INL/MIS-24-81340-Revision-0

Open RAN Security - Current Progress and Next Steps

October 2024

Arupjyoti Bhuyan

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-24-81340-Revision-0

Open RAN Security -Current Progress and Next Steps

Arupjyoti Bhuyan

October 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Dr. Arupjyoti (Arup) Bhuyan

Directorate Fellow, Idaho National Laboratory (INL)

Director, INL Wireless Security Institute (WSI)

Open RAN Security - Current Progress and Next Steps

IEEE Open RAN Security Working Group

Oct 3, 2024

Idaho National Laboratory

INL Wireless Security Institute (WSI)

VISION: National Leadership on Wireless Security for Secure Adoption of Advanced Technologies including 5G/ORAN, 6G, Wi-Fi 6E/7 and related Spectrum

MISSION: Provide best in class security research, assessments, evaluations, engineering support, and technology development to enable government and industry harvest the benefits of advanced wireless technologies

Innovative Research

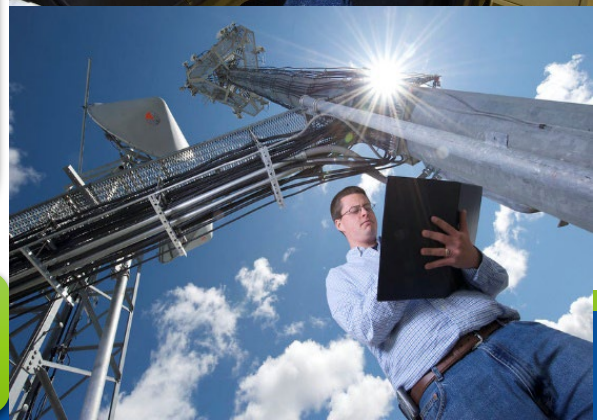
- Lab directed research on security of advanced technologies and secure spectrum use and sharing
- Externally funded research, analysis, and engineering studies to address national security gaps in secure use of 5G & Future G/6G technologies and spectrum
- Proof of Concept for development and deployment of secure real-world use cases with transformational technologies

Evaluation & Validation

- Effective, accurate, responsive testing and verification
- Advanced Lab based systems for highly efficient and intrusive testing
- Unique Wireless Test Bed (WTB) in outdoor environment providing capability to test real world scenarios at scale
- WTB Spectrum flexibility with NTIA experimental station status

External Collaborations

- Academic and Industry Researchers in US
- Hosting of National Security workshops and Conference Tracks addressing key security topics with participation from US Government, Industry, and Academia
- International collaboration with wireless leaders in US Government partner countries

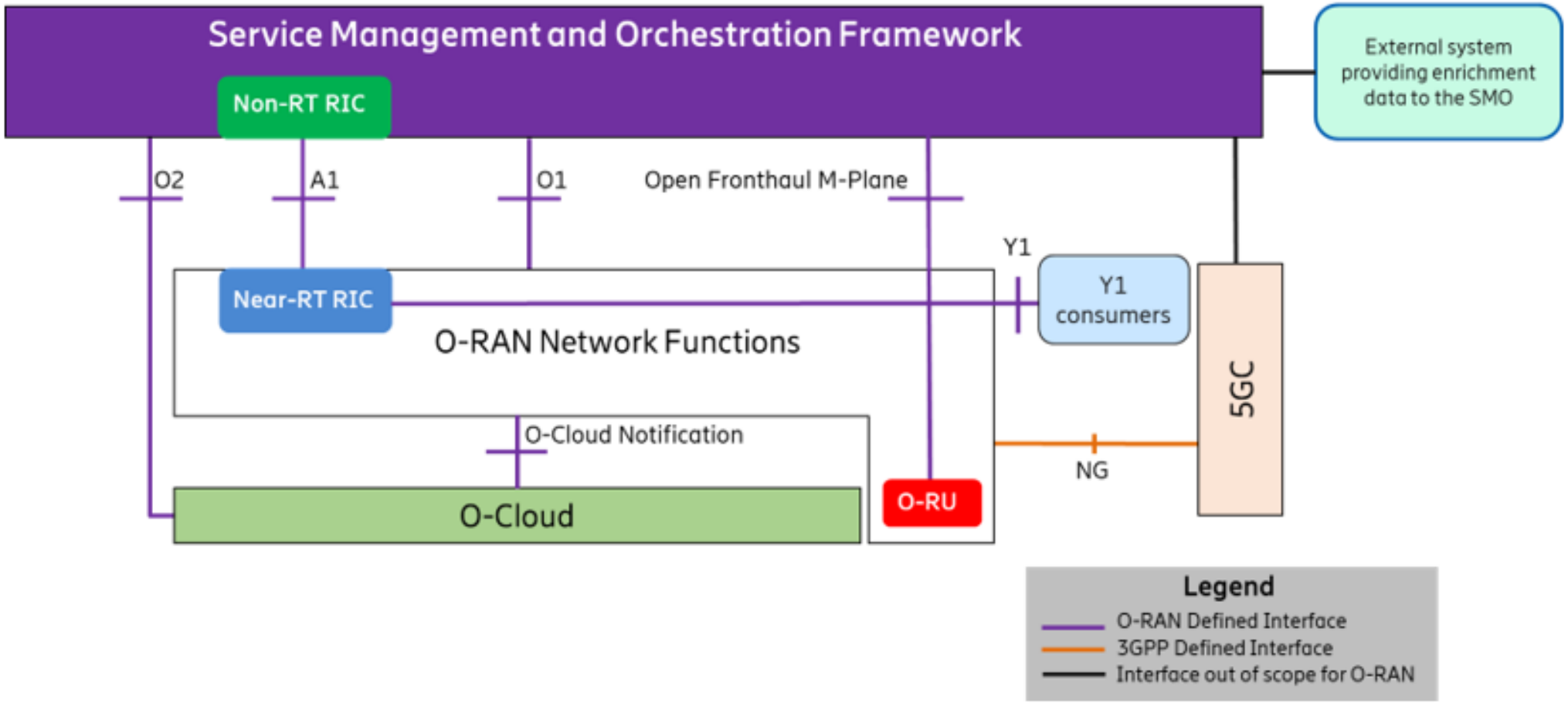


NOTABLE OUTCOMES: Diversely Funded RDD&D Portfolio supported by WSI as a National Authority on Wireless Security and utilizing resources across INL to exceed customer expectation

INL Wireless Security Programs

- **DOD OUSD**: Security Assessment for 5G Use in Untrusted Environments
- **NTIA/FCC/DoD/DOE**: National Spectrum Strategy (NSS) Implementation Plan (7/8 GHz Interference Study)
- **DOE-CIO**: 1) Spectrum Security for Advanced Wireless Technologies; 2) Spectrum Nuclear Power Plant Modernization with Advanced Wireless
- **DOE-CESER**: Study of harmful interference in 6 GHz to incumbents
- **CISA/NRMC/NISAC:** Study of 5G small cell backup batteries
- **NSF**: Collaboration with USC and Univ of Utah for two projects awarded in Phase 1 of Spectrum Innovation Initiative National Radio Dynamic Zones (SII-NRDZ)
- **DOJ/DoD**: Spectrum agile video surveillance communications
- Multiple LDRD research projects for WSI call section 5.3. Secure Wireless Communications and Dynamic Spectrum Sharing

O-RAN Architecture



5.1-1: High Level Architecture of O-RAN

O-RAN.WG1.OAD-R003-v12.00 (June 2024)

O-RAN xApp and rApp

- rApps: higher layer automation policies with a control loop greater than 1 second for Non-RT RIC
- xApps: operate with control loops as low as 10 mSec for Near-Real Time RIC (Near-RT RIC).

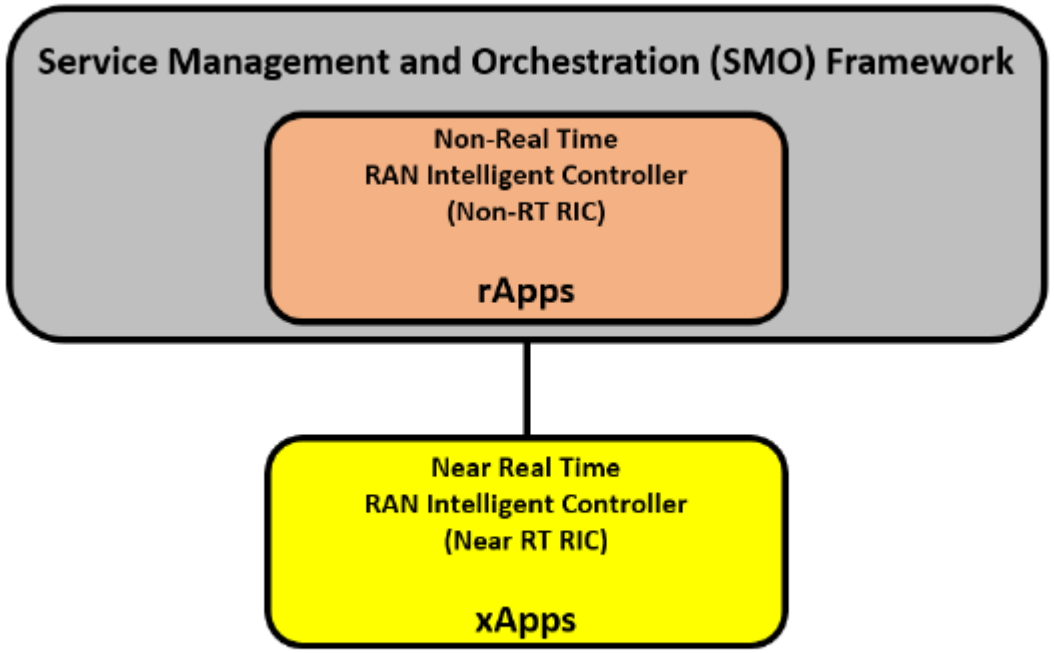
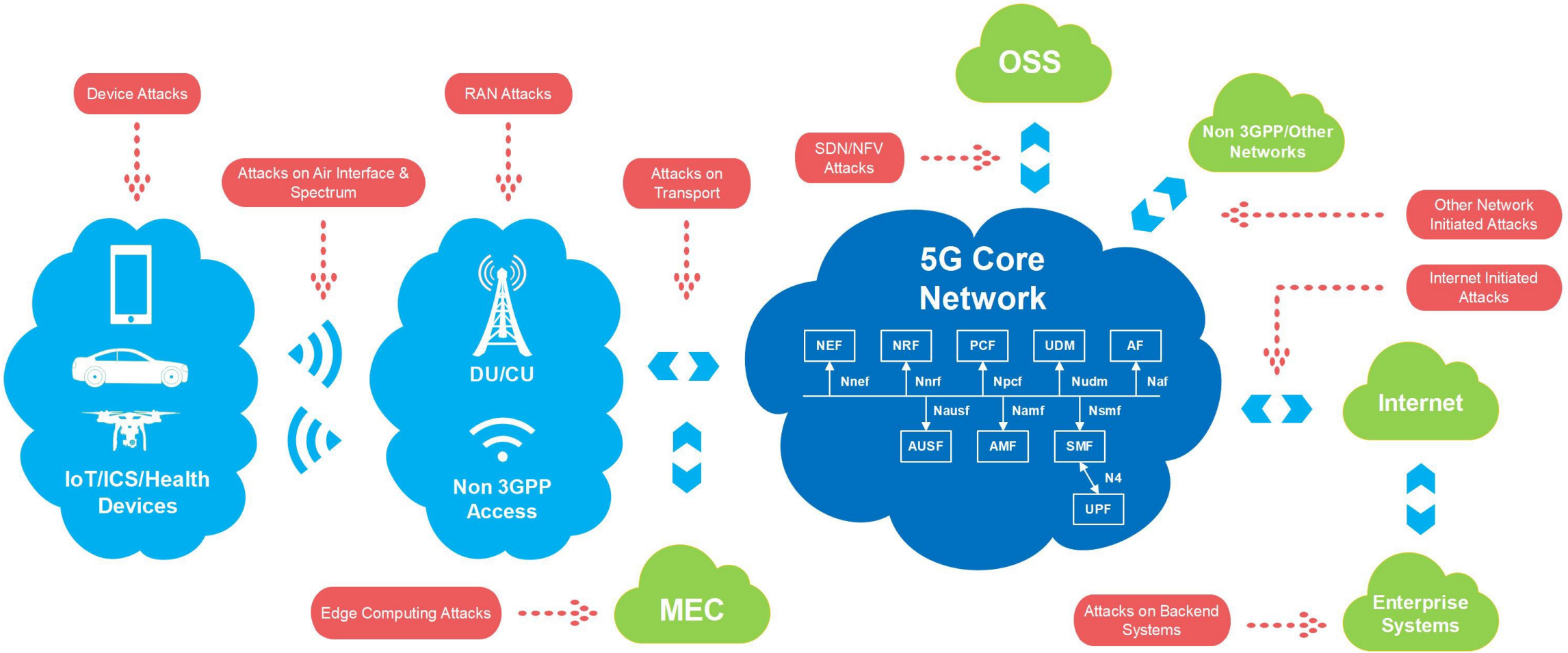


Figure 3 O-RAN Alliance defined rApps and xApps

- ✓ Data integrated with rApps and xApps and access to data sources should be protected with multi-factor authentication, confidentiality, integrity, and availability (ACIA)
- ✓ Secure peering between a) rApps and b) xApps
- ✓ Secure Y1 interface to RAN Analytics Information Exposure (RAIE)
- ✓ Secure AI and ML data sets and models

5G Network & Attack Surfaces

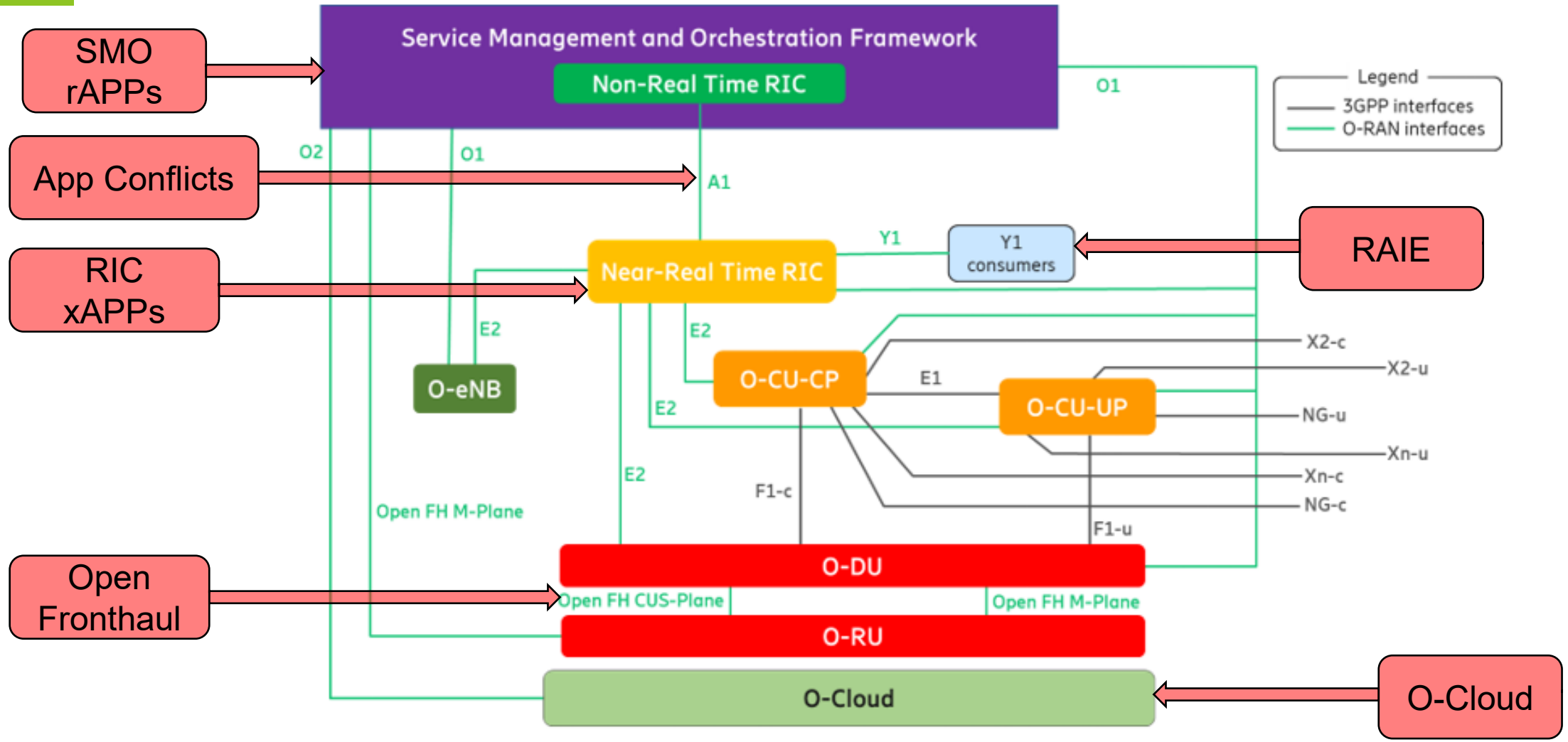


IoT: Internet of Things
ICS: Industrial Control System

MEC: Multi-access Edge Computing

SDN: Software Defined Networking
NFV: Network Function Virtualization
OSS: Operational Support System

O-RAN Attack Surfaces



5.1-2: Logical Architecture of O-RAN

O-RAN.WG1.OAD-R003-v12.00 (June 2024)

O-RAN WG11: Security Work Group

- O-RAN Release 3 Security Specifications as of June 2024 – builds on existing 3GPP Specifications and adds new ones

- ✓ O-RAN Security Threat Modeling and Risk Assessment 3.0
- ✓ O-RAN Security Requirements and Control Specifications 9.0
- ✓ O-RAN Security Protocol Specifications 9.0
- ✓ O-RAN Security Test Specifications 7.0
- ✓ O-RAN Study on Security for Near Real Time RIC and xApps 5.0
- ✓ O-RAN Study on Security for Non-RT-RIC 1.0
- ✓ O-RAN Study on Security for Service Management and Orchestration (SMO) 4.0
- ✓ O-RAN Study on Certificate Management Framework 2.0
- ✓ O-RAN OAuth2.0 Security 2.0
- ✓ O-RAN Study on Security for AI/ML 1.0
- ✓ O-RAN Study on Security for O-CLOUD 6.0

O-RAN TIFG: Test & Integration Focus Group

- O-RAN Criteria and Guidelines of Open Testing and Integration Centre (OTIC) 5.0
- O-RAN End-to-end Test Specification 6.0
- O-RAN Certification and Badging Processes and Procedures 9.0
  - ✓ Technical Specification
  - ✓ Summary Report Template
  - ✓ Test Report Template
- O-RAN Certifications
  - ✓ **O-RAN Certificate**: Verifies that a product complies with O-RAN specifications using O-RAN conformance tests
  - ✓ **O-RAN Interoperability (IOT) Badge**: Proves interoperability between a pair of products
  - ✓ **O-RAN End-to-End (E2E) Badge:** Demonstrates and validates that an end-to-end system or subsystem meets minimum requirements for functionality and security

First International Open RAN Symposium (IORS)

- Hosted by NTIA/ITS during Sep 17-19 in Golden, Colorado
- IORS to be held annually to accelerate the global adoption and deployment of interoperable Open Radio Access Networks (RAN)
- Attendees from US as well as UK, Canda, Germany, Japan, South Korea, India, Taiwan, and Vietnam.
  - ✓ **Government and FFRDCs** including NTIA/ITS, DoD OUSD R&E, NIST, INL, MITRE, i14y Lab/Deutsche Telekom, UK Department of Science, Innovation, and Technology (DSIT), Digital Catapult (UK), Innovation, Science, and Economic Development (ISED), Canada, Industrial Technology Research Institute (ITRI), Taiwan, Taipei Economic & Cultural Office (TECO) in Denver, Ministry of Internal Affairs and Communications (MIC), Japan, and Ministry of Science and ICT (MSIT), Republic of Korea.
  - ✓ **Industry** including Airspan, **AT&T (ACCoRD) ,** Booz Allen Hamilton, CableLabs, Capgemini, Deepsig, **EchoStar/DISH (ORCID),** Ericsson, European Advanced Networking Test Center (EANTC), Fujitsu Network Communications, Globalstar, Hewlett-Packard Enterprises, Juniper, Lekha Wireless Solutions, LF-Aether, LIONS Technology Inc., Mavenir, Nokia, OpenAirInterface (OAI), Parallel Wireless, Qualcomm, Radisys, Samsung, SOLiD, Tejas Networks , Verizon, Viavi, VVDN Technologies, Virginia Tech Applied Research Corporation, zTouch Networks, and TIP.
  - ✓ **Academia** including JHU/APL, NCSU (AERPAW PAWR/OTIC), Penn State, Rutgers, Iowa State University (ARA PAWR/OTIC), University of New Hampshire, VT/CCI (OTIC), KyungHee University, University of Leeds, National Yang Ming Chiao Tung University (NYCU).

IORS Focus on Security

- Technical Discussion Session on “Security Collaboration: Current Progress and Next Steps” led by INL (Arup Bhuyan) and Penn State (Syed Hussain)
- Current collaborations including security open testbeds for collaboration
- Key Open RAN Threats:
  - ✓ New interfaces for RNC Intelligent Controller (RIC)
  - ✓ xApp and rApp security
  - ✓ Malicious and Conflicting Apps
  - ✓ Protocol Stack Security, e.g., TLS, OAuth 2.0, REST, SSH
- Open RAN Security Testing
  - ✓ xApp and rApp security
  - ✓ RIC
  - ✓ RU, DU, and CU

Notes from IORS Breakout Session on Security

- Component level testing, Compositional testing, Lab scale testing, Testing in cloud settings, Deployment setting
- Testing for a minimum viable security profile
- Testing for secure software implementation including Open-source software (OSS), SBOM etc.
- Security certification process - need certification for different applications, e.g., regular traffic vs. security sensitive traffic, normal operations vs. mission critical operations
- Need attack scenarios/red teaming in addition to conformance testing provided by Open Ran specification
- Assure vendor diversity in security testing
- Ways to perform physical layer security testing
- Testing for supply chain security
- Testing for secure spectrum sharing

Idaho National Laboratory