todd Loeffelholz (Airspan)

Session not held. No one thought any factors should be ignored. This discussion was combined with Session 4 below.

[Insert notes here]

Breakout Session #4—How does the priority of features for commercialization impact testing

Led by Sridhar Rajagopal (Mavenir)

(1) Consolidate list of discussion points
(2) Explore possible solutions

[If you were in the discussion and feel some aspect got missed in the discussion notes below, please email sridhar.rajagopal@mavenir.com to get your updates included]

Summary:

1. **Feature prioritization and test impact**
    a. **There will be variation of prioritization based on vendors/suppliers/operators/system integrators**
    b. **Both 3GPP & O-RAN aspects may need to be considered for feature prioritization**
    c. **Feature priority are related to functional priorities (e.g. throughput, latency, energy efficiency) as well as operational priorities (e.g. stability, analytics, FCAPS)**
    d. **To solve this issue, first step would be for priority collection from all geos (we have some for EU / G5 / MoU and ATIS / MVP - but not for all geos). The next step would be to seek further harmonization to the extent possible (which may not be practical) and then labs/OTICs could focus on this common requirement which may reduce efforts on the operators side for their validation**
2. **New feature evolution/ updates and prioritization for testing**
    a. **Features keep evolving - O-RAN specification updates, 3GPP releases**
    b. **Baselining is very important and first step**
    c. **To help with new features and evolution, good to also understand roadmaps in a multi-vendor scenario and also evolution of priorities**
    d. **Test plan updates and process for updates needs clarity and transparency**
    e. **Feature updates may also have different timescales**
        i. **HW refresh may be slower (radio < cell site < data center) (e.g. once in 10 years) while SW updates and upgrades may happen more frequently (e.g. once every 3 months)**
3. **Lifecycle management for features for commercialization**
    a. **Asynchronous updates across vendors in a multi-vendor setup**
    b. **Need to have list of basic sanity tests vs. delta changes. CI/CD is a lot of investment**
    c. **AI/ML tools may help in issue identification and test case prioritization**
    d. **Upgrades/downgrade aspects need to be considered and automation is a critical aspect as well**
    e. **Independent 3rd party may also help**
4. **Prioritization of new features pending commercialization and test impact**
    a. **Discussion on near RT RIC and xAPPs such as energy savings**
    b. **Test plans not fully evolved in standards - test procedures not clear**
    c. **Operators and innovators may not necessarily align to O-RAN UCTG use cases**

Other Discussion points: (We did not get to cover all these items)

1. What features are priority for ALL operators?
    1. E.g. throughput, latency, energy efficiency improving features
    2. How to address testing aspects and configurations for unique operator-specific features?
2. What are the differences between testing in labs and OTA vs. testing in a commercial network?
    1. How to introduce a new feature in a commercial network and test it before launching the feature at scale?
3. How does time constraints for delivery of releases impact testing?
    1. Considerations such as parallel test lines, negative testing,
    2. How does phasing of a feature impact testing? E.g. regression testing
4. How to address and test for feature interactions – e.g. new feature introduction with existing features?
    1. How to make sure a new feature does not degrade established KPIs or functionality of other existing features?
5. How to address and test for backward compatibility of other network elements, operating systems or devices?
    1. E.g. introduction of new radio with existing radios or a new device with feature support vs. existing device that does not have the feature support
6. How to efficiently test features that require comprehensive E2E test setups such as VoNR or inter-vendor HO?
    1. How to address complex features such as network slicing where the requirements are dynamic and on a policy level and need to be mapped to vendor test configurations?
7. Who pays for what testing?
    1. Govt / Consortiums/vendors
    2. UE, E2E testing aspects

Breakout Session #5—Decoupled service management and orchestration (SMO)

Led by Haseeb Akhtar (Ericsson delegate to ORAN ALLIANCE WG1)

[Insert notes here]

Breakout Session #6—Lifecycle management, CI / CD / CT

Led by Irfan Ghauri (OpenAirInterface Foundation)

Argument: Reference implementations facilitate testing and benchmarking and thus create value for the broad Open RAN community (industry, research community and standards-in-the-making) - let us debate

Possible topics:

- The idea: End to end reference implementations of cellular networks (Open RAN) maintained in participating labs - what is required?
- The pieces: network functions, deployment frameworks, automation, labs and testing
    - The role of open source communities, vendors and carriers
    - The role of labs
    - The role of enablers: open source communities, industry, government
- How does everything fit together - Lifecycle management

At the breakout the following discussion ensued:

- Attendance: Julie - NTIA , Jin Li - KEYSIGHT, Doug - NIST, Ashok - NIST, Michele - NORTHEASTERN UNIV., Tianyi - IOWA STATE UNIV., Irfan - OPENAIRINTERFACE
- Discussion around what the CI, CD, CT mean to different people and let us try to converge to a common understanding
- What we are looking at is an end to end deployed Open RAN compliant network that can be used as a reference implementation - there is a relation to the end to end 5G super blueprint concept of LFN that the CI/CD/CT is trying to build out. The O-RAN OSFG is also a thought leader of this concept.
- Stakeholders of the CI/CD/CT framework are
    - open source projects,
    - labs that deploy and test the end to end system,
    - those for whom this end to end has value (vendors for instance) for running use-cases in these labs.
- CI was identified as the process by which new features are added into the open source codebase (along with associated unit tests allowing to test those features). This is process is alternatively known as **Test Driven Development**
- Labs deploying platforms using software from different open source (or other components) define **conformance tests** (CD) based upon their knowledge of the specs, and work closely in a feedback loop with the open source projects to run those tests and report back bugs/features.
- Labs and their partners also continuously and periodically run other tests that we qualify as **Use-case/research related tests (CT).** The results of these tests are to be consumed by different parties including the open source communities as feedback and use-case owners to benchmark the solutions and its Technical Readiness Level (TRL).

- Other topics and open questions:
    - How will parties requiring new features get their features in? One possibility is they will engage with the open source communities and labs for integration and testing respectively
    - Transparency in the features, roadmaps, documentation etc. which is usually a challenge in open source communities - maybe AI/ML can help Michele said
    - Who are the blueprint managers - resources to put this in place - the interest from industry, governments, etc. Who is playing for this and why would they pay?

Interactive Workshop—Building Trust

Discussion led by Lauriston Hardin (NTIA/ITS), assisted by Ian Wong (Viavi Solutions)

- Consistent repeatable across labs - but why?
- Trust relates to risk – trying to overcome folks inertia to risk,i.e. “Nobody gets fired for buying from IBM”
- How do we come up with confidence measures?
- What is your biggest barrier in terms of “risk”?
    - Operator perspective - network serves 100Ms of customers, 100% safe and sure that nothing gets broken, if something goes wrong, it can be rolled back, service is guaranteed
        - There is an established system on how the risk is shared between operator and big vendors
        - In Open RAN, we are still learning
    - In the US market, there are no new customers, so customer experience is everything
        - If it break, you are a big enough company that can fix this for me
    - Academic perspective: How do you model trust/risk? On the side of risk, 3 types: risk tolerant, risk neutral, risk averse.
        - There has to be a type of Nash equilibrium -
    - Facing a rather big change, 6G is going to look a lot more open, the models are changing
    - For O-RAN, need to come sooner, PWSCIF wants to to diversify the supply chain
    - How do the vendors come together to create that momentum to get somebody to be a first mover
        - Appetite to try something new for smaller players
        - Improve coverage, shared network – willing to take the risk and see the benefit

        - Takes a long journey of convincing operators to put the right set of partners
    - Another aspect, established responsibilities and roles, triggered by Cloudification and Softwarization - how can we use these new opportunities that comes with new responsibilities
        - Need a lot more SW developers, etc..
        - Germany: global economy challenges, can DT develop their own SMO?
        - No guarantee that it will come right on time
    - Army doctrine
        - Trust is shared confidence amongst commanders, soldiers..
    - So after a plugfest, do you continue the relationship?
        - Have built the relationships and developed into business relationships
        - What we did in the DT lab, integration in pieces, new radios, new core network combination, number of xapps and scenarios, and all tested in Berlin lab
    - We talked a lot about business case - group of engineers, and are set and assigned to work on things, and you have customers around the globe asking you for new radios, you would put your resources to support your customers. If the specs are good, and the interfaces have been tested, and you have automated those, then the effort will be smaller
    - So where are the “holes” in the trust across the network lifecycle
        - Limited time and resources, if I have to cut corners, i need to make sure my stuff is ok-this can be the vulnerability from a testing perspective
            - Can the multiple vendors act like a team?
        - Test plan doesn't fully meet the operator’s demands-the testing is not delivering what they want - leading to duplication of effort
        - Vulnerable trust links are exactly the links - no single neck to choke-the interop issues - how about SI?
            - SI could be one of the solutions - there are 3 types – operator-led, vendor led, or independent SI
            - There are pros and cons
    - Operators need to answer - what type of ecosystem do you want to see?
        - NFV - HW layer, SW layer, then it will be multi-vendor! But it now become integrator led deployment
        - Vendors of SW, almost died - and nobody was buying - functionality great, performance really bad
    - We (the ecosystem) do not want to trust other partners, we want to work in a zero-trust environment –
    - From an OAT standpoint, this have not been addressed
        - From a major MNO standpoint - we need to leverage the economies of scale
        - Need to have a bare minimum set of tests, and this will not be the end-all

- Why would there not be trust? There's vested interest-there is shared interest in making it work, whether from each vendor, or testing entities, sustainability - if they share info, won't they be helping the competition
- From a TIFG stand-point, won't this be a priority?
  - Yes, improving quality of certificates/badges, improving trust on OTICs, are all priorities, but we're contribution driven so need the community to step up
- Is the ATIS MVP or the G5 MOU group the answer? Can we do a global one?
  - European operators MOU is a good step and aligned on high-level requirements - a lot of work to translate these to a working test plan
  - If we would have that, this includes a lot of tests beyond the O-RAN interface tests, but this is the direction go

Breakout Session #1—How can buyers trust that a lab produces consistent, repeatable, world-wide testing?

Led by Ganesh Shenbagaraman (Radisys)

1. Lab capabilities:
   a. Min capailities of lab (region/MVP specific):Infrastructure in general
   b. Test equipment calibration
2. Processes and Accreditations
   a. Scope of improvement on oversight/diligence from lab: What are the things changing during test execution?
   b. Lab accreditation: ISO 17205 certification
   c. Regular audits of the labs
3. Documentation (Verifiable records)
   a. Settings and config
   b. Test results and complete logs
   c. Failures and reruns - How many returns
   d. Feedback to vendors for improvement?
4. Test results reporting and presentation
   a. Examples: THroughput, latency, jitter
   b. Margins and upper/lower bounds
   c. Statistically varying metrics (Std Dev, Mean, Avg)
   d. Test specs should specify limits.
   e. Number of test runs obtain the variances
   f. Variation across system versions vs baseline
   g. Degradation/regression
   h. Impairments: FH, radio environment, transport
5. Expected from lab (Types of testing)
   a. Automation for repeatability
   b. Conformance/IOT
6. Nice to have capabilities

    a. Long run stability - nice to have
    b. Outdoor env
    c. Exploratory tests
7. Building confidence
    a. Certificate validity - Snapshot - Need to recertify?
    b. Anonymized results in public domain from O-RAN alliance
    c. Trends report over a period
    d. Comparing performance of labs (No of tests, interops, badges and certs)

Breakout Session #2—What makes consistent testing valuable to customers? What do you get when the testing is done?

Led by Ian Wong (VIAVI)

- If you're an operator - it's reducing test burden, increased confidence
- Consistent - if it's inconsistent that's a big issue
- Common
    - Making it reusable, solving the same problems for multiple operators
- How about the supplier
    - If you can do the testing and lower the bar to get into the operator lab
    - Changes the value proposition
- For an MNO, the risk is if the new vendor just doesn't work
    - Consistent testing and results getting E2E test out of the way, then you do performance evaluation, and roadmap
    - Its not just about the tests, but about the features - carrier aggregation, higher order MIMO - like for like
- There are those that are SIs, and those that are not, there's also the private networks, more likely to achieve a certain level of testing - use the certifcates/badges the established
- Confidence of certificates/badges are likely not there
    - Transparency, rigor
- What parts of the common tests have been knocked off
- For each iteration of what's required, there need to be a baseline, and what are the results
- What are the requirement of the labs – ISO?
- Need a governance model, this is what the testing framework look like
    - Isn't this the O-RAN alliancE?
    - There need to be a minimum level of testing setup for this defined
    - So there's some uniformity
    - What triggered a retest?
- Having someone like O-RAN ALLIANCE specify confidence intervals
    - I.e. repeat it 3 times, and it should be passed all 3

    - Spelled out incredibly detailed requirements
- Without some more rigorous quality control, to some extent your least functional lab drags down everyone
- Coverage of the tests are not sufficient from an operator standpoint
- Some of the NTIA funding is helping
- Conformance to the standards – better be through and basic – do less but do it much better
    - Some operators wants plug and play, others may want
- Performance is going to be very user group specific, we aldo don't want to have to
- Can we extract common performance benchmarks? That clearly isn't meeting the requirements today
- How about TIP? Don't they have of these from the MOU group?
    - Yes, but it's not fully there yet
- How about the fact that the performance is highly dependent on the platform, i.e hardware, virtualization platform, SW, etc..
    - This seems to be more on pre-deployment
- How about the OREX model?
    - Maybe for Private 5G
    - But likely not for major MNOs
    - Private 5G should be closer to Enterprise Wifi than RAN
- Approved minimum test cases that people agree to and what the lab looks like and repeatability and confidence levels
    - There's some of that in O-RAN
    - Bar is very low to be an OTIC
    - Improve the OTIC qualification process
    - ISO is not a magic bullet - if the test plan is not rock solid
    - Multiple flavors make it hard to please the operators
    - OTICs can always sell their services to do the system-level tests
    - Having operators chime in what the gap is
- Test plan product have to be consumed
-

[Insert notes here]

Breakout Session #3—Are badging and certification enough? Is there something more specific that can be done to address MNO needs?

Led by Abdel Bagegni (TIP)

Are badging and certification enough? Is there something more specific that can be done to address MNO needs?

- What kinds of badges and certifications are necessary?

- Is there something other than badging and certification that MNOs want?

Breakout Discussions:

What are the main drivers for badging and certifications?

- Create a performance baseline for the industry
- Reduce the operators' testing:
    - RFP component operator test offloading)
- Allow Tier 2 operators to adopt OpenRAN
- Market enablement and opportunities, especially for smaller vendors

Areas of Badging?

- Conformance
- Interoperability
- Functional
- Performance (including reliability, resilience, stress, .etc.)
- End-to-End Testing: What areas are covered by End-to-End Testing?

How do we make these certifications worthy & valuable?

- Provide MNOs with confidence in systems performance
- Not used as a marketing tool

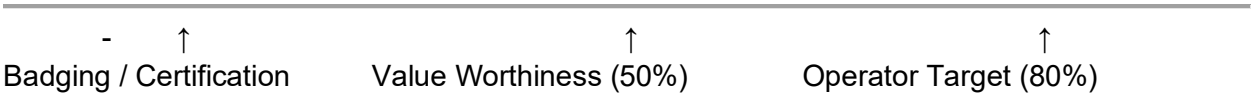
How to encourage vendors to participate

- Provide a commercial route / opportunity
- Competitive factor,
- Give publicity for vendors, especially small vendors
- QA efficiency and lessons learned

How likely would MNOs mandate badges in their procurement process?

Operational Readiness:

0% 100%



Is there something other than badging and certification that MNOs want?
Efforts to minimize testing, provides system performance confidence and shorter timelines to commercial deployments

Recommendations:

- Tighten test plan specifications and success criteria
- Collaboration and information sharing amongst certification bodies
    - Reduce duplications
    - Joint efforts towards a common goal

We've been very focused on Tier 1, there's a lot of Tier 2 and 3 operators. They're generally fast followers. But maybe we might break that mold and see how we can address their needs that maybe.

Breakout Session #4—How do we demonstrate performance parity to legacy systems?

Led by Julie Kub (NTIA/ITS)

1. Define RAN performance benchmarking methodology
    a. Traditional base station
    b. Single vendor base station O-RAN implementation
    c. Multi vendors base station O-RAN implementation

2. Define RAN performance benchmarking test cases
    a. Ensuring **test scenarios** are highly representative of operators' deployments – number of UEs, radio channel impairments, transport network impairments, mobility profiles, mixed end users services and application traffic.
    b. Ensuring **measurements and KPIs** are properly defined for performance test cases including accessibility, retainability, availability, mobility, energy consumption, efficiency among others.

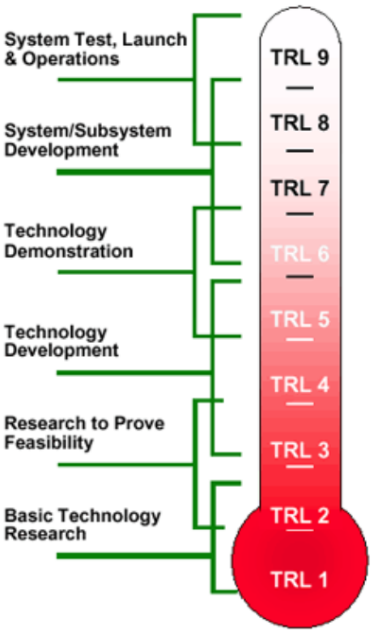
c. Ensuring **consistent and repeatable testing** ensuring that the input parameters are clearly specified e.g. TDD slot formats, carrier bandwidth etc.
d. Ensuring apple to apple comparison as much as possible including **DUT capabilities** such as RU categories, **configuration** such as NR deployment options, network slices
e. Ensuring that the **test durations** are specified e.g. 24, 48, 96 hours e.g.
f. Ensuring that the **test cases can be easily extended** for different deployment scenarios and base station capabilities e.g. macro vs small cells.
g. Ensuring that the **DUTs/SUTs information** including hardware/software options and configurations are logged as part of the test reports.
h. Review and leverage the currently available test cases in the public domain from O-RAN ALLIANCE
i. Develop additional test cases to fill in the gaps

3. Test execution using test automation and reporting output with machine readable outputs (for certain report types)

How are we getting those benchmarks? – there are consortiums that there is this testing

Breakout Session #5—Are technology readiness levels (TRL) necessary?

Led by Charles Turyagyenda (Digital Catapult/SONIC Labs UK)



TRL definitions

TRL	NASA usage[4]	European Union[5]
1	Basic principles observed and reported	Basic principles observed
2	Technology concept and/or application formulated	Technology concept formulated
3	Analytical and experimental critical function and/or characteristic proof-of concept	Experimental proof of concept
4	Component and/or breadboard validation in laboratory environment	Technology validated in lab
5	Component and/or breadboard validation in relevant environment	Technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)
6	System/subsystem model or prototype demonstration in a relevant environment (ground or space)	Technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)
7	System prototype demonstration in a space environment	System prototype demonstration in operational environment
8	Actual system completed and "flight qualified" through test and demonstration (ground or space)	System complete and qualified
9	Actual system "flight proven" through successful mission operations	Actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

1. Attendees: Ladan - Fujistu, Pankaj Argwal - Rakutan, Irfan - Open Air Interface Gwen - R&S, Li - Keysight, A&T
2. Is TRL the right benchmark? Could badging be a better benchmark.
3. Who will be using the TRLs, most likely this would be the MNOs. We need to know the end customer for the TRL.
    a. Is the TRL an overhead on top of the certifications?
    b. TRL will be dependent on the use case, e.g. some use cases don't require as much performance metrics.
    c. TRL should be both on a product level and the system level.
    d. TRL are most used for policy decisions and might not translate directly to the technical features.
    e. Translate the TIP badging to the TRL Levels.
    f. TRL is a relative measure and depends on
    g. Three levels: Good, bad, medium levels might be a better option.
4. First rate the TRL individually on a product level and the rate the TRL for the combined

5. What purpose would TRLs serve to customers?

6. Are TRL levels applicable to disaggregated Open RAN functions that are constituent components of RAN? How would you rate the TRL levels for the Open RAN products currently on the market?

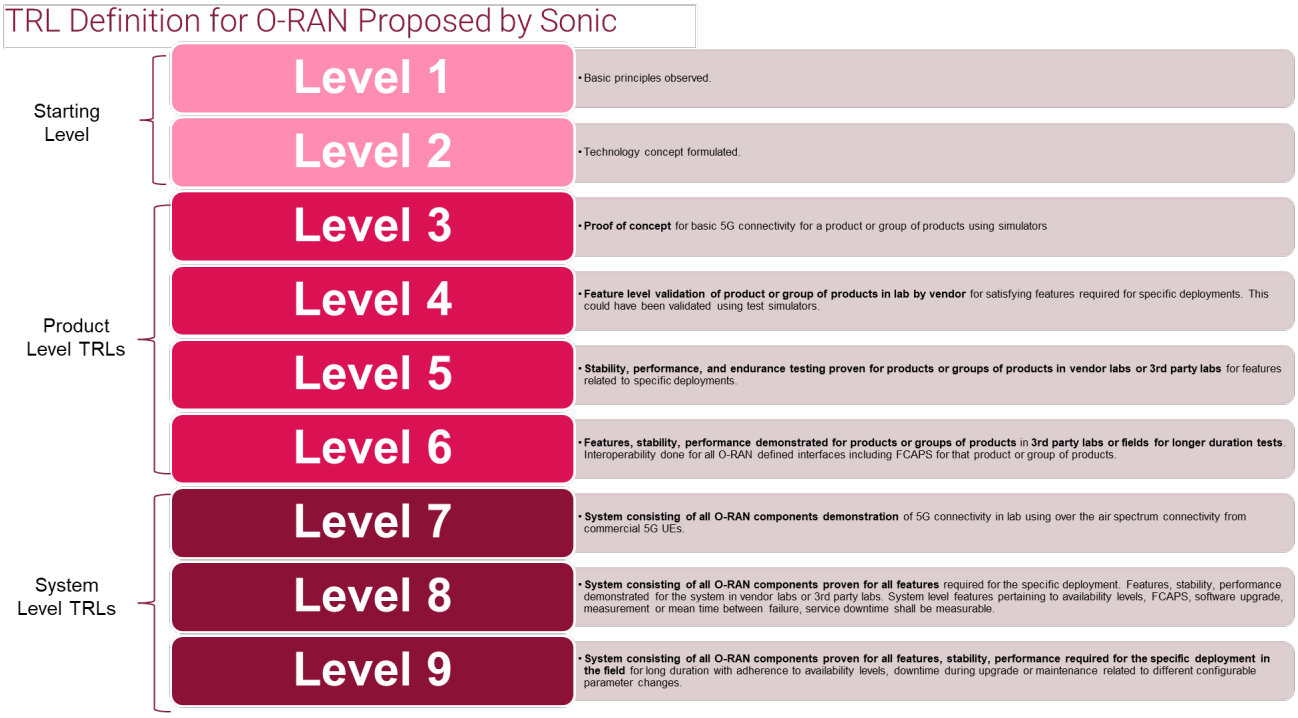
7. Which TRL levels are necessary?

8. What products or test systems do the TRLs describe?

9. Are TRL levels dependent on the deployment scenarios (indoor or Outdoor) of Open RAN systems?

10. Actions and open questions going forward?
    a. OTICs could use TRL levels instead of the TIP Badging.
    b. We need to figure out the TRL level are whether they are component based or system based
    c. TRIs Should be easily mapped to policy decisions.
    d. Application/ use case based weighting of TRLs is a good approach
    e. Integrated systems should have higher TRLS.
    f. TRL grading system is biased towards larger vendors who have more components of the overall system.
    g. What is the benefit for vendors to do the TRLs considering the additional effort required. Whoever does the TRL grading system should provide incentives
    h. How transparent is the tRL system?
    i. What tests need to be done to validate TRL levels?
    j. Would TRL help innovation in the market?

TRL is more a self declaration, but certification/badging is determined via testing? TRL declaration has to be overseen.



Breakout Session #6—System integration

Led by Monika Tarwala (Capgemini)

Possible Questions :System integration

- Who is responsible for system integration?
- What is the scope of the system integrator role?
- What role does the system integrator play in testing?

[Insert notes here]

Enterprise market - is dominated by the SIs; maybe this can be employed in Open RAN?

- We started with a good set of quorums, and didn't expect this level of energy after lunch and 3 days of discussion. Thank you all for your contributions.

Our topic was system Integration and we started with 3 major questions in mind

Who is responsible for SI/ What's the Scope of SI/Role of SI & Testing and challenges.

So, Who is responsible for SI roles

Here we started with 3 Options Operator led SI, Vendor led SI, Independent SI, also went through examples of current situation with Rakuten and Dish models and evaluated pros and cons of each SI, such as

- Operator led SI: they have operational expertise of their network which will save them some costs but at the risk of lack of expertise in the vendor system itself.

- Vendor led SI PROS: Have expertise of product but can be little biased and will favor their preferred combinations.

- Independent SI: PRO: While they have expertise in bringing all products together, but at extra costs.

- When put them in operator's shoes and asked which one they will choose, it varied and later

group agreed that best option will be to go with a Hybrid option of above three

Then we delved into what's the Scope/role of SI:

This could include Integration, Vendor Management, E2E Testing, Deployment and Life cycle management,

While Integration: its simple operators will need to outsource integration efforts to some extent but what extent vertically/horizontally is a question? What part of nw information operator will share with another integrator

Conclusion was probably that a hybrid model will come into picture where operators will keep smo parts to themselves and give other parts to Integrators.

Vendor Management will be necessary role

System Integrators could take over End to End testing responsibilities And also do life cycle management.

While it will be a big challenge , System Integrator could release and maintain their own sw release of certain combinations. And if anything specific is needed it would come at an extra cost.

Other Challenges with Hybrid models would be who will be accountable? While the group was split on this topic that it won't be an issue in case of outages, or anything that goes wrong in the network. I personally beg to differ.

Key Takeaways

- **In-House vs. Third-Party/ vendor SI**: There is no one-size-fits-all approach to SI in Open RAN, and operators will need to evaluate based on their capabilities and needs and probably will follow Hybrid model

- SI could bring in Vendor Management, Life cycle Management, Integration and Testing Support.

- **Cost Efficiency**: Open RAN promises lower CAPEX and OPEX, but achieving those savings requires overcoming significant SI and testing challenges.

- **Standardization Efforts**: The success of Open RAN deployments hinges on ongoing efforts to standardize interfaces, protocols, and testing frameworks across vendors.

Discussion on Collaboration

Discussion led by Ian Wong (VIAVI) as TIFG co-chair, assisted by Olli Andersson (Telecom Infra Project)

[Insert notes here]

Action Items:

Test case/test plan

- O-RAN test cases to make them more robust
    - Labs are stretched thin, want to contribute, but there needs to be a way that we can sustain that
- Julie - outcomes of this workshop will be fed into O-RAN
- Abdel - volunteers to push these outcomes into TIP
    - Can there be a forum?
    - TIP, O-RAN, ACCORD, ATIS, any other open forum?
    - Maybe a periodic meeting, even virtual, for these forums to come together to share views
- Julie- volunteers to organize the 2nd IORS as the forum for bringing this together
    - Maybe meetin. BvdbE g every 2 months which are virtual - working sessions
    - ITS will do work on the policy side, and have projects that are ongoing
    - Abdel is interested to attend this
    - Topics including:
        - Lincoln - Test coordination across the different groups, TIP, ORAN, ACCORD, supported by TIP, and ITS will be doing the work also
        - Does this include - Peer review, making tests more repeatable, etc…
        - This can facilitate inter-lab comparisons
        - i14Y (Andreas), VALOR (Ian W) can volunteer to do these tests for interlab comparison
        - NTIA is now a member in TIP
        - OTICs are setting up PlugFests now - more info available or maybe we can setup a discussion

        - OTIC Accreditation
            - Doug/NIST has volunteered their Director of conformity - to present at TIFG - things that we have to document and make decisions on
            - From here we can create a Work Item to come out of that
        - Julie - IORS wiki that inventory the lab collaborations
    - TIP working on performance test plans to be published before FYUZ (11/11)
        - Ollie/Julie - to summarize the outcomes from FYUZ
        - FYUZ can also be a good place to discuss some policy topics
    - Data?
        - We can describe the Meta-data
        - If it's synthetically generated
    -

Workforce development

-