SCTE
a subsidiary of CableLabs®

Creating Infinite Possibilities.

Establishing a Strong Security Posture for Open RAN

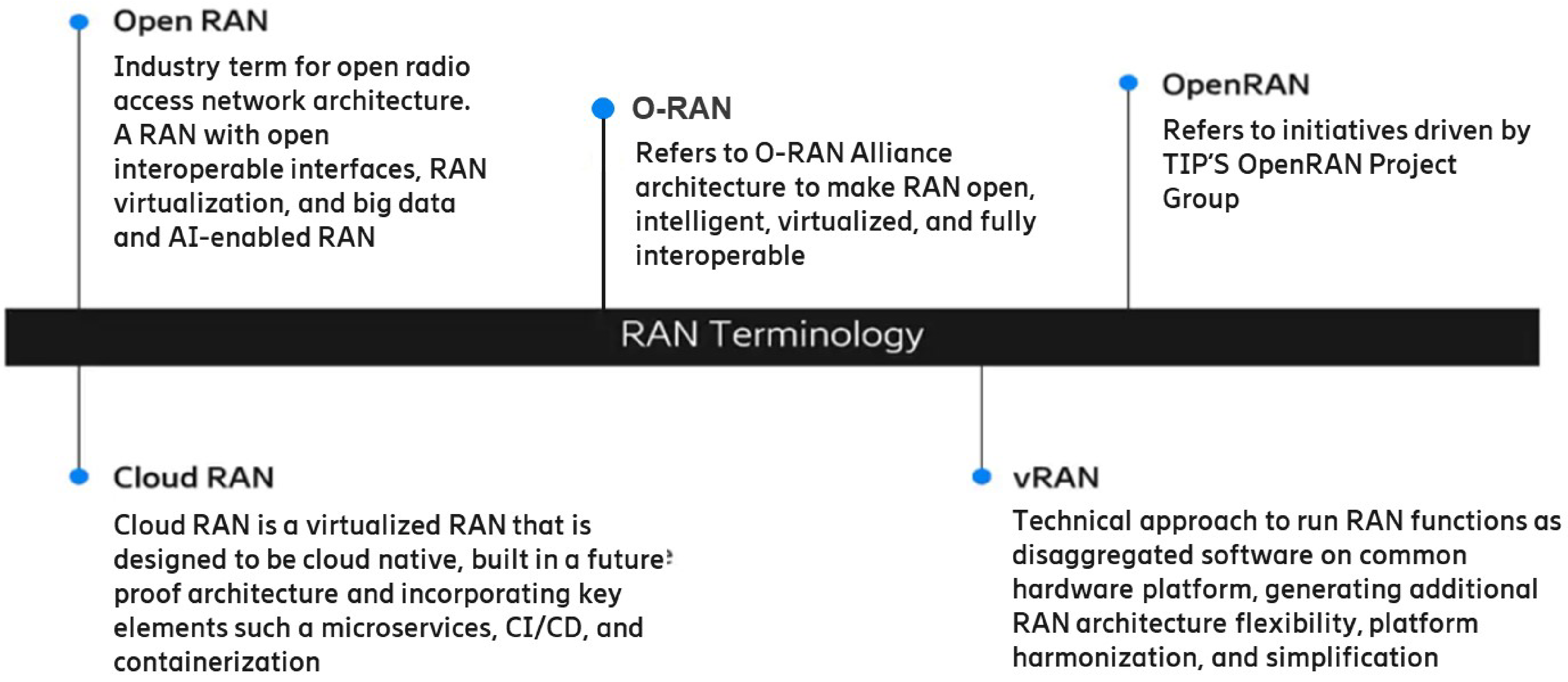
Scott Poretsky

Director of Security, North America
Ericsson
508.261.4429
scott.poretsky@ericsson.com

SCTE CABLE-TEC EXPO®22
SEPTEMBER 19-22 • PHILADELPHIA, PA

2022 Fall Technical Forum
SCTE® • CABLELABS® • NCTA

RAN Terminology



Open RAN

Industry term for open radio access network architecture. A RAN with open interoperable interfaces, RAN virtualization, and big data and AI-enabled RAN

O-RAN

Refers to O-RAN Alliance architecture to make RAN open, intelligent, virtualized, and fully interoperable

OpenRAN

Refers to initiatives driven by TIP'S OpenRAN Project Group

RAN Terminology

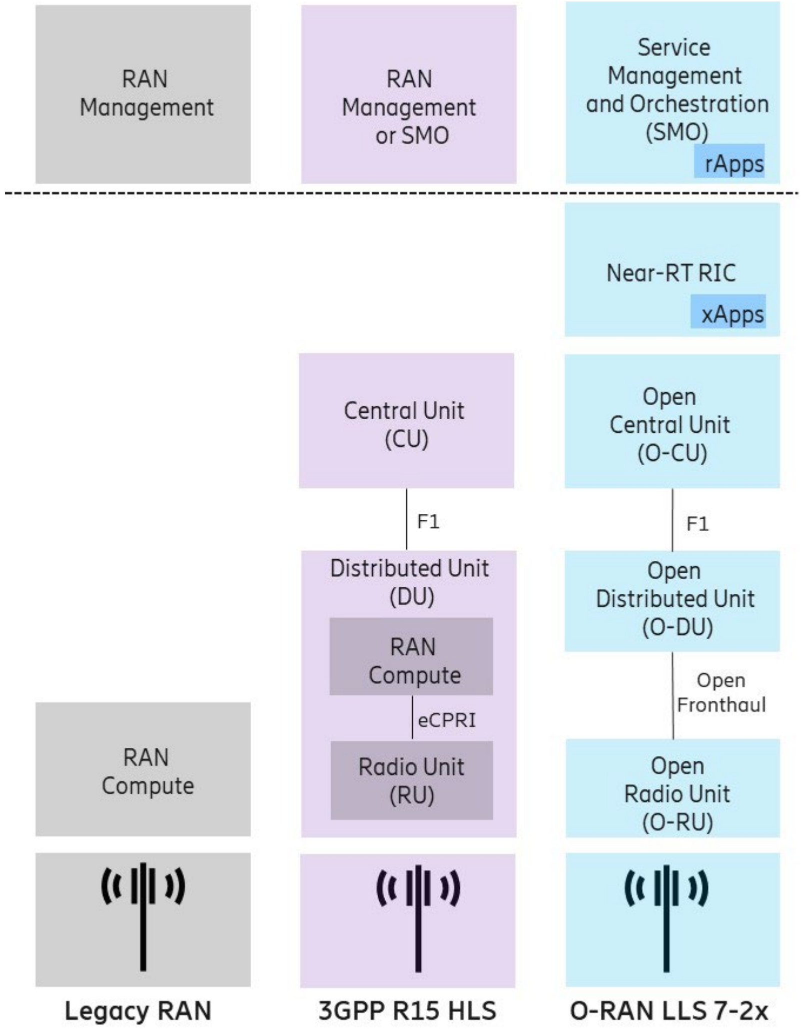
Cloud RAN

Cloud RAN is a virtualized RAN that is designed to be cloud native, built in a future-proof architecture and incorporating key elements such a microservices, CI/CD, and containerization

vRAN

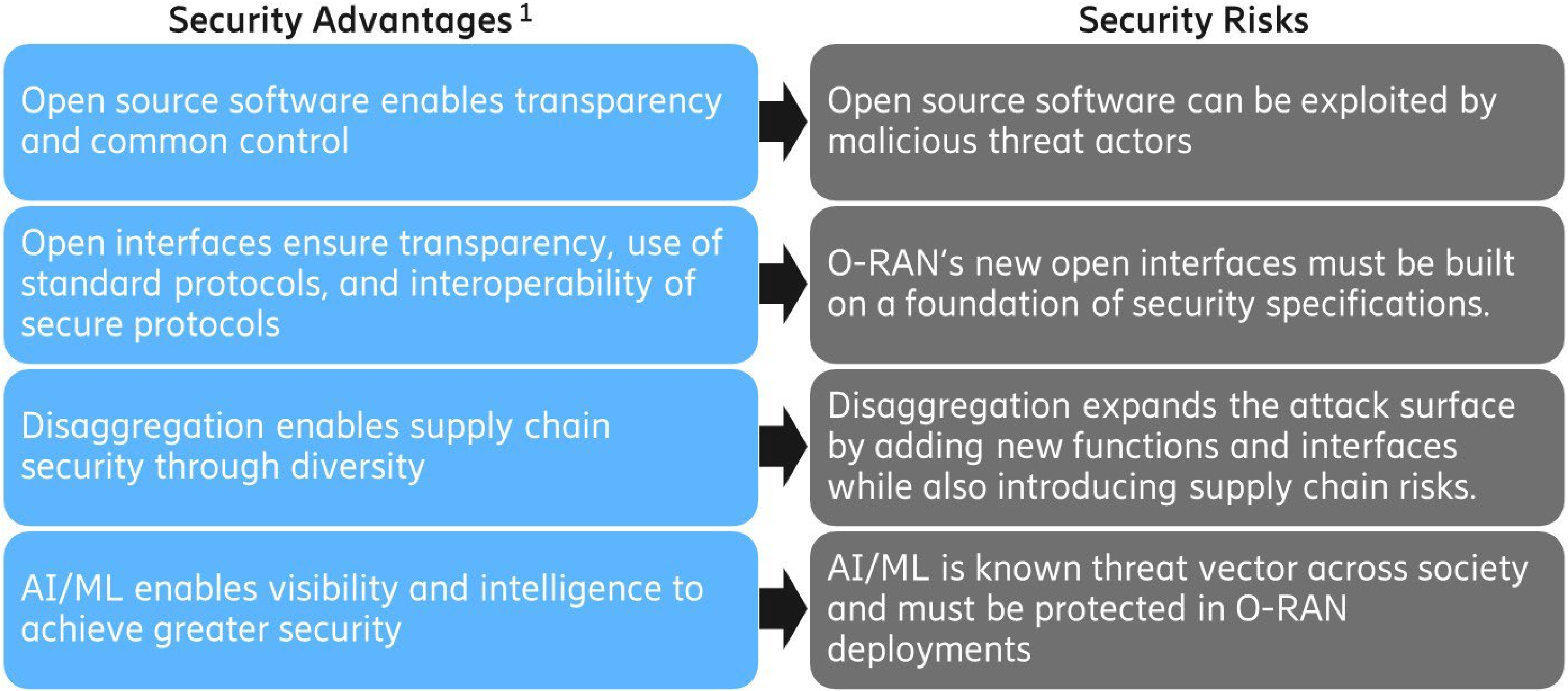
Technical approach to run RAN functions as disaggregated software on common hardware platform, generating additional RAN architecture flexibility, platform harmonization, and simplification

Evolving RAN Architectures



- Traditionally, baseband functionality has been proprietary hardware deployed at the cell sites.
- Baseband functionality can be implemented in software to operate on COTS server hardware at sites co-located with 5GC components.
- Open RAN solutions use the 3GPP specified air interface that is secure
- Ericsson Cloud RAN is based upon 3GPP R15 HLS having the RAN Compute disaggregated into a CU and DU
- The O-RAN architecture introduces a LLS disaggregating the RAN's O-DU and O-RU with the Open Fronthaul interface between them

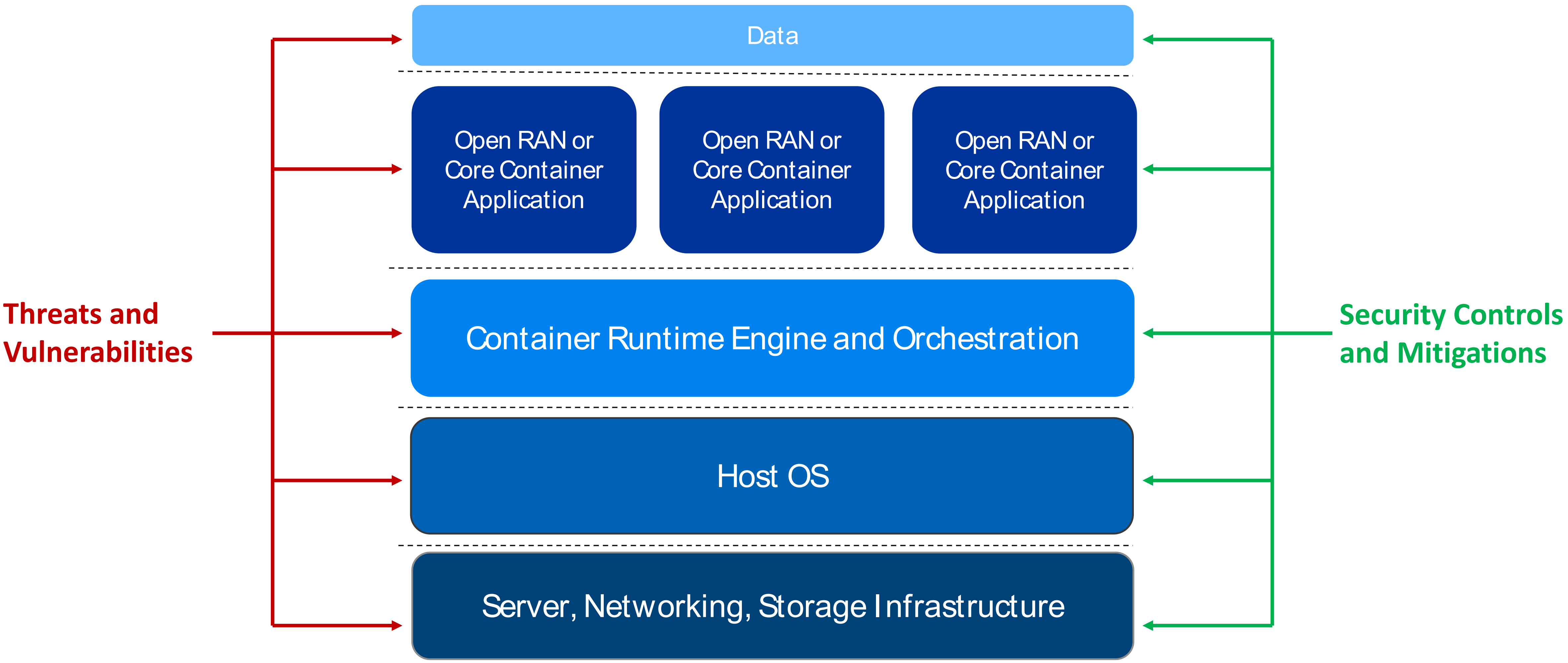
Open RAN Security Posture



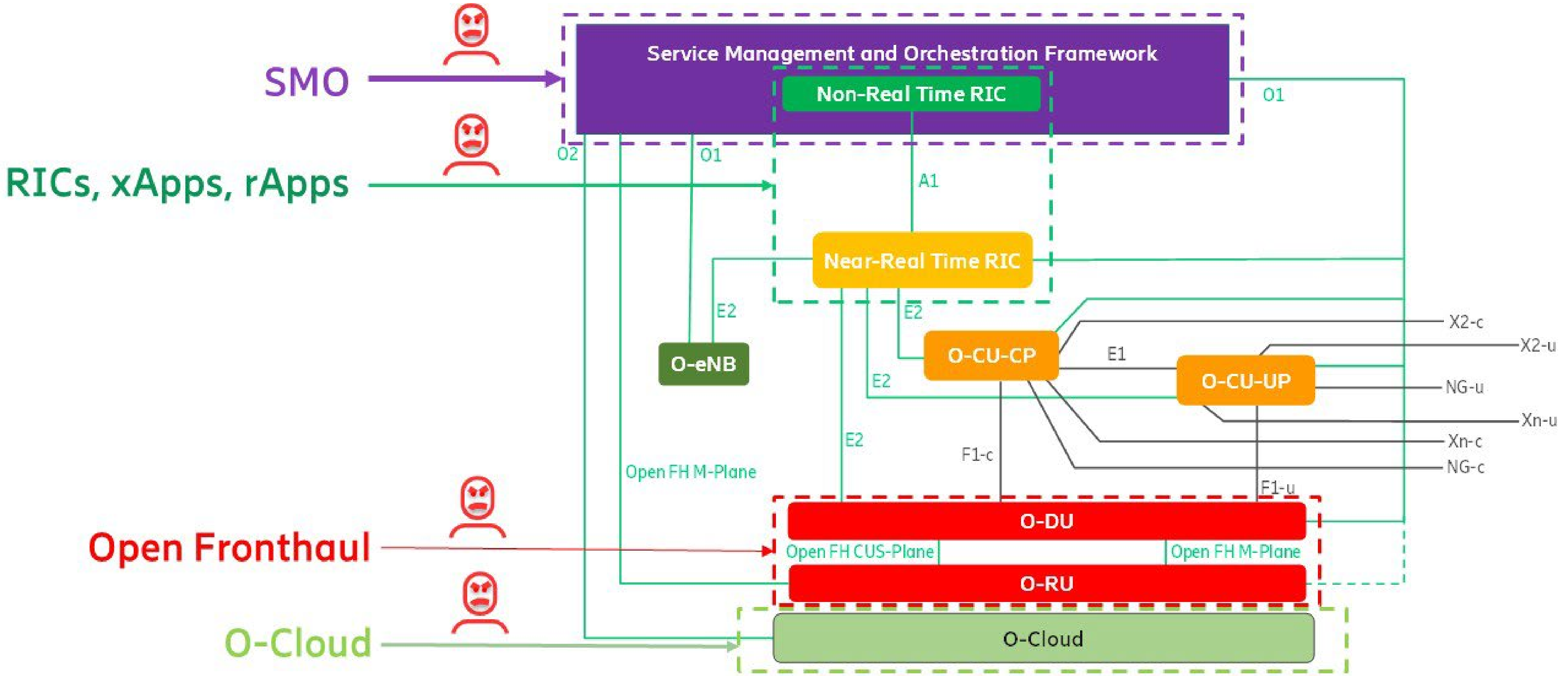
Security Advantages[1]	Security Risks
Open source software enables transparency and common control	Open source software can be exploited by malicious threat actors
Open interfaces ensure transparency, use of standard protocols, and interoperability of secure protocols	O-RAN's new open interfaces must be built on a foundation of security specifications.
Disaggregation enables supply chain security through diversity	Disaggregation expands the attack surface by adding new functions and interfaces while also introducing supply chain risks.
AI/ML enables visibility and intelligence to achieve greater security	AI/ML is known threat vector across society and must be protected in O-RAN deployments

[1] **O-RAN Alliance paper,** "O-RAN Minimum Viable Plan and Acceleration towards Commercialization", July 2021.

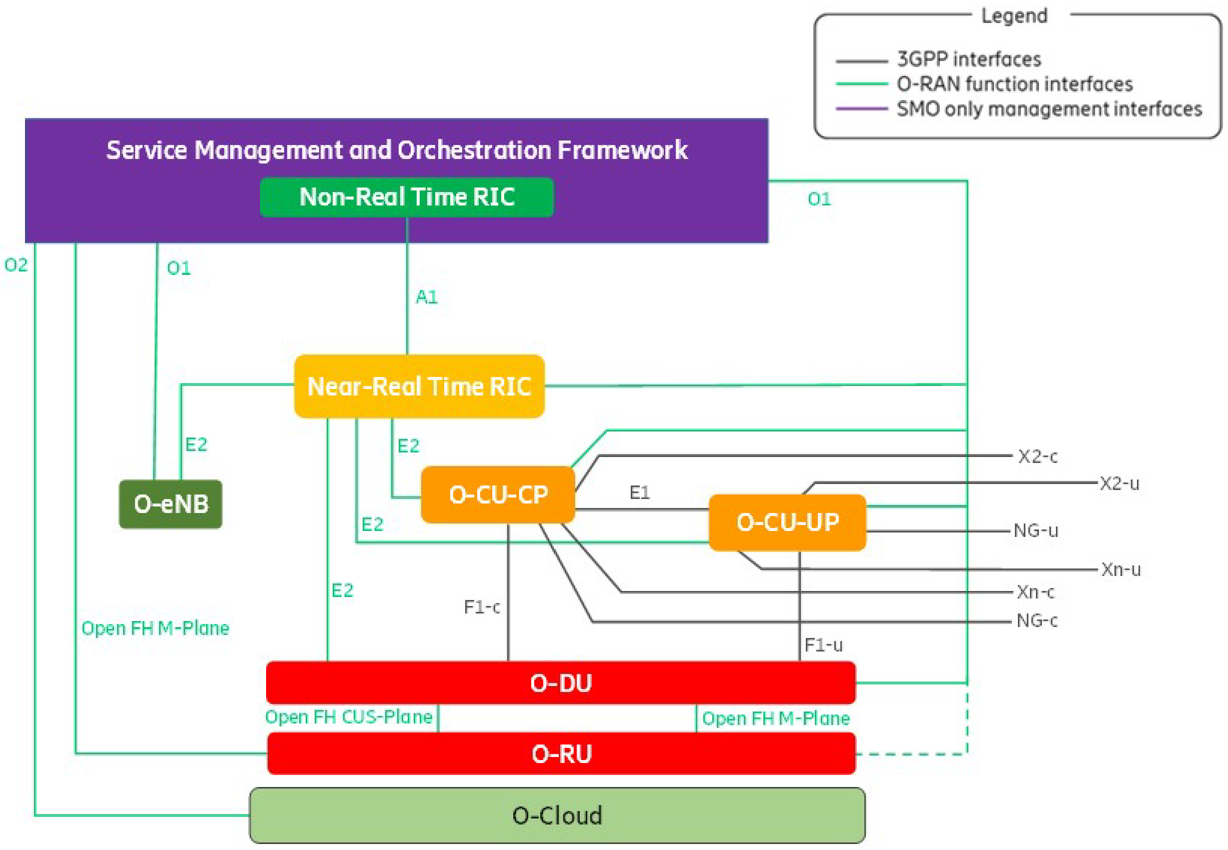
Security Risks and Controls for 5G Critical Infrastructure in the Cloud


Threats and Vulnerabilities
Data
Open RAN or Core Container Application
Open RAN or Core Container Application
Open RAN or Core Container Application
Container Runtime Engine and Orchestration
Host OS
Server, Networking, Storage Infrastructure
Security Controls and Mitigations

O-RAN's Attack Surface



Acknowledgements of O-RAN's Expanded Attack Surface



[source: O-RAN Alliance]

See also: https://www.ericsson.com/4a4b77/assets/local/security/security-considerations-open-ran.pdf, cited in FCC NoI on Open RAN, 2021.

O-RAN Alliance

June 2021

*"The O-RAN Architecture includes new interfaces and functions, **expanding the threat surface** to introduce new security risks. "*

Germany BSI

November 2021

*"medium to **high security risks** can be identified in numerous interfaces and components specified in the context of O-RAN"*

EU NIS Cooperation Grou

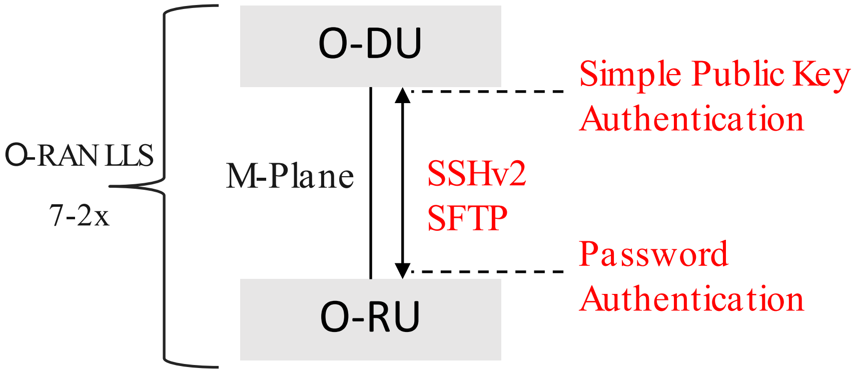
May 2022

*"An **expanded threat surface** and a more complex environment leading to higher risks of vulnerability or failure"*

See also: https://www.ericsson.com/4a4b77/assets/local/security/security-considerations-open-ran.pdf, cited in FCC NoI on Open RAN, 2021.

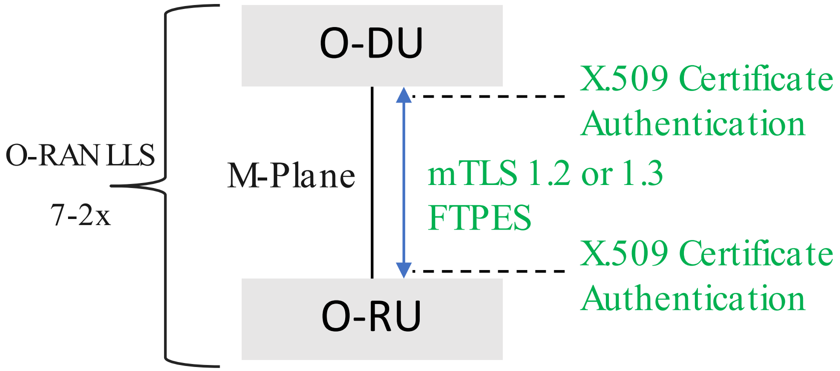
Secure Authentication for O-RAN's M-Plane

SSHv2 with Passwordbased Authentication



- Weak Security
- Does not meet industry best practice
- Violates USG guidance

mTLSwith Certificate-based Authentication

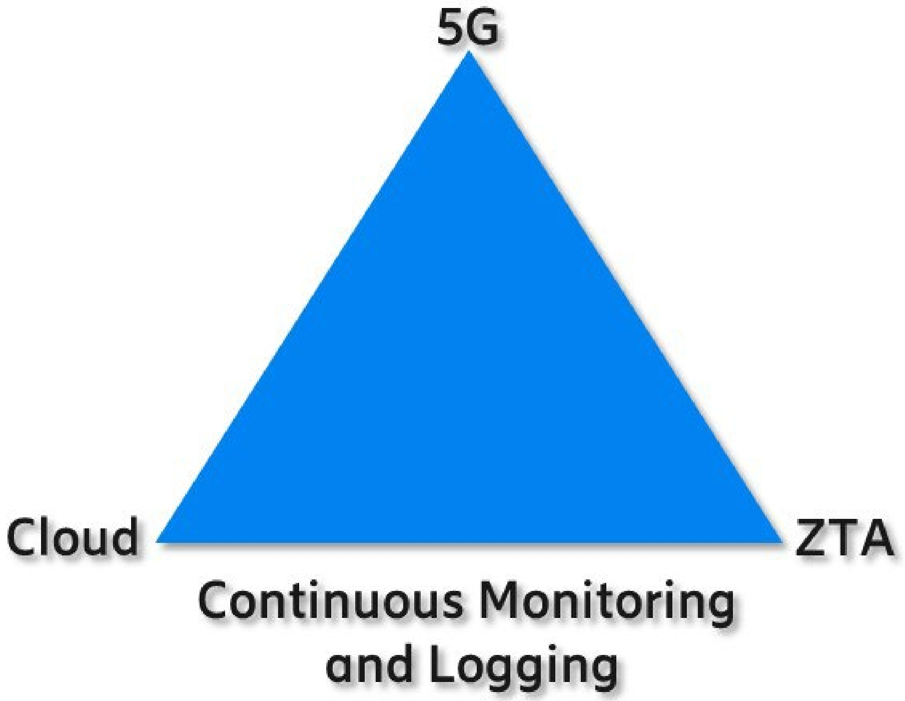

O-DU
O-RAN LLS
7-2x
M-Plane
mTLS 1.2 or 1.3
FTPES
X.509 Certificate Authentication
X.509 Certificate Authentication
O-RU

- Strong Security
- Meets industry best practice
- Aligns with USG Guidance

Both are mandatory for vendors to implement and optional for operators to use

Zero Trust Architecture in Open RAN

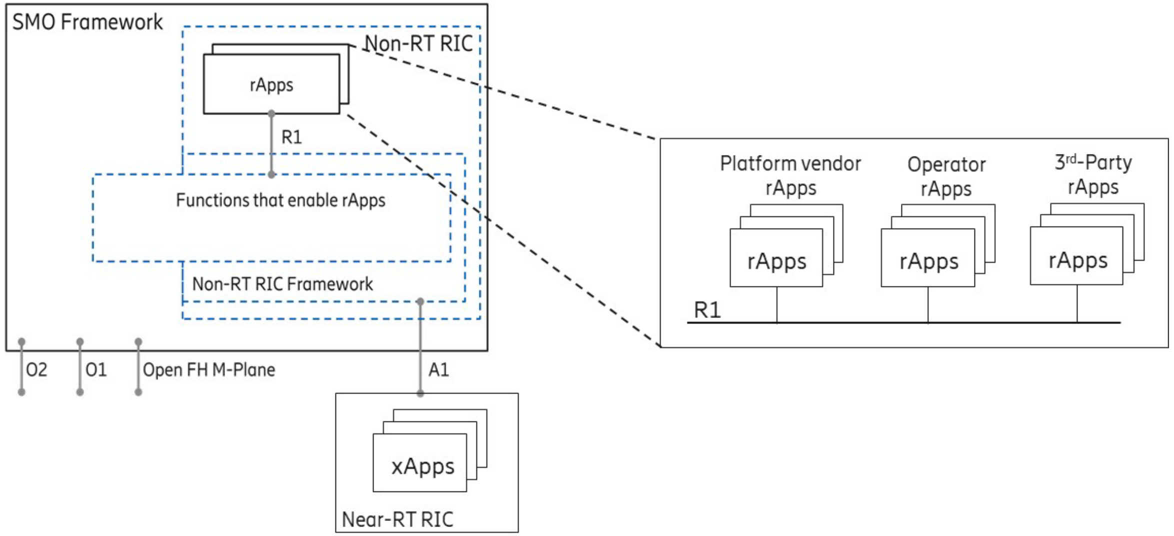
“Strive to bring a **Zero Trust** mindset into 5G cloud” – US DHS CISA



- ZTA definition
  - There is no implicit trust granted to an asset based upon ownership, physical location, or network location (NIST)
  - Assume the adversary is already inside the network (CISA)
- ZTA changes how we think about securing RAN from external and internal threats
- Likelihood scoring is influenced by the pursuit of a ZTA
- Mitigations are applied for confidentiality, integrity, availability, and authenticity protections for Open RAN functions, interfaces, and data
- O-RAN Alliance is pursuing a Zero Trust Architecture (ZTA) in accordance with NIST SP 800-207

SMO Enhances Open RAN Security

SMO = Service Management and Orchestration



- SMO is responsible for Open RAN domain management, optimization and orchestration.
- SMO plays an important role in the Open RAN security posture.
- SMO supports a ZTA for 5G cloud deployments
- SMO has network-wide visibility from internal and external data sources
- rApps can be purpose-built to provide RAN protecting security functions.
- A secure, standardized R1 interface enables any rApp to work with other rApps to form complex security decisions.

Recommendations to Secure Open RAN

Consider the following recommendations for securing Open RAN deployments:

1. Protect O-RAN's expanded attack surface due to more interfaces and functions
2. Ensure interfaces are secured according to industry best practices such as mTLS with PKI X.509 certificates, CMPv2, and OAuth 2.0
3. Pursue a Zero Trust Architecture aligned w/ NIST SP 800-207 and CISA guidance
4. Practice due diligence in the cloud and implement cloud security best practices
5. Leverage the SMO to enhance the Open RAN security posture

Creating Infinite Possibilities.

Thank You!

Scott Poretsky

Director of Security, North America
Ericsson
508.261.4429
scott.poretsky@ericsson.com