 O-RAN.WG11.SharedORU-Security-Analysis-TR.0-R004-v06.00

Technical Report

O-RAN Work Group 11 (Security Work Group)

Study on Security

for Shared O-RU (SharedORU)

Copyright © 2024 by the O-RAN ALLIANCE e.V. Register of Associations, Bonn VR 11238, VAT ID DE321720189.

The copying or incorporation into any other work of part or all of the material available in this document in any form without the prior written permission of O-RAN ALLIANCE e.V. is prohibited, save that you may print or download extracts of the material of this document for your personal use, or copy the material of this document for the purpose of sending to individual third parties for their information provided that you acknowledge O-RAN ALLIANCE as the source of the material and that you inform the third party that these conditions apply to them and that they must comply with them.

O-RAN ALLIANCE e.V., Buschkauler Weg 27, 53347 Alfter, Germany

Contents

1 Scope 3

2 References 5

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Shared O-RU Assets 8

4.1 Architecture 8

4.2 Functions 9

4.3 Interfaces 11

4.4 Information 12

5 Threats 14

5.1 Threat Model 14

5.2 Threat Template 14

5.3 Potential Threats and Exploits 15

5.4 Shared O-RU Threats 15

6 Threat Analysis 17

6.1 Lateral Movement Between Network Functions 19

6.2 User Access Threats 22

6.3 Data Access Threats 24

6.4 Availability Threats 26

6.5 Configuration Threats 28

6.6 Neutral Host Controller (NHC) Threats 30

6.7 Resiliency Threats 32

7 Security Controls 33

8 Risk Assessment 35

8.1 Lateral Movement Between Network Functions 35

8.2 User Access Threats 36

8.3 Data Access Threats 37

8.4 Availability Threats 37

8.5 Configuration Threats 38

8.6 Neutral Host Controller Threats 39

8.7 Resiliency Threats 39

9 Primary Security Issues 41

10 Recommendations 42

Annex A: Shared O-RU All-in-One Architecture 45

Annex change history 47

# Scope

This technical report provides the threat model and risk assessment for the Shared O-RU. The report identifies threats and risks and recommends potential security controls to protect against those threats through safeguards or mitigation.

The steps of the threat modelling process are as follows:

1. Identify assets: Identify the assets of the Shared O-RU that must be protected.
2. Identify threats: Identify the threats that could adversely impact the Shared O-RU and threats that can use the Shared O-RU to adversely impact other components of the O-RAN system.
3. Identify the attack surface and attack vectors: Identify the points in the Shared O-RU where an attacker could
   1. gain entry to a O-RU Host or O-RU Tenant (SRO) of a Shared O-RU
   2. gain entry to another O-RAN component through the Shared O-RU
   3. exploit a vulnerability or misconfiguration at the Shared O-RU
   4. compromise the Shared O-RU to degrade performance or impact availability
   5. expose data at rest / data in use at the Shared O-RU
   6. expose data in motion between the Shared O-RU and other O-RAN network functions
4. Measure risk: The extent to which confidentiality, integrity, or availability is threatened, based upon a risk-based analysis considering the impact level resulting from an attack and the likelihood of occurrence.
5. Recommend controls: The management, operational, and technical controls for an information system to protect the confidentiality, integrity and availability of the Shared O-RU and its information.

The sections in this Shared O-RU Security Analysis Technical Report (TR) follow the process described above.

This Technical Report makes the following considerations:

* The attack surface of the Shared O-RU includes assets that are interfaces, functions, and data.
  + Data-at-rest, Data-in-motion, and Data-in-use must be considered.
  + O-RAN Alliance WG4 is in the process of defining optional architectures for Shared O-RU. This will influence the set of assets to be protected.
* The O-RAN Alliance is pursuing a zero-trust architecture (ZTA) for its specifications based upon NIST SP 800-207 [i.8]. This will affect the risk scoring as external and internal threats are considered.
* Security controls will be recommended for specifications of the Shared O-RU. The recommended controls provided in this report will be shared with the responsible O-RAN Alliance working group, such as WG1 and WG4, so that the appropriate specification relevant to the recommendation can be updated.
* Some of the identified Shared O-RU assets may already be in scope for of other ongoing WG11 security work items. The Shared O-RU Security Analysis Technical Report work item may inform those work items.

# References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[i.1] O-RAN ALLIANCE PD: "O-RAN Document Drafting Rules (ODR)".

[i.2] O-RAN ALLIANCE TS: "O-RAN Architecture Description (OAD)".

[i.3] MVPC-FP-Shared-O-RU-Feature-Plan-v05.00, Shared O-RU Feature Plan

[i.4] O-RAN ALLIANCE TS: "O-RAN Security Protocols Specifications".

[i.5] O-RAN ALLIANCE TS: "O-RAN Security Requirements and Controls Specifications".

[i.6] O-RAN ALLIANCE TR: "O-RAN Threat Modelling and Risk Assessment".

[i.7] O-RAN ALLIANCE TS: "O-RAN Security Test Specifications".

[i.8] Zero Trust Architecture, NIST SP 800-207, NIST, August 2020, <https://csrc.nist.gov/publications/detail/sp/800-207/final>.

[i.9] US National Security Agency (NSA) / Cybersecurity and Infrastructure Security Agency (CISA), Security Guidance for 5G Cloud Infrastructures, Part I, Oct 28, 2021, Part II, Nov 18, 2021, Part III, Dec 2, 2021, Part IV, Dec 16, 2021. <https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/smdpage11747/2/> (as of Feb 28, 2022).

[i.10] ISO/IEC 27001:2013 Information Security Management System (ISMS).

[i.11] VOID

[i.12] OWASP Top 10 Web Application Security Risks, 2021, <https://owasp.org/www-project-top-ten/>.

[i.13] Cloud Security Alliance (CSA), Top Threats to Cloud Computing: Egregious Eleven, 2019, https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven.

[i.14] Cloud Security Alliance (CSA), Top Threats to Cloud Computing: Pandemic Eleven, 2022, https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven.

[i.15] OWASP Top 10 Proactive Controls, 2021, <https://owasp.org/projects/spotlight/historical/2021.02.10/>

[i.16] Center for Internet Security (CIS) Critical Security Controls, https://www.cisecurity.org/controls/cis-controls-list

[i.17] Cloud Security Alliance (CSA) Cloud Control Matrix (CCM), https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[i.18] ISO/IEC 27001:2013 Information Security Management System (ISMS).

[i.19] NIST SP 800-53r5, Security and Privacy Controls for Information Systems and Organizations, 2020.

[i.20] O-RAN ALLIANCE TS: "Management Plane Specification".

[i.21] NIST SP 800-57 Part 1 Rev. 5, Recommendation for Key Management, 2020

[i.22] IETF RFC 6066: “Transport Layer Security (TLS) Extensions: Extension Definitions”

[i.23] IETF RFC 8446: “The Transport Layer Security (TLS) Protocol Version 1.3”

# Definitions of terms, symbols and abbreviations

For the purposes of the present document, the following terms and definitions apply:

## Terms

This document uses the verbal forms for the expression of provisions as defined in O-RAN Document Drafting Rules (ODR)[i.1].

This document uses the term Zero Trust Architecture (ZTA) as defined by US NIST in [i.8] and applied to 5G cloud deployments by US CISA in [i.9]. A ZTA provides protection from external and internal threats, assuming the following:

1. there is no implicit trust granted to an asset based upon ownership, physical location, or network location [i.8].
2. the adversary is already inside the network. Perimeter defenses are no longer sufficient to secure a network, and there should always be an assumption that a threat actor has established a foothold in the network [i.9].

This document uses the term “attack surface” defined by US NIST as

*The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.* [https://csrc.nist.gov/glossary/term/attack\_surface]

This document refers to “sensitive information” defined by US NIST as

*information whose loss, misuse, or unauthorized access or modification could adversely affect security.* [https://csrc.nist.gov/glossary/term/sensitive]

**Trust Anchor (TA)** (as per [i.21], section 2.1)**:**

1. An authoritative entity for which trust is assumed. In a PKI, a trust anchor is a certification authority, which is represented by a certificate that is used to verify the signature on a certificate issued by that trust-anchor. The security of the validation process depends upon the authenticity and integrity of the trust anchor’s certificate. Trust anchor certificates are often distributed as self-signed certificates.
2. The self-signed public key certificate of a trusted CA.

## Symbols

None

## Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 and the following apply:

AI Artificial Intelligence

DAR Data at Rest

DIM Data in Motion

DIU Data in Use

gNB gNodeB (applies to NR)

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

ML Machine Learning

MNO Mobile Network Operator

NF Network Function

NHC Neutral Host Controller

O-CU Open-Centralized Unit

O-DU Open-Distributed Unit

O-RU Open-Radio Unit

OFH Open Fronthaul

PII Personally Identifiable Information

PKI Public Key Infrastructure

SMOService Management and Orchestration

SOH Shared Operator Host

SRO Shared Resource Operator

TLS Transport Layer Security

ZTA Zero Trust Architecture

# Shared O-RU Assets

## Architecture

The potential benefits of Shared O-RU are RAN Sharing, Neutral Host, high RAN reliability (redundancy) and RAN processing pooling. Shared O-RU involves cooperation with the SMO, O-CU, O-DU, and O-RU network. Securing the Shared O-RU is imperative to protect the O-RAN deployment and each of its tenants. Five optional configurations are being considered for Shared O-RU [i.3] and while there are common security risks, each configuration may also introduce unique security risks. The Attack Surface of the Shared O-RU includes assets groups Functions, Interfaces, and Information, which each have assets that should be protected. The assets that should be protected are listed in the following sections.

Figure 4.1-1 shows the Shared O-RU building blocks and protocol stack.

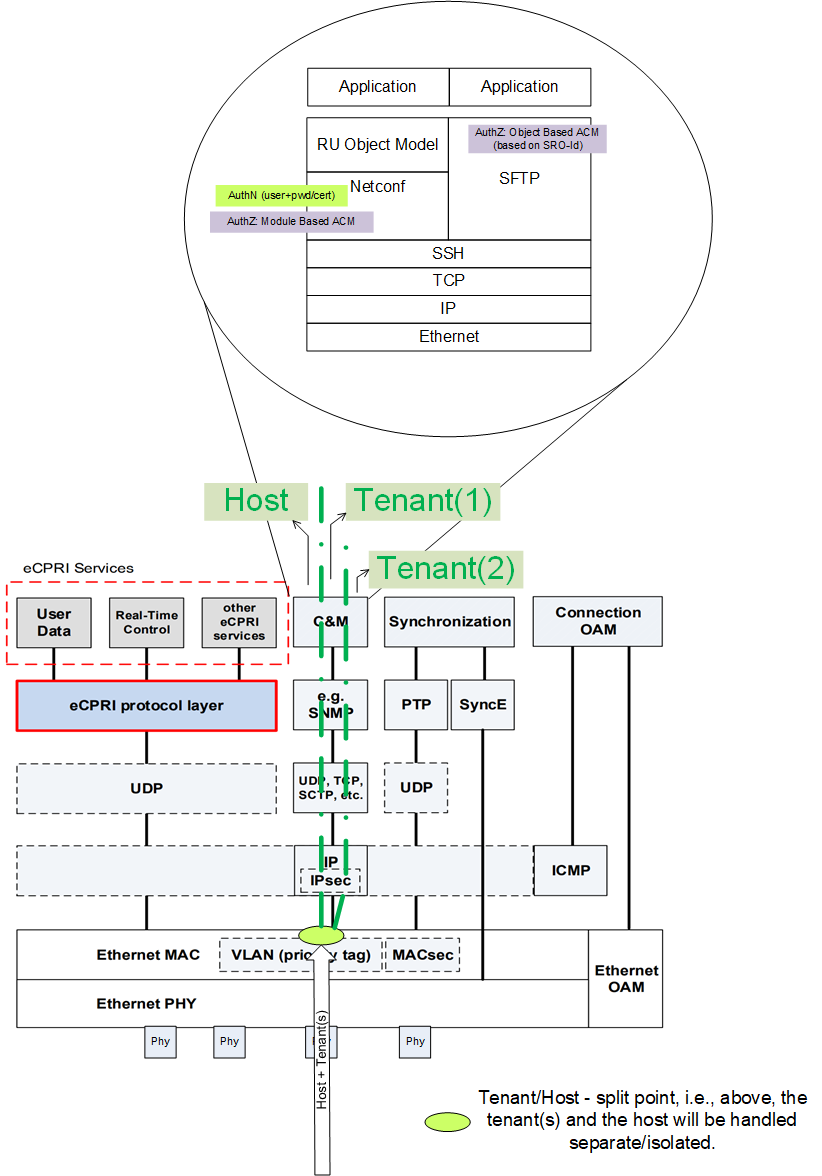


Figure 4.1-1: Shared O-RU Tenant/Host Split

The following points are considered:

* The Shared O-RU can be receiving data via a single/shared physical port. This connectivity is used to transfer tenant and host-specific controller functionality.
* The tenant/host-split point is the earliest point in the protocol stack when host and tenants are going to be separated/isolated.
* Each of the tenants can obtain access (i.e., read/write) to its own resources, and a tenant has no means to access neighbor resources.
* The host can obtain access (i.e., read/write) to common M-plane resources.
* The user will be authenticated by using username and password/certificate and in case of netconf/ssh by using public/private key. In successful case the user is obtaining authorization on Module Level. Access control management (ACM) functionality required on that protocol level.
* Every tenant who is requesting access to ‘own’= tenant specific resources, needs to be identified using its unique SRO-Id, and after successful authentication, the tenant will be authorized to access its own resources.

## Functions

The following functions should be considered in the Shared O-RU risk analysis:

* ASSET-C-31: Shared O-RU
* ASSET-C-32: O-RU Host (Shared Operator Host)
* ASSET-C-33: O-RU Tenant (Shared Resource Operator)
* ASSET-C-34: O-DU Host (Shared Operator Host)
* ASSET-C-35: O-DU Tenant (Shared Resource Operator)
* ASSET-C-36: O-CU Host (Shared Operator Host), includes O-CU-CP and O-CU-CP software
* ASSET-C-37: O-CU Tenant (Shared Resource Operator), includes O-CU-CP and O-CU-CP software
* ASSET-C-38: SMO Host (Shared Operator Host)
* ASSET-C-39: SMO Tenant (Shared Resource Operator)
* Neutral Host Controller (NHC)

NOTE: NHC is not an agreed upon function in the O-RAN architecture, but NHC is considered in scope for security analysis.

Figures 4.2-1, 4.2-2, and 4.2-3 below show these assets in Shared O-RU architecture.



Figure 4.2-1 Security Architecture for Shared O-RU Options 1 and 2



Figure 4.2-2 Security Architecture for Shared O-RU Options 3 and 4



Figure 4.2-3 Security Architecture for Shared O-RU Options 5

NOTE: NHC is not an agreed upon function in the O-RAN architecture



Figure 4.2-4 Security Architectures for Shared O-RU Resiliency

## Interfaces

The following interfaces, as shown in Figures 4.2-1, 4.2-2, and 4.2-3, are considered in this phase of the Shared O-RU security analysis:

* ASSET-C-22: O1
* ASSET-C-24: OFH M-Plane: OAM Config and Carrier Config

New interfaces for Shared O-RU currently in specifications development will be considered in a later phase of the security analysis. This includes Fast Dynamic Scheduling between Host and Tenant O-DUs and Slow Dynamic Scheduling between Host and Tenant SMOs.

## Information

The following Shared O-RU information and data should be considered in a risk analysis:

* O1 Data
  + ASSET-D-03: O1 Critical management plane data
  + ASSET-D-09: O1 Informational data
* M-Plane Data
  + ASSET-D-02: Critical Management Plane Data
  + ASSET-D-18: O-RAN network function configuration data
  + ASSET-D-24: Netconf Data Stores
  + ASSET-D-25: O-RAN Analog Training or Test Data
* Secret Stores
  + ASSET-D-16: X.509 certificates
  + ASSET-D-17: Private keys
  + ASSET-D-19: Cryptographic Keys (such as session keys for, e.g., IPsec, MACsec, …)
  + ASSET-D-20: Administrator credentials (passwords and tokens)
  + ASSET-D-32: Cryptographic keys used during secure boot, for encryption/decryption, etc.
* Service Account Management Data
  + ASSET-D-yy-new1: Credentials (Services)
* User Account Management Data
  + ASSET-D-20: Credentials (Administrators)
* PII
  + ASSET-D-30: O-RAN specific UE IDs
  + ASSET-D-yy-new3: Sensitive Information (e.g., public IP address, …)
* Event logs
  + ASSET-D-29: Security Event Log Files
* Trusted Environment
  + ASSET-D-yy-new2: Trusted Environment
* CUS-plane Data
  + ASSET-D-04: Open Fronthaul Control-plane (C-Plane) data
  + ASSET-D-05: Open Fronthaul User-plane (U-Plane) data
  + ASSET-D-01: Open Fronthaul Synchronization-plane (S-Plane) data

Asset identifier with a number indicates that the asset has been identified in the O-RAN Threat Modelling and Risk Assessment document [i.6]. Inclusion of an asset identifier ASSET-X-yy-new indicates the asset has not yet been added to [i.6].

# Threats

## Threat Model

The STRIDE model is used to classify threats:

1. S - Spoofing identity. An application or program can masquerade as another to gain advantages not typically allowed for that program.
2. T - Tampering with data. This involves the malicious modification of data, including making unauthorized changes to a database and alteration of data as it flows between computers.
3. R - Repudiation. A user or program refuses the authenticity of a good or reasonable command or action.
4. I - Information disclosure. This involves the exposure of information to individuals with unauthorized access to it. For example, users gain the ability to read a file that they normally would not have been granted access to, or an intruder can read data in transit between computers.
5. D - Denial of service. These attacks deny service to valid users, such as making a website unavailable or unusable by flooding it with illegitimate requests to keep legitimate users without access.
6. E - Elevation of privileges. An unauthorized user gains privileged rights to access previously no granted to compromise or destroy the system, such as a change in membership.

|  |  |
| --- | --- |
| **Threat types** | **Impact types** |
| Spoofing | Authenticity |
| Tampering | Integrity |
| Repudiation | Non-repudiation |
| Information disclosure | Confidentiality |
| Denial of Service | Availability |
| Elevation of Privilege | Authorization |

## Threat Template

Template to present the threat characteristics:

|  |  |
| --- | --- |
| **Threat ID** |  |
| **Threat title** |  |
| **Threat description** |  |
| **Threat type** | Spoofing  Tampering  Repudiation  Information disclosure  Denial of Service  Elevation of Privilege |
| **Vulnerabilities** |  |
| **Impact type** | Authenticity  Integrity  Non-repudiation  Confidentiality  Availability  Authorization |
| **Affected Assets** |  |

## Potential Threats and Exploits

A threat analysis is facilitated by an understanding of potential threats, as identified by the Cloud Security Alliance (CSA) and the Open Web Application Security Project (OWASP).

The OWASP Top 10 Web Application Security Risks [i.12] was updated in 2021 to include the following:

A01:2021 Broken Access Control

A02:2021 Cryptographic Failure

A03:2021 Injection (including Cross-Site Scripting)

A04:2021 Insecure Design

A05:2021 Security Misconfiguration

A06:2021 Vulnerable and Outdated Components

A07:2021 Identification and Authentication Failures

A08:2021 Software and Data Integrity Failures (including Insecure Deserialization)

A09:2021 Security Logging and Monitoring Failures

A10:2021 Server-Side Request Forgery

The CSA Top Threats to Cloud in 2019 was labelled the “Egregious Eleven” [i.13], as listed below:

1. Data Breaches
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access, and Key Management
5. Account Hijacking
6. Insider Threat
7. Insecure Interfaces and APIs
8. Weak Control plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Uses of Cloud Services

The CSA updated its list of top threats to cloud in 2022 and renamed it the “Pandemic Eleven” [i.14], as listed below:

1. Insufficient Identity, Credential, Access and Key Management, Privileged Accounts

2. Insecure Interfaces and APIs

3. Misconfiguration and Inadequate Change Control

4. Lack of Cloud Security Architecture and Strategy

5. Insecure Software Development

6. Unsecure Third-Party Resources

7. System Vulnerabilities

8. Accidental Cloud Data Disclosure

9. Misconfiguration and Exploitation of Serverless and Container Workloads

10. Organized Crime, Hackers & APT

11. Cloud Storage Data Exfiltration

## Shared O-RU Threats

The security risks associated with the Shared O-RU are due to:

1. resource sharing in a multi-tenant environment

2. interworking between host and tenant network functions

3. interfaces between Shared O-RU and other O-RAN functions

The Shared O-RU threat analysis considers the threats listed in clause 5.3 that are relevant to O-RAN and Shared O-RU. The following threats to Shared O-RU have been identified and will be analyzed in clause 6 – Threat Analysis.

Threats due to Multi-Tenancy

* O-DU Host access to O-DU Tenant through Shared O-RU
* O-DU Tenant access to O-DU Host through Shared O-RU
* SMO Host access to SMO Tenant
* SMO Tenant access to SMO Host

Threats at Shared O-RU functions

* Parameter conflicts at Shared O-RU
* Privilege levels for authorization to data and processes in O-RU, O-DU, and SMO
* Escalation of privilege at NHC

Threats to Shared O-RU interfaces

* Untrusted peering between Shared O-RU and O-DU
* Insecure APIs
* Message flooding
* Unprotected data in transit

# Threat Analysis

Threat Analysis tables are provided for each of the identified Shared O-RU threats in the subsections below. The Shared O-RU Threats are classified into the following 7 threat groups:

* Lateral Movement Between Network Functions
* User Access Threats
* Data Access Threats
* Availability Threats
* Configuration Threats
* Neutral Host Controller Threats
* Resiliency

Table 6-1 summarizes the identified threats for each of the Shared O-RU threat groups. The threat analysis considers a zero trust architecture (ZTA) for which (i) micro-perimeters are established for each asset and (ii) there is no implicit trust granted to assets or users [i.8]. Shared O-RU assets, as discussed in the Functions, Interfaces, and Information asset groups in clause 4- Assets, are considered for the threat analysis. The threat analysis was performed on the five architectural options being considered for deployment of Shared O-RU [i.3], which allow use of M-Plane Hybrid or Hierarchical mode and optional use of a Neutral Host Controller (NHC).

Table 6-1 summarizes the identified threats for each of the Shared O-RU threat groups. This may not be an exhaustive list and may be expanded in future versions of this Technical Report.

Use of the term “MNO Tenant” or “Tenant” refers to a “Shared Resource Operator (SRO)” as defined in O-RAN ALLIANCE TS: "Management Plane Specification.[i.20].

Table 6-1 Shared O-RU Threats

|  |  |
| --- | --- |
| **Threat-Id** | **Threat Description (Brief)** |
| **Lateral Movement Between Network Functions** | |
| T-SharedORU-01 | O-DU Tenant accesses O-DU Host |
| T-SharedORU-02 | O-DU Host accesses O-DU Tenant |
| T-SharedORU-03 | O-DU Tenant accesses O-DU Tenant |
| T-SharedORU-04 | Password Attack on OFH M-Plane |
| T-SharedORU-05 | Untrusted peering to O-DU |
| T-SharedORU-06 | Untrusted peering to the Shared O-RU |
| T-SharedORU-07 | Untrusted peering to the SMO |
| T-SharedORU-08 | SMO Tenant accesses SMO Host |
| T-SharedORU-09 | SMO Host accesses SMO Tenant |
| T-SharedORU-10 | O-DU Host accesses O-CU Tenant |
| T-SharedORU-11 | O-DU Tenant accesses O-CU Host |
| T-SharedORU-12 | O-DU Tenant accesses O-CU Tenant |
| T-SharedORU-13 | SMO Host accesses O-CU Tenant |
| T-SharedORU-14 | SMO Tenant accesses O-CU Host |
| **User Access Threats** | |
| T-SharedORU-15 | Physical port access to Shared O-RU Host/Tenant |
| T-SharedORU-16 | Physical port access to O-DU Host/Tenant |
| T-SharedORU-17 | Physical port access to O-CU Host/Tenant |
| T-SharedORU-18 | Malicious User Login Attempt to SMO Host/Tenant |
| T-SharedORU-19 | Malicious User Login Attempt to O-CU Host/Tenant |
| T-SharedORU-20 | Malicious User Login Attempt to O-DU Host/Tenant |
| T-SharedORU-21 | Malicious User Login Attempt to Shared O-RU Host/Tenant |
| **Data Access Threats** | |
| T-SharedORU-22 | Unauthorized internal threat actor gains access to data in Shared O-RU |
| T-SharedORU-23 | Unauthorized external threat actor gains access to data in Shared O-RU |
| T-SharedORU-24 | Exposure of data at rest at Shared O-RU |
| T-SharedORU-25 | Exposure of Shared O-RU data at rest at SMO |
| T-SharedORU-26 | Exposure of Shared O-RU data at rest at O-DU |
| T-SharedORU-27 | Exposed data in transit between Shared O-RU and O-DU Host/Tenant |
| T-SharedORU-28 | Exposed data in transit between Shared O-RU and SMO Host/Tenant |
| T-SharedORU-43 | Eavesdropping of unprotected CUSM-plane data within shared O-RU |
| **Availability Threats** | |
| T-SharedORU-29 | Modify/Delete OFH C-Plane messages |
| T-SharedORU-30 | Clock hijacking on OFH S-Plane |
| T-SharedORU-31 | Parameter conflicts at Shared O-RU |
| T-SharedORU-32 | Volumetric DDoS attack from O-DU targeting Shared O-RU |
| T-SharedORU-33 | Volumetric DDoS attack from SMO targeting Shared O-RU |
| T-SharedORU-34 | Volumetric DDoS attack targeting O-DU |
| T-SharedORU-35 | Shared O-RU initialization hijacking by DHCP compromise |
| T-SharedORU-36 | Shared O-RU M-plane hijacking by DNS compromise |
| **Configuration Threats** | |
| T-SharedORU-37 | Misconfiguration of MNO Host Role |
| T-SharedORU-38 | Incorrect Assignment of Spectrum Resources |
| T-SharedORU-39 | Chain of Trust in a Multi-Tenant Environment |
| T-SharedORU-40 | Hijack of MNO Host Role |
| T-SharedORU-41 | Inability of SMO to Revoke Host Privileges from a Malicious Tenant |
| T-SharedORU-42 | Misuse of “sudo” privileges |
| T-SharedORU-55 | Set Incorrect Array-Carrier configuration on O-DU (Standby) |
| T-SharedORU-56 | Modify Array-Carrier pre-configuration on Shared O-RU |
| T-SharedORU-57 | Modify/Inject M-Plane messages with Array-Carrier configuration |
| **Neutral Host Controller Threats** | |
| T-SharedORU-44 | SMO peers with untrusted NHC |
| T-SharedORU-45 | Shared O-RU peers with untrusted NHC |
| T-SharedORU-46 | NHC peers with untrusted entities |
| T-SharedORU-47 | Malicious actor at the NHC can access information on the SMO |
| T-SharedORU-48 | Malicious actor at the NHC can access information on the Shared O-RU |
| T-SharedORU-49 | NHC is source of DDoS attack on SMO |
| T-SharedORU-50 | NHC is source of DDoS attack on Shared O-RU |
| T-SharedORU-51 | Shared O-RU data exposure at NHC |
| **Resiliency Threats** | |
| T-SharedORU-52 | Thrashing O-DU Failovers |
| T-SharedORU-53 | Dual (Dueling) Active O-DUs |
| T-SharedORU-54 | Modify/Inject O1 messages at the SMO |

## Lateral Movement Between Network Functions

This section provides threat analysis tables for threats to access between Shared O-RU network functions.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-01 |
| **Threat title** | O-DU Tenant accesses O-DU Host |
| **Threat description** | The O-DU Tenant accesses the O-DU Host through the Shared O-RU. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Host |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-02 |
| **Threat title** | O-DU Host accesses O-DU Tenant |
| **Threat description** | The O-DU Host accesses the O-DU Tenant through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-03 |
| **Threat title** | O-DU Tenant accesses O-DU Tenant |
| **Threat description** | An O-DU Tenant accesses another O-DU Tenant through the Shared O-RU supporting multiple tenants. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-04 |
| **Threat title** | Password Attack on OFH M-Plane |
| **Threat description** | Use of single-factor authentication with password on the Open Fronthaul M-Plane can be exploited by an internal malicious actor to gain access to the Shared O-RU. The attack can be a brute-force attack or stolen password. There is increased risk of password attack in a multi-tenant environment. The internal malicious actor may be the MNO Host, a MNO Tenant (SRO), or a 3rd-party. [i.9] |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | Shared O-RU, O-DU Host, O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-05 |
| **Threat title** | Untrusted peering to O-DU |
| **Threat description** | Attacker exploits weak authentication on the O-DU to establish a session with a malicious app masquerading as a Shared O-RU. From the O-DU, a malicious actor can move laterally across Shared O-RUs and northbound to the O-CU and SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Host, O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-06 |
| **Threat title** | Untrusted peering to the Shared O-RU |
| **Threat description** | Attacker exploits weak authentication on the Shared O-RU to establish session with a malicious app masquerading as a O-DU Host or O-DU Tenant |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-07 |
| **Threat title** | Untrusted peering to the SMO |
| **Threat description** | Attacker exploits weak authentication on the SMO to establish session with a malicious app masquerading as a Shared O-RU. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-08 |
| **Threat title** | SMO Tenant accesses SMO Host |
| **Threat description** | The SMO Tenant accesses the SMO Host through the Shared O-RU. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO Host |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-09 |
| **Threat title** | SMO Host accesses SMO Tenant |
| **Threat description** | The SMO Host accesses the SMO Tenant through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-10 |
| **Threat title** | O-DU Host accesses O-CU Tenant |
| **Threat description** | The O-DU Host accesses the O-CU Tenant through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-11 |
| **Threat title** | O-DU Tenant accesses O-CU Host |
| **Threat description** | The O-DU Tenant accesses the O-CU Host through the Shared O-RU. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Host |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-12 |
| **Threat title** | O-DU Tenant accesses O-CU Tenant |
| **Threat description** | The O-DU Tenant accesses another O-CU Tenant through the Shared O-RU supporting multiple tenants. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-13 |
| **Threat title** | SMO Host accesses O-CU Tenant |
| **Threat description** | The SMO Host accesses the O-CU Tenant through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-14 |
| **Threat title** | SMO Tenant accesses O-CU Host |
| **Threat description** | The SMO Tenant accesses the O-CU Host through the Shared O-RU. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Host |

## User Access Threats

This section provides threat analysis tables for user access threats to Shared O-RU.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-15 |
| **Threat title** | Physical port access to Shared O-RU Host/Tenant |
| **Threat description** | A host, tenant, or third-party gains physical port connectivity to the Shared O-RU. With this physical access the actor exploits weak physical layer authentication to gain access to the Shared O-RU. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-16 |
| **Threat title** | Physical port access to O-DU Host/Tenant |
| **Threat description** | A host, tenant, or third-party gains physical port connectivity to a O-DU Host or O-DU Tenant. With this physical access the actor exploits weak physical layer authentication to gain access to the O-DU. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Host, O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-17 |
| **Threat title** | Physical port access to O-CU Host/Tenant |
| **Threat description** | A host, tenant, or third-party gains physical port connectivity to a O-CU Host or O-CU Tenant. With this physical access the actor exploits weak physical layer authentication to gain access to the O-CU. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Host, O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-18 |
| **Threat title** | Malicious User Login Attempt to SMO Host/Tenant |
| **Threat description** | The attacker attempts to access the SMO Host or SMO tenant though a management interface. The attacker may be an internal or external actor. Weak account management and/or authentication can be exploited to gain access to move laterally across the deployment for nefarious purposes such as reconnaissance or damage. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-19 |
| **Threat title** | Malicious User Login Attempt to O-CU Host/Tenant |
| **Threat description** | The attacker attempts to access the O-CU Host or O-CU Tenant though a management interface. The attacker may be an internal or external actor. Weak account management and/or authentication can be exploited to gain access to move laterally across the deployment for nefarious purposes such as reconnaissance or damage. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Host, O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-20 |
| **Threat title** | Malicious User Login Attempt to O-DU Host/Tenant |
| **Threat description** | The attacker attempts to access the O-DU Host or O-DU Tenant though a management interface. The attacker may be an internal or external actor. Weak account management and/or authentication can be exploited to gain access to move laterally across the deployment for nefarious purposes such as reconnaissance or damage. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Host, O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-21 |
| **Threat title** | Malicious User Login Attempt to Shared O-RU Host/Tenant |
| **Threat description** | The attacker attempts to access the O-RU Host or O-RU Tenant though a management interface. The attacker may be an internal or external actor. Weak account management and/or authentication can be exploited to gain access to move laterally across the deployment for nefarious purposes such as reconnaissance or damage. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | Shared O-RU Host, Shared O-RU Tenant |

## Data Access Threats

This section provides threat analysis tables for threats to Shared O-RU data access.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-22 |
| **Threat title** | Unauthorized internal threat actor gains access to data in Shared O-RU |
| **Threat description** | Malicious internal threat actor exploits compromised credentials or weak or misconfigured authorization to gain access to view or modify sensitive data-at-rest or data-in-use in the Shared O-RU. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-23 |
| **Threat title** | Unauthorized external threat actor gains access to data in Shared O-RU |
| **Threat description** | Malicious external threat actor exploits compromised credentials or weak or misconfigured authorization to gain access to view or modify sensitive data-at-rest or data-in-use in the Shared O-RU. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-24 |
| **Threat title** | Data exposure at Shared O-RU |
| **Threat description** | Data-at-rest or data-in-use on the Shared O-RU is exposed to a tenant. Attacker exploits weak confidentiality protection to view data owned by the MNO Host or a MNO Tenant. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-25 |
| **Threat title** | Shared O-RU data exposure at SMO |
| **Threat description** | Data-at-rest or data-in-use on the SMO related to a Shared O-RU is exposed to an unauthorized tenant / SMO user. Attacker exploits weak confidentiality protection to view data owned by the MNO Host or a MNO Tenant of a shared O-RU. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-26 |
| **Threat title** | Shared O-RU data exposure at O-DU |
| **Threat description** | Data-at-rest or data-in-use on the O-DU related to a Shared O-RU is exposed to an unauthorized tenant. Attacker exploits weak confidentiality protection to view data owned by the MNO Host or a MNO Tenant of a shared O-RU. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-27 |
| **Threat title** | Exposed data in transit between Shared O-RU and O-DU Host/Tenant |
| **Threat description** | Data-in-transit between the Shared O-RU and an O-DU Host or O-DU Tenant could be exposed to another MNO or malicious threat actor. Weak confidentiality protection of data-in-transit allows the host, tenant, or actor to view intercepted data owned by the MNO Host or a MNO Tenant. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU, M-Plane, CUS-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-28 |
| **Threat title** | Exposed data in transit between Shared O-RU and SMO Host/Tenant |
| **Threat description** | Data-in-transit between the Shared O-RU and a SMO Host or SMO Tenant could be exposed to another MNO or malicious threat actor. Weak confidentiality protection of data-in-transit allows the host, tenant, or actor to view intercepted data owned by the MNO Host or a MNO Tenant. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU, O1 |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-43 |
| **Threat title** | Eavesdropping of unprotected CUSM-plane data within shared O-RU |
| **Threat description** | The SMO assigns the role of Host and MNO SRO(s). The tenant maliciously or intended is obtaining access to transport protocol stack and is therefore able to eavesdrop sensitive data from neighbor tenants and the host. The tenant may have capability for sniffing/capturing of CUSM-plane data. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

## Availability Threats

This section provides threat analysis tables for availability threats to Shared O-RU.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-29 |
| **Threat title** | Modify/Delete OFH C-Plane messages |
| **Threat description** | A MNO Host, MNO Tenant, or 3rd-party, maliciously modifies or deletes control plane messages on the OFH C-Plane between the Shared O-RU and Host O-DU or Tenant O-DU. This type of integrity attack can also result in an availability attack. |
| **Threat type** | Tampering |
| **Impact type** | Integrity, Availability |
| **Affected Asset** | Shared O-RU, O-DU Host, O-DU Tenant, CUS-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-30 |
| **Threat title** | Clock hijacking on OFH S-Plane |
| **Threat description** | A MNO Host, MNO Tenant, or 3rd-party maliciously takes the role of Grand Master clock on the S-Plane to degrade performance on the U-Plane. This type of authorization exploit can also result in an availability attack. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization, Availability |
| **Affected Asset** | Shared O-RU, O-DU Host, O-DU Tenant, CUS-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-31 |
| **Threat title** | Parameter conflicts at Shared O-RU |
| **Threat description** | O-DU Host and O-DU Tenants may force conflicting parameter settings at the Shared O-RU that can degrade performance or cause an outage. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-32 |
| **Threat title** | Volumetric DDoS attack from O-DU targeting Shared O-RU |
| **Threat description** | An O-DU Host or O-DU Tenant maliciously or unintentionally sends a high-rate of malformed, mis-sequenced, invalid, or valid packets over the Open Fronthaul interface to the Shared O-RU. This kind of attack can cause a Denial of Service on the Shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU, M-Plane, CUS-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-33 |
| **Threat title** | Volumetric DDoS attack from SMO targeting Shared O-RU |
| **Threat description** | The SMO Host maliciously or unintentionally sends a high-rate of malformed, mis-sequenced, invalid, or valid packets over the Open Fronthaul interface to the Shared O-RU. This kind of attack can cause a Denial of Service on the Shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU, O1 |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-34 |
| **Threat title** | Volumetric DDoS attack targeting O-DU |
| **Threat description** | Shared O-RU maliciously or unintentionally sends a high-rate of malformed, mis-sequenced, invalid, or valid packets over the Open Fronthaul interface to the O-DU Host or O-DU Tenant. This kind of attack can cause a Denial of Service on the O-DU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | O-DU Host, O-DU Tenant, CUS-Plane, M-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-35 |
| **Threat title** | Shared O-RU initialization hijacking by DHCP compromise |
| **Threat description** | Shared O-RU bootup and initialization sequence depends on parameters passed to it via DHCP options. An attacker can compromise DHCP server and use it to hijack the O-RU and prevent Shared O-RU from reaching carrier-active state. This kind of attack can cause a Denial of Service on the shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-36 |
| **Threat title** | Shared O-RU M-plane hijacking by DNS compromise |
| **Threat description** | Shared O-RU M-plane initialization depends on DNS, if FQDN is returned as the NETCONF controller of shared O-RU during its initialization. The name resolution of FQDN can be manipulated by an attacker using a compromised DNS server and prevent Shared O-RU from reaching carrier-active state due to unavailability of carrier configuration. This kind of attack can cause a Denial of Service on the shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU |

## Configuration Threats

This section provides threat analysis tables for configuration threats to Shared O-RU.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-37 |
| **Threat title** | Misconfiguration of MNO Host Role |
| **Threat description** | The SMO assigns the role of MNO Host and MNO SRO(s). The assignment of Host role to the wrong SRO can expose data. A threat actor could exploit an incorrectly assigned role of Host to control function of the Shared O-RU |
| **Threat type** | Information Disclosure, Denial of Service |
| **Impact type** | Confidentiality, Availability |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-38 |
| **Threat title** | Incorrect Assignment of Spectrum Resources |
| **Threat description** | Shared O-RU is responsible for assignment and control of spectrum resources, including component carrier and frequencies within a carrier. Tenant access to the wrong resources, due to malicious intent or could be exploited to gain access to information. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-39 |
| **Threat title** | Chain of Trust in a Multi-Tenant Environment |
| **Threat description** | The Chain of Trust is a certificate-based chain used to authenticate an entity. The Chain of Trust is established by validating the hardware and software for the entity up to the root certificate as the trust anchor. The Shared O-RU mutually authenticates O-DU Hosts and O-DU Tenants. Certificates from O-DU tenants must be validated as trustworthy. Malicious actors can exploit untrustworthy certificates to gain access to the Shared O-RU. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | Shared O-RU, O-DU Host, O-DU Tenant, O-CU Host, O-CU Tenant, SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-40 |
| **Threat title** | Hijack of MNO Host Role |
| **Threat description** | The SMO assigns the role of MNO Host and MNO SRO(s). A tenant may maliciously or unintentionally obtain the host role. The elevation of privilege would enable the tenant, acting as host, to have authorized access on the Shared O-RU to sensitive data, credentials, and system privileges. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-41 |
| **Threat title** | Inability of SMO to Revoke Host Privileges from a Malicious Tenant |
| **Threat description** | A malicious tenant obtains the role of Host or MNO SRO. The role enables the malicious tenant to perform actions such as obtaining sensitive data and launching DoS attack. Due to static assignment of privileges, the SMO cannot revoke Host privileges from the malicious tenant. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-42 |
| **Threat title** | Misuse of “sudo” privileges |
| **Threat description** | A malicious tenant obtains the privileges of a Host or MNO SRO. These privileges enable the malicious tenant to perform actions such as obtaining sensitive data and launching DoS attack. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-55 |
| **Threat title** | Set Incorrect Array-Carrier configuration on O-DU (Standby) |
| **Threat description** | Threat actor spoofs SMO to set or modify the pre-configured array-carrier configuration on the O-DU in Standby state. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | O-DU-1, O-DU-2, O1 interface |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-56 |
| **Threat title** | Modify Array-Carrier pre-configuration on Shared O-RU |
| **Threat description** | Threat actor can gain access to Shared O-RU to modify its pre-configured array-carrier |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-57 |
| **Threat title** | Modify/Inject M-Plane messages with Array-Carrier configuration |
| **Threat description** | Threat actor Modifies/Injects M-Plane messages with Array-Carrier configuration sent to the Shared O-RU. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | Shared O-RU, M-Plane |

## Neutral Host Controller (NHC) Threats

This section provides threat analysis tables for threats introduced by the NHC.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-44 |
| **Threat title** | SMO peers with untrusted NHC |
| **Threat description** | One of the optional architectures for deployment of Shared O-RU uses a NHC. In this architectural option, the SMO communicates with the Shared O-RU through a NHC. Lack of strong authentication would allow the SMO to peer with an untrusted NHC, which a malicious threat actor could exploit for further attacks. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-45 |
| **Threat title** | Shared O-RU peers with untrusted NHC |
| **Threat description** | One of the optional architectures for deployment of Shared O-RU uses a NHC. In this architectural option, the Shared O-RU communicates with the SMO through a NHC. Lack of strong authentication would allow the Shared O-RU to peer with an untrusted NHC, which a malicious threat actor could exploit for further attacks. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-46 |
| **Threat title** | NHC peers with untrusted entities |
| **Threat description** | One of the optional architectures for deployment of Shared O-RU uses a NHC. In this architectural option, the Shared O-RU and SMO communicate through a NHC. Lack of strong authentication would allow the NHC to peer with an untrusted SMO or Shared O-RU, which a malicious threat actor could exploit for further attacks. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | NHC |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-47 |
| **Threat title** | Malicious actor at the NHC can access information on the SMO |
| **Threat description** | Without proper authorization controls, a malicious actor who has gained access to the SMO from the NHC could be able to access information on the SMO to view, modify or delete. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-48 |
| **Threat title** | Malicious actor at the NHC can access information on the Shared O-RU |
| **Threat description** | Without proper authorization controls, a malicious actor who has gained access to the Shared O-RU from the NHC could be able to access information on the Shared O-RU to view, modify or delete. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-49 |
| **Threat title** | NHC is source of DDoS attack on SMO |
| **Threat description** | The NHC maliciously or unintentionally sends a high-rate of malformed, mis-sequenced, invalid, or valid packets over the O1 interface to the SMO. This kind of volumetric attack can cause a Denial of Service on the SMO. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-50 |
| **Threat title** | NHC is source of DDoS attack on Shared O-RU |
| **Threat description** | The NHC maliciously or unintentionally sends a high-rate of malformed, mis-sequenced, invalid, or valid packets over the M-Plane interface to the Shared O-RU. This kind of volumetric attack can cause a Denial of Service on the Shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-51 |
| **Threat title** | Shared O-RU data exposure at NHC |
| **Threat description** | Data-at-rest on the NHC related to a Shared O-RU is exposed to an unauthorized tenant. Attacker exploits weak confidentiality protection to view data owned by the MNO Host or a MNO Tenant of a shared O-RU. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

## Resiliency Threats

This section provides threat analysis tables for threats introduced by the O-DU Resiliency use case.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-52 |
| **Threat title** | Thrashing O-DU Failovers |
| **Threat description** | Threat actor spoofs SMO to cause O-DU-1 and O-DU-2 to thrash between Active state and Standby state |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | O-DU, O1 interface |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-53 |
| **Threat title** | Dual (Dueling) Active O-DUs |
| **Threat description** | Threat actor spoofs SMO to cause O-DU-1 and O-DU-2 to both be in Active state. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | O-DU, O1 interface |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-54 |
| **Threat title** | Modify/Inject O1 messages at the SMO |
| **Threat description** | Threat actor spoofs O-DU to modify, inject, flood O1 messages to the SMO to prevent SMO detection of O-DU failure. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO, O1 interface |

# Security Controls

Industry recommendations for strong security controls are provided from sources such as the OWASP Top 10 Proactive Controls [i.15], Center for Internet Security (CIS) Critical Security Controls [i.16], Cloud Security Alliance (CSA) Cloud Control Matrix (CCM) [i.17], ISO/IEC 27001:2013 Information Security Management System (ISMS) [i.18], NIST SP 800-53r5 Security and Privacy Controls for Information Systems and Organizations [i.19], and Cybersecurity and Infrastructure Security Agency (CISA) Security Guidance for 5G Cloud Infrastructures [i.9].

The OWASP Top 10 Proactive Controls are as follow:

C1: Define Security Requirements

C2: Leverage Security Frameworks and Libraries

C3: Secure Database Access

C4: Encode and Escape Data

C5: Validate All Inputs

C6: Implement Digital Identity

C7: Enforce Access Controls

C8: Protect Data Everywhere

C9: Implement Security Logging and Monitoring

C10: Handle All Errors and Exceptions

The CIS Critical Security Controls are as follow:

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 3: Data Protection

CIS Control 4: Secure Configuration of Enterprise Assets and Software

CIS Control 5: Account Management

CIS Control 6: Access Control Management

CIS Control 7: Continuous Vulnerability Management

CIS Control 8: Audit Log Management

CIS Control 9: Email Web Browser and Protections

CIS Control 10: Malware Defenses

CIS Control 11: Data Recovery

CIS Control 12: Network Infrastructure Management

CIS Control 13: Network Monitoring and Defense

CIS Control 14: Security Awareness and Skills Training

CIS Control 15: Service Provider Management

CIS Control 16: Application Software Security

CIS Control 17: Incident Response Management

CIS Control 18: Penetration Testing

Relevant controls from the CSA CCM are 2. Application and Interface Security, 5. Cryptography, Encryption, and Key Management, 7. Data Security and Privacy Lifecycle Management, and 10. Identity and Access Management (IAM).

Relevant controls from ISO/IEC 27001:2013 are 5. Access Controls, 6. Cryptography, and 9. Communications Security.

Relevant controls from NIST SP 800-53r5 are 1. Access Controls, 16. Risk Assessment, 18. System and Communications Protection, and 19. System and Information Integrity.

Relevant controls from CISA’s Security Guidance are TLS 1.2, or higher, with PKI and X.509 certificates, Multi-Factor Authentication (MFA), Principle of Least Privilege, Continuous Monitoring and Logging, and data confidentiality and protection as components of a zero trust architecture as defined in NIST SP 800-207 [i.8].

With consideration of these external sources, the following security controls should be evaluated for the Shared O-RU risk analysis:

Control-1: TLS with PKI and X.509 certificates

Control-2: OAuth 2.0

Control-3: IAM (using RBAC, ABAC, PBAC, TBAC)

Control-4: Principle of Least Privilege

Control-5: Certificate Management

Control-6: API Message Integrity Protection and Input Validation

Control-7: API Message Authentication

Control-8: Encryption for Data at Rest

Control-9: Encryption for Data in Motion

Control-10: Integrity Protection for Data at Rest

Control-11: Integrity Protection for Data in Motion

Control-12: Integrity Protection for Data in Use

Control-13: Digital Signatures

Control-14: Monitoring and Logging

Control-15: Alerting

Control-16: Rate-Limiting

Control-17: Configuration Validation

Control-18: Network Segmentation and Traffic Filtering

Control-19: 802.1X Port-based Network Access Control

Control-20: Conflict Mitigation

Control-21: Multi-Factor Authentication (MFA)

Control-22: Transport Path Separation

Control-23: Authenticated Resource Release Enforcement

# Risk Assessment

This section provides risk assessment tables for each of the identified assets. These tables list the assets, threats, impacts, and possible security controls.

A malicious actor may be a nation-state adversary, cybercriminal, or employee. In a ZTA, perimeter defenses alone are insufficient. O-RAN deployments, including Shared O-RU, must be protected from untrusted external sources attempting to have access, while also assuming internal threat actors are inside the network with access to its functions and data. Security controls for a ZTA, protecting against external and internal threats, should be implemented through a risk-based approach. A risk analysis calculates risk levels by assessing the threat’s Likelihood of attack and the Impact from the attack. External and internal threats are from the perspective of the O-RAN architecture. External Threats are external to the O-RAN and Internal Threats are internal to O-RAN.

Impact scores can be lowered with consideration of existing security controls. Impact scoring is based upon current security controls. Impact scoring does not consider security controls that may be potentially specified in the future.

Likelihood scores may be higher when the goal is a ZTA, because external and internal threats must be considered. When likelihood scoring during a risk analysis, it is necessary to consider internal threats performing reconnaissance attacks impacting confidentiality and privacy and attacks causing damage or degrading performance impacting availability. Internal threat actors are less likely to perform damaging attacks that are quickly and easily detected and blocked, but more likely to attempt reconnaissance attacks to collect information. As a result, reconnaissance type attacks can be scored Likelihood = High while damaging/availability attacks can be scored Likelihood = Medium or Low.

A risk analysis of the Shared O-RU threats is provided in the tables below. A security best practice is to periodically repeat the risk analysis to consider evolving threats and security controls, which may produce an adjusted risk score based upon Impact and Likelihood.

## Lateral Movement Between Network Functions

Table 8-1. Shared O-RU Risk Analysis - Lateral Movement Between Network Functions

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset-Id** | **Asset Name** | **Threat-Id** | **Threat Description (Brief)** | **Impact/ Likelihood Raw Score** | **Possible Security Controls** | **Security Control-Id** |
| ASSET-C-34 | O-DU Host | T-SharedORU-01 | O-DU Tenant accesses O-DU Host | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-35 | O-DU Tenant | T-SharedORU-02 | O-DU Host accesses O-DU Tenant | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-35 | O-DU Tenant | T-SharedORU-03 | O-DU Tenant accesses O-DU Tenant | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-31, ASSET-C-34, ASSET-C-35 | Shared O-RU, O-DU Host, O-DU Tenant | T-SharedORU-04 | Password Attack on OFH M-Plane | Impact = High Likelihood = High | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-34, ASSET-C-35 | O-DU Host, O-DU Tenant | T-SharedORU-05 | Untrusted peering to O-DU | Impact = High Likelihood = High | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-06 | Untrusted peering to the Shared O-RU | Impact = High Likelihood = High | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-38, ASSET-C-39 | SMO Host, SMO Tenant | T-SharedORU-07 | Untrusted peering to the SMO | Impact = High Likelihood = High | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-38 | SMO Host | T-SharedORU-08 | SMO Tenant accesses SMO Host | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-39 | SMO Tenant | T-SharedORU-09 | SMO Host accesses SMO Tenant | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-37 | O-CU Tenant | T-SharedORU-10 | O-DU Host accesses O-CU Tenant | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-36 | O-CU Host | T-SharedORU-11 | O-DU Tenant accesses O-CU Host | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-37 | O-CU Tenant | T-SharedORU-12 | O-DU Tenant accesses O-CU Tenant | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-37 | O-CU Tenant | T-SharedORU-13 | SMO Host accesses O-CU Tenant | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-36 | O-CU Host | T-SharedORU-14 | SMO Tenant accesses O-CU Host | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |

## User Access Threats

Table 8-2. Shared O-RU Risk Analysis – User Access Threats

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset-Id** | **Asset Name** | **Threat-Id** | **Threat Description (Brief)** | **Impact/ Likelihood Raw Score** | **Possible Security Controls** | **Security Control-id** |
| ASSET-C-31 | Shared O-RU | T-SharedORU-15 | Physical port access to Shared O-RU | Impact = High Likelihood = Medium | 802.1X port-based NAC | Control-19 |
| ASSET-C-34, ASSET-C-35 | O-DU Host, O-DU Tenant | T-SharedORU-16 | Physical port access to O-DU | Impact = High Likelihood = Medium | 802.1X port-based NAC | Control-19 |
| ASSET-C-36, ASSET-C-37 | O-CU Host, O-CU Tenant | T-SharedORU-17 | Physical port access to O-CU | Impact = High Likelihood = Medium | 802.1X port-based NAC | Control-19 |
| ASSET-C-38, ASSET-C-39 | SMO Host, SMO Tenant | T-SharedORU-18 | Malicious User Login Attempt to SMO Host/Tenant | Impact = High Likelihood = High | MFA | Control-21 |
| ASSET-C-36, ASSET-C-37 | O-CU Host, O-CU Tenant | T-SharedORU-19 | Malicious User Login Attempt to O-CU Host/Tenant | Impact = High Likelihood = High | MFA | Control-21 |
| ASSET-C-34, ASSET-C-35 | O-DU Host, O-DU Tenant | T-SharedORU-20 | Malicious User Login Attempt to O-DU Host/Tenant | Impact = High Likelihood = High | MFA | Control-21 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-21 | Malicious User Login Attempt to Shared O-RU Host/Tenant | Impact = High Likelihood = High | MFA | Control-21 |

## Data Access Threats

Table 8-3. Shared O-RU Risk Analysis – Data Access Threats

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset-Id** | **Asset Name** | **Threat-Id** | **Threat Description (Brief)** | **Impact/ Likelihood Raw Score** | **Possible Security Controls** | **Security Control-id** |
| ASSET-C-31 | Shared O-RU | T-SharedORU-22 | Unauthorized internal threat actor gains access to data in Shared O-RU | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-23 | Unauthorized external threat actor gains access to data in Shared O-RU | Impact = High Likelihood = Low | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-24 | Exposure of data at rest at Shared O-RU | Impact = High Likelihood = High | Data Encryption | Control-8 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-25 | Exposure of Shared O-RU data at rest at SMO | Impact = High Likelihood = High | Data Encryption | Control-8 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-26 | Exposure of Shared O-RU data at rest at O-DU | Impact = High Likelihood = High | Data Encryption | Control-8 |
| ASSET-C-31, ASSET-C-24, ASSET-C-25 | Shared O-RU, M-Plane, CUS-Plane | T-SharedORU-27 | Exposed data in transit between Shared O-RU and O-DU Host/Tenant | Impact = Low Likelihood = Medium | Confidentiality and Integrity protection for data in transit. PDCP is specified on the OFH U-Plane. TLS 1.2/1.3 and SSHv2 are specified for the OFH M-Plane. | Control-9, Control-11 |
| ASSET-C-31, ASSET-D-03 | Shared O-RU, O1 | T-SharedORU-28 | Exposed data in transit between Shared O-RU and SMO Host/Tenant | Impact = Low Likelihood = Medium | Confidentiality and Integrity protection for data in transit. TLS 1.2/1.3 and SSHv2 are specified for the O1 interface. | Control-9, Control-11 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-43 | Eavesdropping of unprotected CUSM-plane data within shared O-RU | Impact = High  Likelihood =  High | Transport Path Separation | Control-22 |

## Availability Threats

Table 8-4. Shared O-RU Risk Analysis – Availability Threats

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset-Id** | **Asset Name** | **Threat-Id** | **Threat Description (Brief)** | **Impact/ Likelihood Raw Score** | **Possible Security Controls** | **Security Control-id** |
| ASSET-C-31, ASSET-C-34, ASSET-C-35, ASSET-C-25 | Shared O-RU, O-DU Host, O-DU Tenant, CUS-Plane | T-SharedORU-29 | Modify/Delete OFH C-Plane messages | Impact = High Likelihood = Medium | Integrity protection | Control-11 |
| ASSET-C-31, ASSET-C-34, ASSET-C-35, ASSET-C-25 | Shared O-RU, O-DU Host, O-DU Tenant, CUS-Plane | T-SharedORU-30 | Clock hijacking on OFH S-Plane | Impact = High Likelihood = Medium | Message integrity protection, Message authentication | Control-6, Control-7 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-31 | Parameter conflicts at Shared O-RU | Impact = High Likelihood = High | Integrity Protection for data-in-use, Conflict mitigation | Control-12, Control-20 |
| ASSET-C-31, ASSET-C-24, ASSET-C-25 | Shared O-RU, M-Plane, CUS-Plane | T-SharedORU-32 | Volumetric DDoS attack from O-DU targeting Shared O-RU | Impact = High Likelihood = Medium | Rate-Limiting, Network Segmentation | Control-16, Control-18 |
| ASSET-C-31, ASSET-C-22 | Shared O-RU, O1 | T-SharedORU-33 | Volumetric DDoS attack from SMO targeting Shared O-RU | Impact = High Likelihood = Medium | Rate-Limiting, Network segmentation | Control-16, Control-18 |
| ASSET-C-34, ASSET-C-35, ASSET-C-24, ASSET-C-25 | O-DU Host, O-DU Tenant, M-Plane, CUS-Plane | T-SharedORU-34 | Volumetric DDoS attack targeting O-DU | Impact = High Likelihood = Medium | Rate-Limiting, Network Segmentation | Control-16, Control-18 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-35 | Shared O-RU initialization hijacking by DHCP compromise | Impact = High Likelihood = Medium | API Message Input Validation and Message Authentication | Control-6, Control-7 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-36 | Shared O-RU M-plane hijacking by DNS compromise | Impact = High Likelihood = Medium | API Message Input Validation and Message Authentication | Control-6, Control-7 |

## Configuration Threats

Table 8-5. Shared O-RU Risk Analysis – Configuration Threats

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset-Id** | **Asset Name** | **Threat-Id** | **Threat Description (Brief)** | **Impact/ Likelihood Raw Score** | **Possible Security Controls** | **Security Control-id** |
| ASSET-C-31 | Shared O-RU | T-SharedORU-37 | Misconfiguration of MNO Host | Impact = High Likelihood = High | Configuration Validation | Control-17 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-38 | Incorrect Assignment of Spectrum Resources | Impact = High Likelihood = Medium | Configuration Validation | Control-17 |
| ASSET-C-31, ASSET-C-34, ASSET-C-35, ASSET-C-36, ASSET-C-37, ASSET-C-38, ASSET-C-39 | Shared O-RU, O-DU Host, O-DU Tenant, O-CU Host, O-CU Tenant, SMO Host, SMO Tenant | T-SharedORU-39 | Chain of Trust in a Multi-Tenant Environment | Impact = High Likelihood = Medium | Certificate Management, Configuration Validation | Control-5, Control-17 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-40 | Hijack of Host MNO Role | Impact = High Likelihood = Medium | Configuration Validation | Control-17 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-41 | Not Released Host Role (Host Role resume) | Impact = High  Likelihood =  High | Authenticated Resource Release Enforcement | Control-23 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-42 | Misuse of “sudo” privileges | Impact = High  Likelihood =  High | IAM | Control-3 |
| ASSET-C-34, ASSET-C-22 | O-DU, O1 | T-SharedORU-55 | Set Incorrect Array-Carrier configuration on O-DU (Standby) | Impact = High Likelihood = Medium | mTLS/TLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-56 | Modify Array-Carrier pre-configuration on Shared O-RU | Impact = High  Likelihood =  Medium | IAM with Principle of Least Privilege | Control-3, Control-4 |
| ASSET-C-31, ASSET-C-24 | Shared O-RU, M-Plane | T-SharedORU-57 | Modify/Inject M-Plane messages with Array-Carrier configuration | Impact = High  Likelihood =  Medium | TLS 1.2 or 1.3 | Control-11 |

## Neutral Host Controller Threats

Table 8-6. Shared O-RU Risk Analysis – Neutral Host Controller Threats

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset-Id** | **Asset Name** | **Threat-Id** | **Threat Description (Brief)** | **Impact/ Likelihood Raw Score** | **Possible Security Controls** | **Security Control-id** |
| ASSET-C-38, ASSET-C-39 | SMO Host, SMO Tenant | T-SharedORU-44 | SMO peers with untrusted NHC | Impact = High Likelihood = Medium | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-45 | Shared O-RU peers with untrusted NHC | Impact = High Likelihood = Medium | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| TBA | NHC | T-SharedORU-46 | NHC peers with untrusted entities | Impact = High Likelihood = Medium | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-38, ASSET-C-39 | SMO Host, SMO Tenant | T-SharedORU-47 | Malicious actor at the NHC can access information on the SMO | Impact = High Likelihood = Medium | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-48 | Malicious actor at the NHC can access information on the Shared O-RU | Impact = High Likelihood = High | OAuth 2.0, IAM, principle of least privilege | Control-2, Control-3, Control-4 |
| ASSET-C-38, ASSET-C-39 | SMO Host, SMO Tenant | T-SharedORU-49 | NHC is source of DDoS attack on SMO | Impact = High Likelihood = Medium | Rate-Limiting, Network Segmentation | Control-16, Control-18 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-50 | NHC is source of DDoS attack on Shared O-RU | Impact = High Likelihood = Medium | Rate-Limiting, Network Segmentation | Control-16, Control-18 |
| ASSET-C-31 | Shared O-RU | T-SharedORU-51 | Shared O-RU data exposure at NHC | Impact = High Likelihood = High | Data Encryption | Control-8 |

## Resiliency Threats

Table 8-7. Shared O-RU Risk Analysis – Resiliency Threats

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Asset-Id** | **Asset Name** | **Threat-Id** | **Threat Description (Brief)** | **Impact/ Likelihood Raw Score** | **Possible Security Controls** | **Security Control-id** |
| ASSET-C-34, ASSET-C-22 | O-DU, O1 | T-SharedORU-52 | Thrashing O-DU Failovers | Impact = High Likelihood = Medium | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-34, ASSET-C-22 | O-DU, O1 | T-SharedORU-53 | Dual (Dueling) Active O-DUs | Impact = High Likelihood = Medium | mTLS 1.2 or 1.3 with PKI and X.509 certificates | Control-1 |
| ASSET-C-38, ASSET-C-22 | SMO, O1 | T-SharedORU-54 | Modify/Inject O1 messages at the SMO | Impact = High Likelihood = Medium | TLS 1.2 or 1.3 | Control-11 |

# Primary Security Issues

The security analysis described in the document has identified the following issues:

1. New interfaces currently in specifications development process are out of scope in WG11 until further progress is made on the specifications in WG4. These interfaces are Fast Dynamic Scheduling between Host and Tenant O-DUs and Slow Dynamic Scheduling between Host and Tenant SMOs.
2. At this time, Neutral Host Controller (NHC) is not included in the O-RAN architecture, as specified in [i.2]. Security analysis of the NHC may need to be performed again depending upon decisions made by WG1 and WG4. This work item will form normative requirements for the NHC only when WG1 has officially added the NHC to the O-RAN architecture. Until that time there will be no update via CR to add NHC to the following documents:
   * *O-RAN Security Requirements Specification* [i.5]
   * *O-RAN Security Threat Modeling and Remediation Analysis* [i.6]
   * *O-RAN Security Test Specification* [i.7]

# Recommendations

The security analysis described in the document has produced the following recommendations:

1. ZTA requires confidentiality, integrity, and availability protection for network functions and internal interfaces used in the Shared O-RU architecture. Critical security controls for Shared O-RU to comply with a ZTA are:
   * mTLS for authentication
   * OAuth 2.0 for authorization
   * TLS for data in transit
   * Encrypt data at rest
   * MFA for human user login
   * Logging with tenant-awareness
   * Role-Based Access Controls (RBAC) for human users to access data
2. Open Fronthaul specification currently allows password-based authentication [i.20]. PKI-based X.509 certificates is recommended for machine-to-machine authentication in a Shared O-RU multi-tenant environment. If SSH is used then asymmetric keys should be used instead of password.
3. In a multi-tenant environment, 802.1X will enforce port-based network access control on all Shared O-RU ethernet-based management interfaces and ethernet-based network interfaces. WG11 should address 802.1X requirements for Shared O-RU with relevant working groups, including WG1, WG4, WG5, and WG6.
4. Shared O-RU is at risk of conflicting parameters from Shared Operator Host (SOH) and Shared Resource Operator (SRO). Conflict mitigation should be implemented. The mechanism for handling conflicting parameters is specified in clause 19.11 “Partitioning of shared O-RU carrier resources” of the O-RAN Open Fronthaul M-Plane specification [i.20]. This clause identifies common Shared O-RU resources shared across SROs, and defines the expectation that logic for resolving conflicting configuration logic resides outside of Shared O-RU. This was based on WG4 technical evaluation of proposals that concluded the Shared O-RU is not the preferred place for resolving conflicting configuration.
5. SRO isolation should be implemented for SOHs and SROs having co-located resources and/or sharing resources. Tenant isolation for Shared O-RU is addressed in clauses 19.3.1, 19.3.3, and 19.6.1 of the O-RAN Open Fronthaul M-Plane specification [i.20]. These clauses introduce new access privilege groups for NETCONF clients that share the O-RU and define how the ‘carrier’ access privilege is used in the context of carrier management on the Open Fronthaul. Each tenant, also called SRO, user account is associated with a sro-id and ‘carrier’ access privilege.
6. For mTLS, both the client and the server need to have access to a Trust Anchor to verify the peer. There are several options for providing this functionality:

NOTE1: It is the responsibility of the Shared Resource Operator and Shared Operator Host to develop Trust Anchor management processes. Such processes are outside the scope of O-RAN.

NOTE2: In case the shared O-RU owns several certificates, an O-RU controller might need to send a hint to the shared O-RU in its ClientHello message during the TLS handshake indicating which TAs the O-RU controller supports. The extensions used to indicate the client supported TAs are different for TLS 1.2 and TLS 1.3:

* 1. For TLS 1.2, use the trusted\_ca\_key extension; see Section 6 of RFC 6066 ([i.22]).
  2. For TLS 1.3, use the certificate\_authorities extension; see Section 4.2.4 of RFC 8446 ([i.23])

**Option 1: Shared Operator Host** **PKI issues certificates to each of the Shared Resource Operators**: This is also explained in the WG4 Management Plane Specification ([i.20], Clause 6.2.6.2.  
 The Shared Operator Host issues digital certificates for each of the Shared Resource Operators to enable them to mutually authenticate the TLS connection with the Multi-Operator O-RU. Clients should enrol with previously issued certificates.

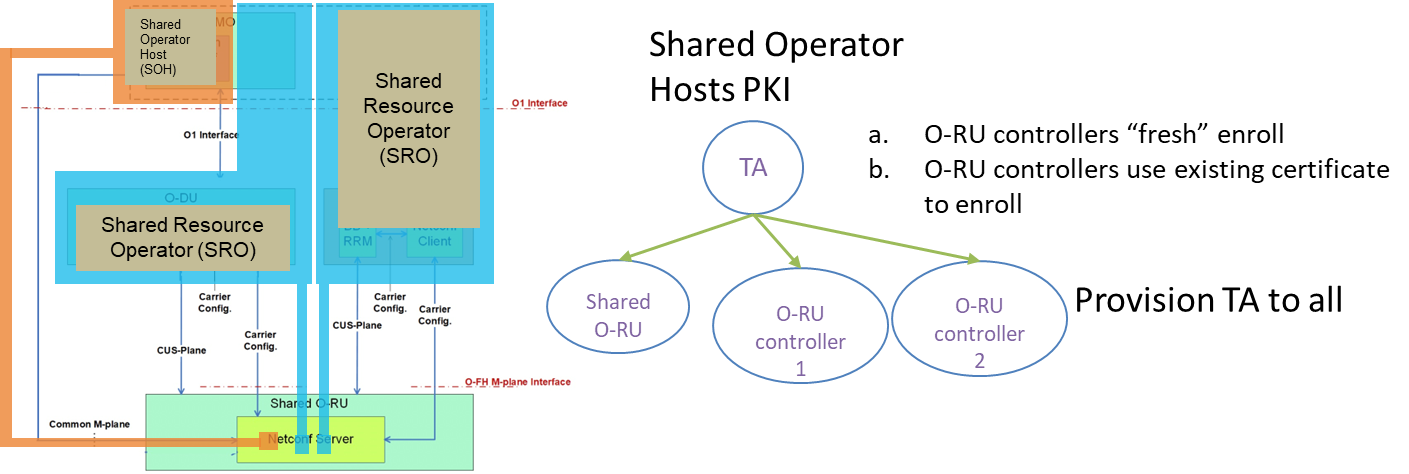
****

Figure 10-1 EXAMPLE: Shared Operator Host PKI issues certificates to each of the Shared Resource Operators

As the Shared O-RU only owns a single certificate, the O-RU controller does not need to send a hint to the Shared O-RU (see NOTE2 above).

**Option 2:**

**Shared O-RU enrolment only:** the Shared O-RU enrols only with the PKI of its SOH and is installed with the TAs of all SROs. Shared Resource Operators are provisioned with SOHs TA. Option 2 appears to balance the effort to implement and maintain the solution best with the advantages gained.

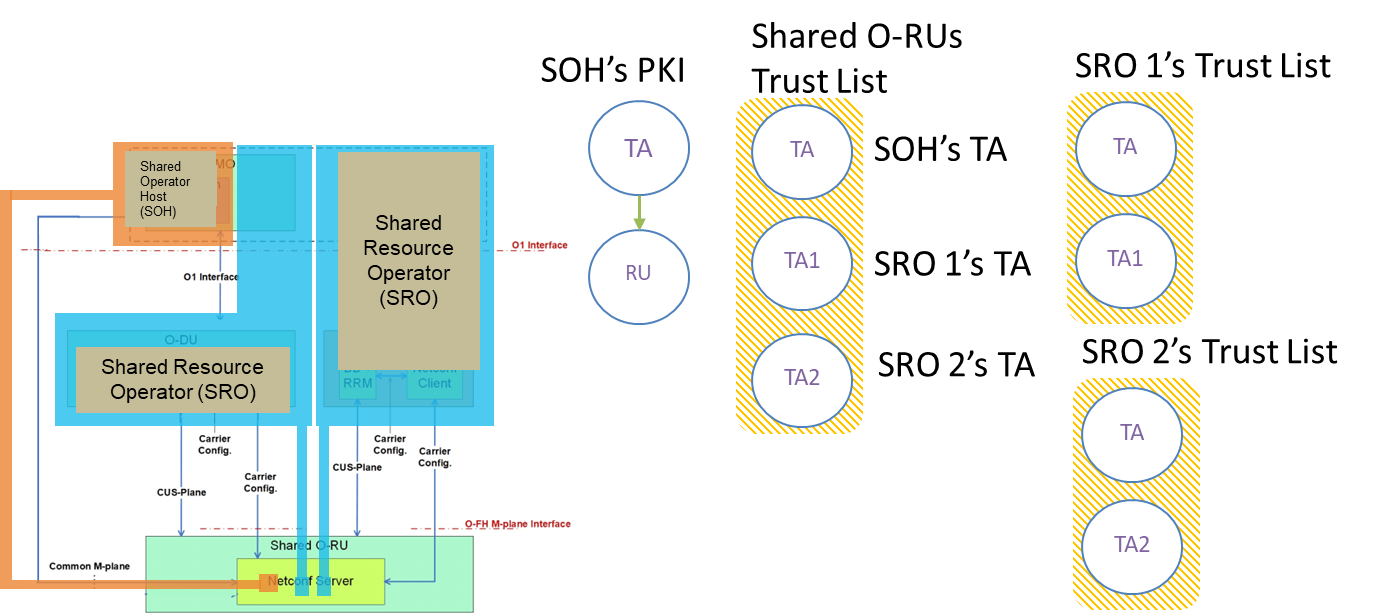


Figure 10-2 EXAMPLE: Shared O-RU enrolment only

As the Shared O-RU only owns a single certificate, the O-RU controller does not need to send a hint to the Shared O-RU (see NOTE2 above).

**Option 3:**

**Shared O-RU and O-RU controllers enrol with a single, separate PKI:** Clients should enrol with previously issued certificates.

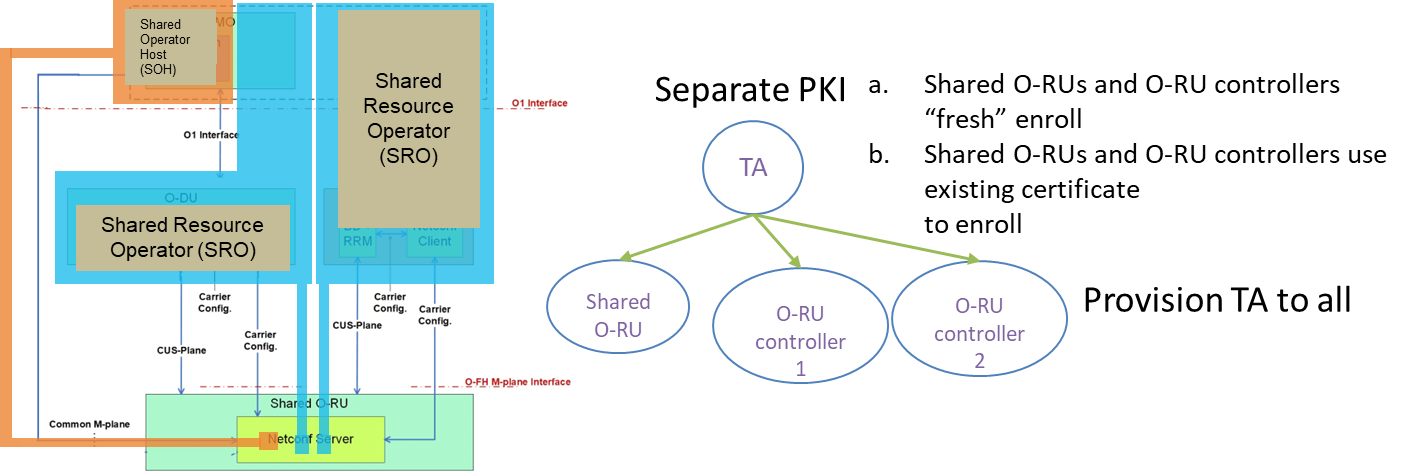
****

Figure 10-3 EXAMPLE: Shared O-RU and O-RU controllers enrol with a single, separate PKI

As the Shared O-RU only owns a single certificate, the O-RU controller does not need to send a hint to the Shared O-RU (see NOTE2 above).

**Option 4:**

**Cross-certification**: Tas cross-certify, either directly or through a Bridge CA.

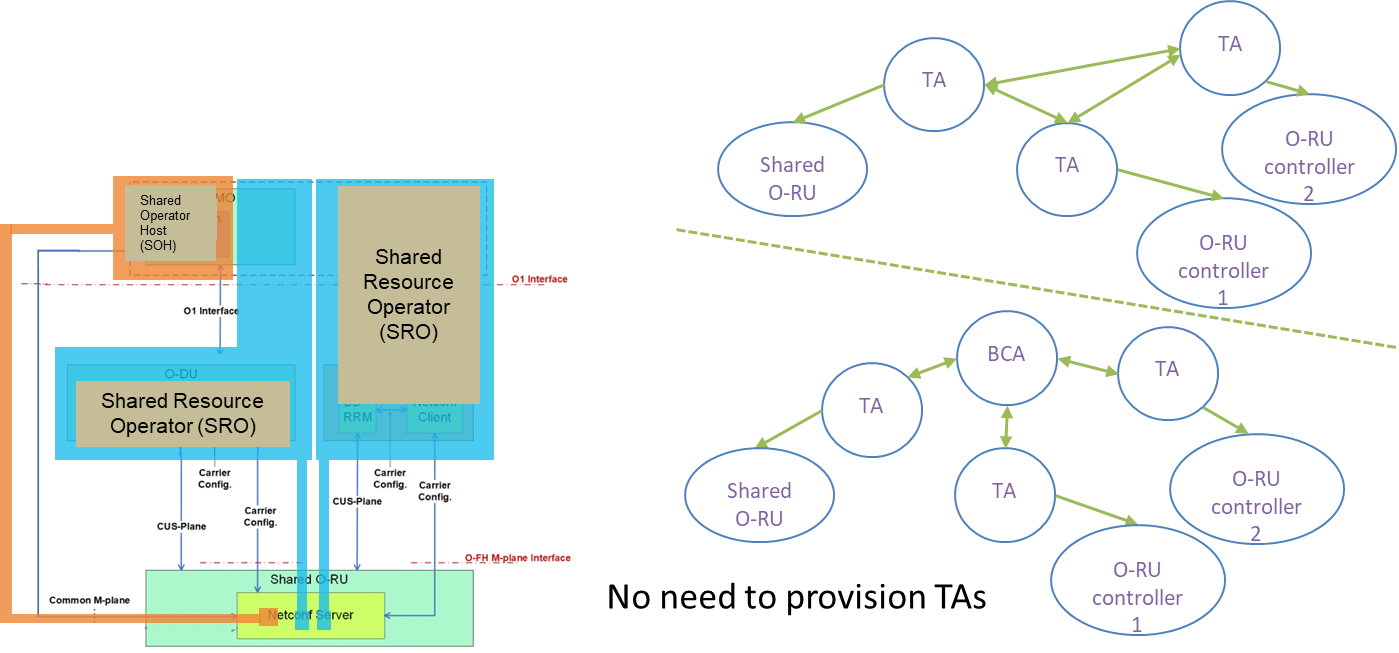


Figure 10-4 EXAMPLE: Cross-Certification

As the Shared O-RU only owns a single certificate, the O-RU controller does not need to send a hint to the Shared O-RU (see NOTE2 above).

Annex A: Shared O-RU All-in-One Architecture

This section describes the concept of a Shared O-RU architecture as shown in Figure A.1-1. The “All-in-One” architecture represents a single deployment scenario. The Shared O-RU is connected to one or more tenants, while one tenant takes over the host role.

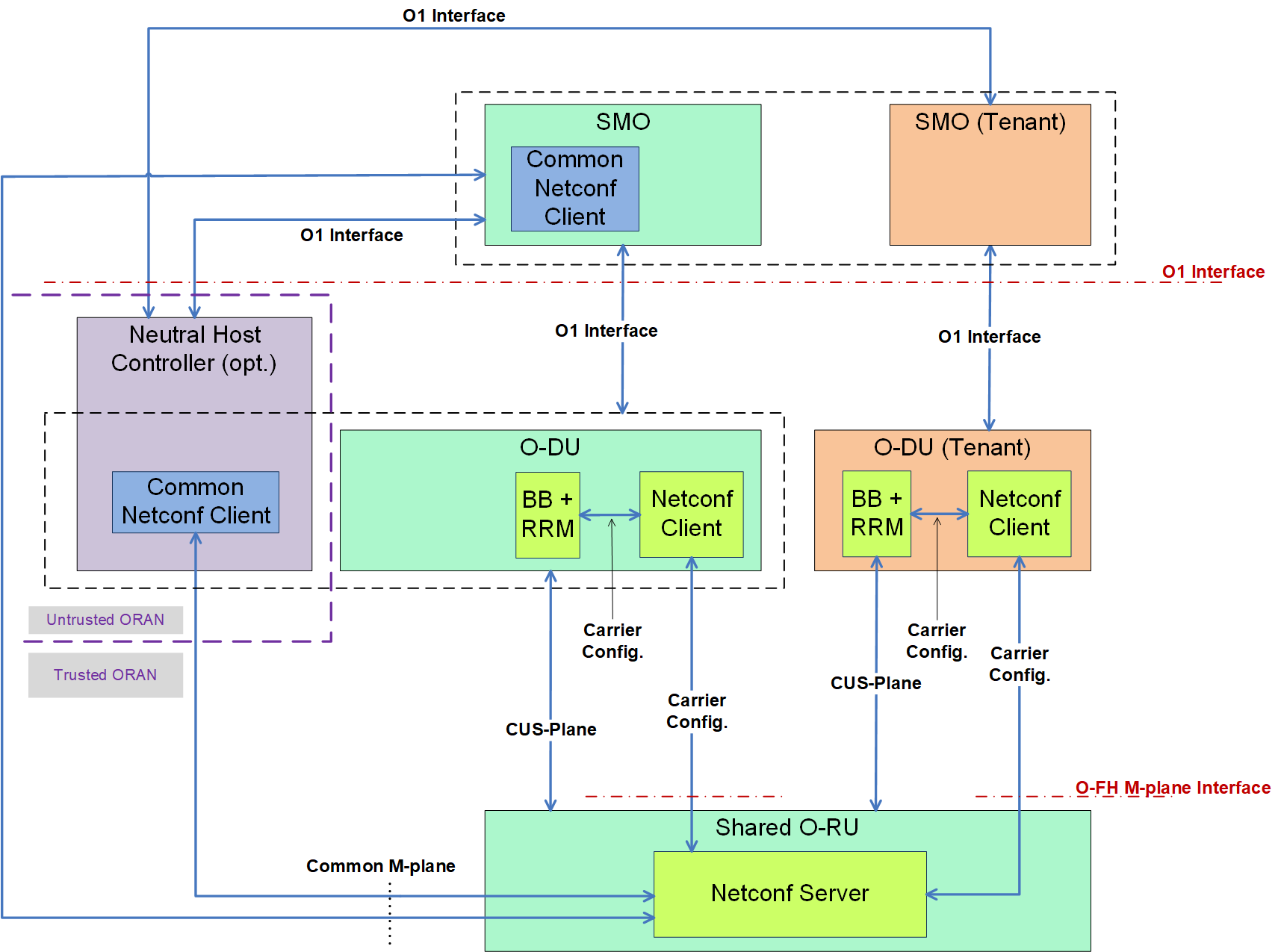


Figure A.1‑ Shared O-RU ’All-in-One’ Architecture (overview)

The following points are considered for the All-in-One architecture:

* The separation of Host and Tenant refers to the multi-MNO deployment scenario, while a merging of both network functions is referring to the single-MNO deployment.
* The Neutral Host Controller is interfaced via a ‘common M-plane’ to O-RU Netconf Server, and the O-DU (host/tenant) is interfaced via a ‘Carrier Configuration’ to the O-RU Netconf Server.
* The common Netconf client functionality can be embedded either inside O-DU network function or can be placed in an external entity namely neutral host controller (NHC). Anyway, for both deployments the common Netconf client is interfaced to the server via a common M-plane, while the Netconf client is interfaced to the Netconf server for carrier configuration purposes.
* The neutral host controller (NHC) is assumed to be inside an ‘untrusted ORAN’, while the O-RAN specific entities are residing inside the ‘trusted ORAN’. The separation of ‘trusted’ and ‘untrusted’ O-RAN is creating additional threat vectors.

Figure A.1-2 shows a simplified view of the ‘All-in-One’ architecture. The following points about “host” and “tenant” is considered:

* The shared O-RU is at the same time interfaces to a host and to a tenant. The term ‘host’ refers to all entities which include host specific functionalities, e.g., Neutral Host Controller or SMO host etc. The term ‘tenant’ refers to all entities which include tenant specific functionalities.
* Both, the host, and the tenant, support a CUS-plane interface, and both support the carrier configuration function via the O-FH M-plane interface. These can be regarded as basic functions of a tenant.
* The host is supporting the common M-plane which is transferred over the O-FH M-plane interface. This is a specific function provided by the host.
* For the shared O-RU the concurrent support of a ‘host’ and ‘tenant’ is required, and therefore needs to be considered for security.

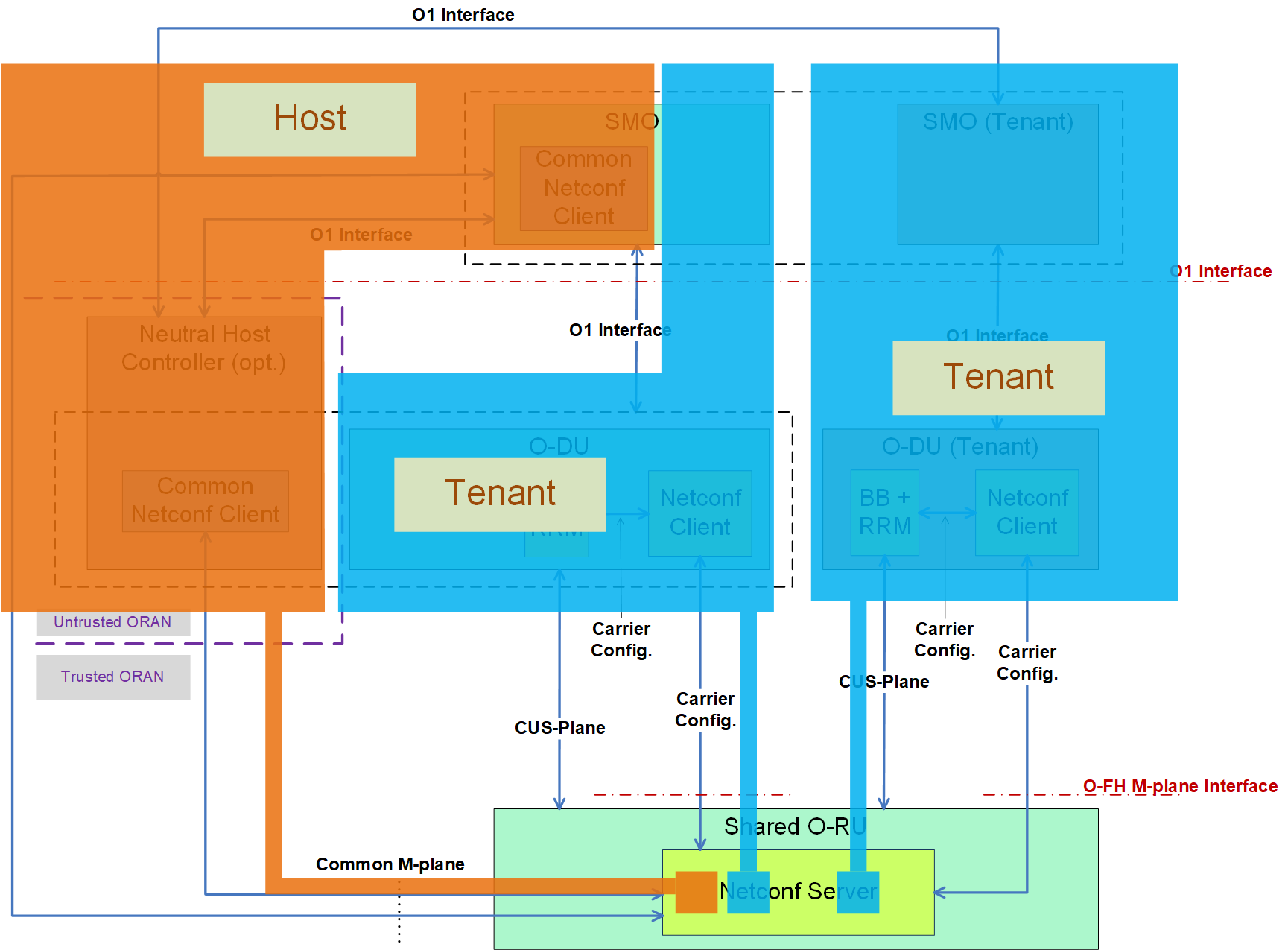


Figure A.1‑2 Shared O-RU Simplified ‘All-in-One’ Architecture (Security Viewpoint)

# Annex change history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Revision** | **Doc status** | **Author** | **Description** |
| October 2022 | V01.00 | First release | WG11 | Document creation, template |
| March 2023 | V02.00 | Second release | WG11 | Adds assets, threat analysis, and risk analysis |
| July 2023 | V03.00 | Third release | WG11 | Completed security analysis with Issues and Recommandations. |
| November 2023 | V04.00 | Fourth release | WG11 | Adds security analysis for Shared O-RU Resiliency. Adds use of SOH and SRO terminology. |
| March 2024 | V05.00 | Fifth release | WG11 | Add resiliency threats to Risk table. |
| July 2024 | V06.00 | Sixth release | WG11 | Updates Shared O-RU asset-ids |