O-RAN - Security Focus Group (SFG)

O-RAN Security Threat Modeling and Remediation Analysis

Prepared by the O-RAN ALLIANCE e.V.

O-RAN ALLIANCE e.V.
Buschkauler Weg 27, 53347 Alfter, Germany
Register of Associations, Bonn VR 11238
VAT ID DE321720189

Revision History

Date	Revision	Doc status	Author	Description
2020.09.15	00.00.01	Working version - draft	WG1-STG	The structure of the document in 6 parts + Initial contents are originated from the existing O-RAN security document, 3GPP documentation, Ericsson whitepaper, ENISA 5G threat landscape, etc.
2020.09.28	00.00.02	Working version - draft	WG1-STG	Roles, Assets, Threats (initial draft list)
2020.10.08	00.00.03	Working version - draft	WG1-STG	Consolidation of Roles, Assets, Threats and Assumptions Update according to feedbacks from Ericsson Development of the threat inventory
2020.10.09	01.00.00	Working version - draft	WG1-STG	Delivery of the initial version
2020.11.04	02.00.00	Working version - draft	WG1-STG	Update according to STG comments and the different inputs provided during the weekly and vF2F meeting
2020.11.18	03.00.00	Working version - draft	WG1-STG	Update according to STG comments during weekly meetings (04/11, 18/11): - Initial list of security requirements is provided - Matrix provided by Ericsson has been included - An example has been added in the SR-ROB requirement (section 4.1.16) - S-Plane requirements have been removed as the text has been taken from reports generated and maintained by the Fronthaul work unit.
2020.12.09	03.00.01	Working version - draft	WG1-STG	Update according to STG comments (STG Work Item: O-RAN security analysis). In addition, the following contents have been added: - ML assets and threats have been added - A new chapter for the statement of compatibility with 3GPP has been added - Threat agent analysis - Etc.

2021.01.04	04.00.00		WG1-STG	Update according to STG comments (STG Work Item: O-RAN security analysis). In addition, the following contents have been added: - A new section 'Methodology' has been added to outline the method followed in realising this security analysis (1.2) - The list of threats has been refined and harmonized - A new threat against PNF has been included (section 5.4.7) - The coverage matrix of threats is completed according to the modifications made on the list of assets and threats (section 5.5) - The coverage matrix of threats by security requirements has been added in 6.2 - Etc.
2021.01.25	04.00.01	Working version - draft	WG1-STG	Update according to STG comments received through the wiki page
2021.02.02	05.00.00	Working version - draft	WG1-STG	Use of the O-RAN specification template
2021.03.03	V01.00.01	Final for review	SFG	Updates according to Nokia's comments on normative aspects of requirements. Change requirements into recommended principles.
2021.03.05	V01.00.02	Final for review	SFG	Updating history table
2021.03.10	V01.00.03	Final version for publication	SFG	Update according to SFG comments

Contents

List of Tables

List of Figures

Chapter 1 Introductory Material

1.1 Scope

The contents of the present document are subject to continuing work within O-RAN and may change following formal O-RAN approval. Should the O-RAN ALLIANCE modify the contents of the present document, it will be re-released by O-RAN with an identifying change of release date and an increase in version number as follows:

Release xx.yy.zz

where:

xx the first two-digit value is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc. (the initial approved document shall have xx=01).

yy the second two-digit value is incremented when editorial only changes have been incorporated in the document.

zz the third two-digit value is included only in working versions of the document indicating incremental changes during the editing process; externally published documents never have this third two-digit value included.

The present document specifies the O-RAN Security Threat Modeling and Remediation Analysis. It identifies assets to be protected, analyzes the O-RAN components for vulnerabilities, examines potential threats associated with those vulnerabilities and provides security principles which stakeholders should adress when building a secure end-to-end O-RAN system.

The purpose of this version of the document is to present a list of system-level security principles as a basic guidline to be considered in the design, development, and operation of the O-RAN system. The principles are short and concise and can be used by organizations to improve the security of their O-RAN components.

In next future versions of the document, the aim is to accomplish a normative security referential by:

- Elaborating on each of security principles in more details,
- Setting precisely what is required (SHALL), recommended (SHOULD) or optional (MAY),
- Refining security principles into requirements, recommendations and potential countermeasures.

1.2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document.

[1] 3GPP TR 21.905: “Vocabulary for 3GPP Specifications”

[2] 3GPP TS 33.511 V16.4.0 (2020-07): Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

[3] 3GPP TS 33.501: Security architecture and procedures for 5G system

[4] 3GPP TR 33.926: Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

[5] 3GPP TS 33.117: Catalogue of general security assurance requirements

[6] ENISA threat landscape for 5g networks

[7] ‘A Survey on C-RAN Security’ Article in IEEE Access · June 2017, DOI: 10.1109/ACCESS.2017.2717852

[8] Intelligent O-RAN for Beyond 5G and 6G Wireless Networks

Solmaz Niknam, Abhishek Roy, Harpreet S. Dhillon, Sukhdeep Singh, Rahul Banerji, Jeffery H. Reed, Navrati Saxena, and Seungil Yoon

arXiv:2005.08374v1, Submitted on 17 May 2020

[9] 5G Americas | Security Considerations for the 5G Era July 2020

[10] 5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation

https://arxiv.org/pdf/1803.03845.pdf

[11] 5G NR Physical Layer Vulnerability- Jamming, Sniffing and Spoofing

http://www.techplayon.com/5g-nr-physical-channel-vulnerability-jamming-sniffing-and-spoofing/

[12] ERICSSON 'Security Considerations of Open RAN' whitepaper and slides.
https://www.ericsson.com/en/security/security-considerations-of-open-ran

[13] ORAN.WG1.O-RAN-Architecture-Description-v04.00.03

[14] ISO 27005 : https://www.iso.org/standard/75281.html

[15] NIST Special Publication 800-154 2 Guide to Data-Centric System Threat Modeling

https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf

[16] Resource Allocation Scheme in 5G Network Slices

https://www.researchgate.net/publication/324942931_Resource_Allocation_Scheme_in_5G_Network_Slices

[17] 3GPP TS 33.818: "Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products".

[18] NIST SP 800-190 - Application Container Security Guide

[19] ENISA - Security aspects of virtualization

[20] CSA - Best Practices for Mitigating Risks in Virtualized Environments

[21] Fraunhofer AISEC - threat analysis of container-as-a-service for network function virtualization

[22] Ecology-Based DoS Attack in Cognitive Radio Networks

https://arxiv.org/pdf/1603.01315.pdf

[23] AN ARCHITECTURAL RISK ANALYSIS OF MACHINE LEARNING SYSTEMS: Toward More Secure Machine Learning

https://berryvilleiml.com/docs/ara.pd

1.3 Definitions, Abbreviations and Terms

1.3.1 Definitions

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

A1: Interface between non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications/functions, and support AI/ML workflow.

A1 policy: Type of declarative policies expressed using formal statements that enable the non-RT RIC function in the SMO to guide the near-RT RIC function, and hence the RAN, towards better fulfilment of the RAN intent.

A1 Enrichment information: Information utilized by near-RT RIC that is collected or derived at SMO/non-RT RIC either from non-network data sources or from network functions themselves.

E2: Interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs.

E2 Node: a logical node terminating E2 interface. In this version of the specification, O-RAN nodes terminating E2 interface are:

- for NR access: O-CU-CP, O-CU-UP, O-DU or any combination;
- for E-UTRA access: O-eNB.

FCAPS: Fault, Configuration, Accounting, Performance, Security.

Intents: A declarative policy to steer or guide the behavior of RAN functions, allowing the RAN function to calculate the optimal result to achieve stated objective.

Near-RT RIC: O-RAN near-real-time RAN Intelligent Controller: a logical function that enables real-time control and optimization of RAN elements and resources via fine-grained data collection and actions over E2 interface.

Non-RT RIC: O-RAN non-real-time RAN Intelligent Controller: a logical function that enables non-real-time control and optimization of RAN elements and resources, AI/ML workflow including model training and updates, and policy-based guidance of applications/features in Near-RT RIC.

O-CU: O-RAN Central Unit: a logical node hosting O-CU-CP and O-CU-UP

O-CU-CP: O-RAN Central Unit – Control Plane: a logical node hosting the RRC and the control plane part of the PDCP protocol.

O-CU-UP: O-RAN Central Unit – User Plane: a logical node hosting the user plane part of the PDCP protocol and the SDAP protocol.

O-DU: O-RAN Distributed Unit: a logical node hosting RLC/MAC/High-PHY layers based on a lower layer functional split.

O-RU: O-RAN Radio Unit: a logical node hosting Low-PHY layer and RF processing based on a lower layer functional split. This is similar to 3GPP's "TRP" or "RRH" but more specific in including the Low-PHY layer (FFT/iFFT, PRACH extraction).

O1: Interface between management entities (NMS/EMS/MANO) and O-RAN managed elements, for operation and management, by which FCAPS management, Software management, File management shall be achieved.

RAN: Generally referred as Radio Access Network. In terms of this document, any component below Near-RT RIC per O-RAN architecture, including O-CU/O-DU/O-RU.

1.3.2 Abbreviations

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

AI/ML	Artificial Intelligence/Machine Learning
eNB	eNodeB (applies to LTE)
gNB	gNodeB (applies to NR)
KPI	Key Performance Indicator
KQI	Key Quality Indicator
MIMO	Multiple Input, Multiple Output
PRB	Physical Resource Block
QoE	Quality of Experience
RIC	O-RAN RAN Intelligent Controller
SINR	Signal-to-Interference-plus-Noise Ratio
UAV	Unmanned Aerial Vehicle
V2X	Vehicle to Everything
SMO	Service Management and Orchestration
MNO	Mobile Network Operator
SDN	Software Defined Network
RBAC	Role-based Access Control
LBT	Listen Before Talk

NF	Network Function
NFV	Network Function Virtualisation
PDCP	Packet Data Convergence Protocol
VM	Virtual machine
VNF	Virtualised Network Function
LLS	Lower Layer Split
NETCONF	Network Configuration Protocol
SSH	Secure Shell
IPSEC	Internet Protocol Security
TLS	Transport Layer Security
PTP	Precision Timing Protocol
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure

1.3.3 Terms

In this document, the significance is following the words defined in the RFC 2119 publication by IETF. These words are:

- "SHALL" This word, or the words "REQUIRED" and "MUST" mean that the process is an absolute requirement of the specification.
- "SHOULD" This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood, and the case carefully weighed before choosing a different course.
- "MAY" This word or the adjective "optional" means that this item is truly optional. One vendor may choose to include the process because a particular marketplace requires it or because it enhances the product, for example, another vendor may omit the same item.

Chapter 2 Overview

2.1 Objective and structure

O-RAN architecture [13] is quite different from the architecture of 3GPP RAN, where new components, interfaces and technologies are proposed, new actors (stakeholders) arise and novel business models are made possible. The attack surface is bigger and we foresee that O-RAN design and deployment will raise numerous security challenges and resulting risks because of the new O-RAN specific interfaces and components, the virtualization/containerization techniques, the support of open source code, the capability to support an AI/ML model, etc.

Therefore, the security analysis and the threat model for O-RAN must be carefully studied and relevant assets/stakeholders/vulnerabilities/threats/requirements/countermeasures/recommendations must be identified to reduce risk exposure and mitigate any harmful effects expected.

The material presented in this analysis aims at supporting various O-RAN stakeholders understanding the relevant threats resulting to an exposure of O-RAN assets by exploiting the vulnerabilities.

The objective is to give a comprehensive and high-level view on how security is organized in O-RAN system. In this document, we assume that 3GPP security requirements are met. Unless explicitly stated, features relate to O-RAN specifications.

This analysis is consolidated from various relevant sources, including main 5G standardization documents and telecommunication best practices (e.g. 3GPP, ETSI, NIST, ENISA and GSMA).

The first main part outlines the main stockholder roles involved in managing and using O-RAN system. Further, it addresses the prerequisites and assumptions needed to securely implement and run O-RAN systems. It also identifies the list of critical assets to be protected in integrity, availability, confidentiality, replay and authenticity.

The second main part addresses the threat model. It identifies the threat agents, determines the threat surface, identifies vulnerabilities, and lists the threats for each O-RAN component or interface. For each threat, the description, threatened asset(s), vulnerabilities, threat agents and affected components are given.

The third main part describes the security principles to be achieved to counter the identified threats. In addition, it illustrates the coverage between threats and security principles.

In next future versions of this document, security requirements, recommendations and countermeasures will be dervived from security principles. Further, a risk assessment and remediation analaysis will be carried out.

Note that this document focuses only on the components, interfaces and protocols specified by O-RAN alliance. Components, interfaces and protocols specified by 3GPP are only referenced where needed but are not within the scope of this specific O-RAN security analysis.

The current document is a working document with the need to update the content on a regular basis following the risk evaluation.

Note: In this document, the term NF (Network Function) is used to designate either VNF (Virtual Network Function), CNF (Containerized or cloud-native Network Function) or PNF (Physical Network Function).

Note: Terms “Containers” and “Virtual Machines” are used interchangeably in this document as the implementation of O-RAN SW components could either be container-based, VM-based or hybrid (Containers and VMs together).

2.2 Methodology

The methodology adopted in this document is based on the standard ISO 27005 [14] which provide a detailed and flexible structure to release a risk assessment.

Refer to NIST SP 800-154 [15] for the definition of Attack, Attack Surface, Attack Vector, Controls, Risk, Risk Mitigation, Threat, and Vulnerability.

The methodology followed in this document comprises three stages:

1) Identification (scope of this version of the document)

   a. **Identify stakeholders:** First, we need to identify the stakeholders involved in the implementation, management, operation and maintenance of the O-RAN system. Roles and responsibilities of each stakeholder are given.

   b. **Define assumptions:** The list of minimum prerequisites and assumptions need to be defined for the operational environment (not under the control of the O-RAN system) required to successfully operate the O-RAN system.

   c. **Identify assets:** First, we need to locate relevant assets the O-RAN system hold and give details about the type (Data, component, etc.), the security properties (CIA) at rest and in transit and location.

   d. **Identify threats:** We need to identify the relevant threats associated with the new O-RAN components, interfaces and technologies. In addition, the threat surface and agents are given.

   e. **Identify vulnerabilities:** O-RAN system may have weaknesses in its new O-RAN components, interfaces and technologies which need to be identified.

   f. **Define security principles:** We need to define security principles to be achieved in order to reduce risk exposure.

   g. **Elaborate and refine security principles:** Each security principle needs to be detailed and refined into requirements, recommendations and countermeasures.

   h. **Identify existing/ongoing countermeasures:** We need to identify all of O-RAN existing/ongoing controls and to take into account the protection provided by these controls before applying any new ones.

2) Risk assessment (will be provided in a future version)

   a. After the identification stage, we need to focus efforts on the biggest threats, so we should use the information you've gathered during the identification stage to prioritize the biggest risks. There are many ways to do this, but the most common approach involves the following equation:

Risk = (the probability of a threat exploiting a vulnerability) x (total impact of the vulnerability being exploited)

3) Risk treatment (will be provided in a future version)

   a. Now that we know the level of risk that each threat poses, we need to decide how we'll treat them. There are four options:

      i. **Modify the risk** by implementing a control to reduce the likelihood of it occurring.

      ii. **Avoid the risk** by ceasing any activity that creates it. This response is appropriate if the risk is too big to manage with a security control.

      iii. **Share the risk** with a third party. There are two ways we can do this: by outsourcing the security efforts to another organization or by purchasing cyber insurance to ensure we have the funds to respond appropriately in the event of a disaster. Neither option is ideal, because we are ultimately responsible for our organization's security, but they might be the best solutions if we lack the resources to tackle the risk.

      iv. **Retain the risk**. This means that our organization accepts the risk and believes that the cost of treating it is greater than the damage that it would cause.

2.3 Perimeter

This chapter comprises the architecture in the scope of the security analysis. The architecture includes the list of O-RAN components, interfaces and protocols manipulating critical assets and implementing security functions.

In the second part, components which are out of scope are given.

2.3.1 Scope regarding architecture

As specified in [13], the logical architecture of O-RAN includes the following components, interfaces and protocols:

O-RAN components:

- Network functions and applications
  - Service Management and Orchestration (SMO)
  - Non-RT RIC and rApps
  - Near-RT RIC and xApps
  - O-CU-CP/UP
  - O-DU
  - O-RU
  - O-eNB
- Cloud computing platform
  - O-Cloud comprising a collection of physical infrastructure nodes that meet O-RAN requirements to host the relevant O-RAN functions (such as Near-RT RIC, O-CU-CP, O-CU-UP, and O-DU), the supporting software components (such as Operating System, Virtual Machine Monitor, Container Runtime, etc.) and the appropriate management and orchestration functions.

Maintained interfaces by O-RAN:

- A1 Interface between Non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications/functions, and support AI/ML workflow.
- O1 Interface connecting the SMO to the Near-RT RIC, one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs.
- O2 Interface between the SMO and the O-Cloud
- E2 Interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, one or more O-DUs, and one or more O-eNBs.
- Open Fronthaul CUS-Plane Interface between O-RU and O-DU
- Open Fronthaul M-Plane Interface between O-RU and O-DU as well as between O-RU and SMO

Relevant Protocols used by O-RAN system for enforcing security:

- TLS
  - Should be used to protect the traffic between the O-RAN system and other network elements. It establishes a secure channel and provides CIA (Confidentiality, Integrity, Authenticity) features.
  - Should be used in O1 interface for NETCONF over TLS and JSON/REST over TLS
  - Should be used in A1 interface
- SSH
  - Should be used in O1 interface and Fronthaul M-Plane for NETCONF over SSH
- IPSEC
  - Should be used to protect E2 traffic
- FTP and FTPS
  - Should be used to protect file transfers over O1 and Fronthaul M-Plane interfaces
- PTP (Precision Timing Protocol, IEEE 1588-2019)

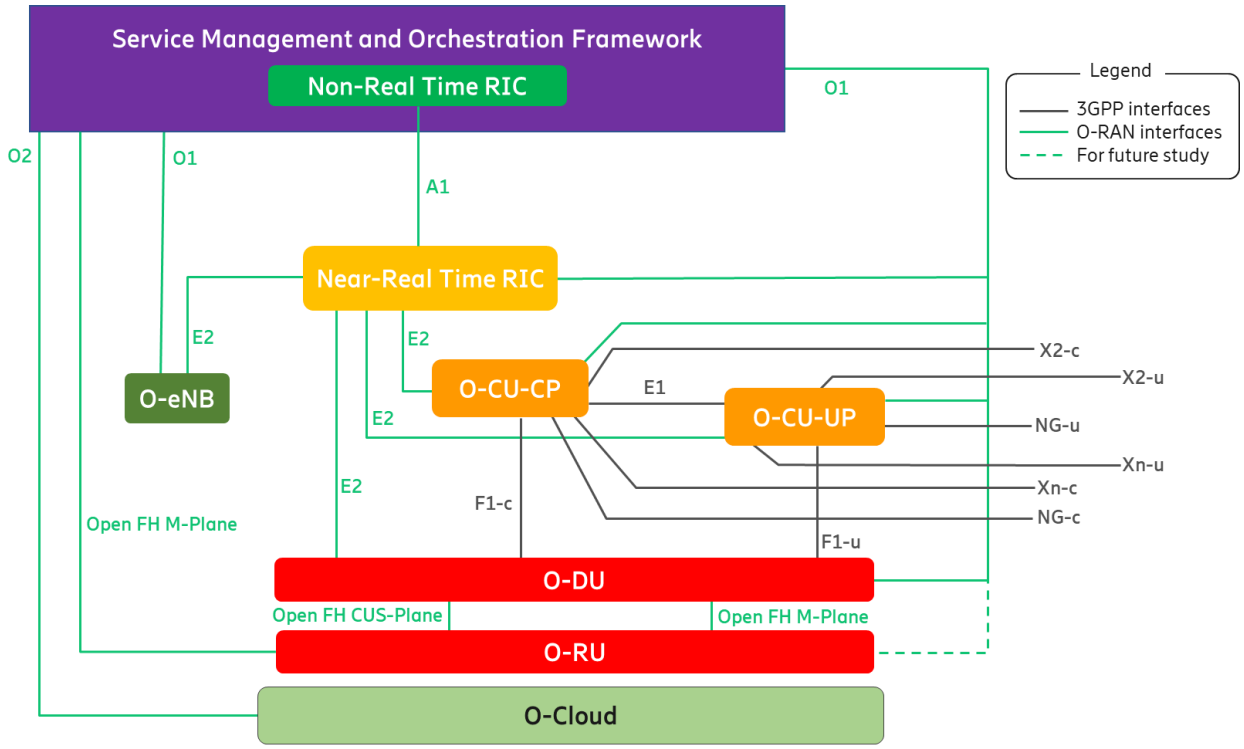

Figure 2-1 : Logical Architecture of O-RAN system [13]

2.3.2 Components not considered

The following components are not in the perimeter of the O-RAN system defined by the alliance; therefore, they are considered out of scope of this study:

- 3GPP interfaces are already studied and maintained by 3GPP,
- UE,
- MEC,
- Core,
- Antennas.

Chapter 3 Statement of compatibility with 3GPP

This chapter gives the statement of compatibility with 3GPP/SCAS security Assets, Threats and Requirements. The statement of compatibility shows that 3GPP Assets/Threats/Requirements are applicable and that there is no conflict affecting the security of O-RAN components.

3.1 Assets and Threats

Table 3-1 : Statement of compatibility with 3GPP – Assets and Threats

3GPP/SCAS document reference/section	Description	Applicable to O-RAN	Rationale
TR 33.926, clauses 5 and 6	It describes the generic assets and threats of 3GPP network products	Yes	Since these assets/threats are for generic 3GPP (virtualized) network products, they are also applicable to O-RAN. It means that there is no need to repeat those assets/threats in this document.
TR 33.818, clause 5.2.4	It describes the generic assets, threats and requirements of 3GPP/ETSI NFV virtualized network products.	Yes	
TR 33.848, clause 5	It considers the consequences of virtualization on 3GPP architectures, in order to identify threats and subsequent security requirements relating to ETSI-defined interfaces and Security functional requirements related to Virtualization layer, hardware and resource isolation.	Yes	

In addition, O-RAN also needs to consider the assets/threats related to the additional specific O-RAN interfaces and components. As a result, sections §4.3 and §5.4 elaborates the O-RAN specific assets and threats respectively.

3.2 Security requirements

Table 3-2 : Statement of compatibility with 3GPP – Security requirements

3GPP/SCAS document reference/section	Description	Applicable to O-RAN	Rationale
TS 33.117, clauses 4.3 and, 4.42	It describes the general approach taken towards security functional requirements deriving from 3GPP specifications and the corresponding test cases, independent of a specific network product class.	Yes	Since these requirements are for generic 3GPP (virtualized) network products, they are to be fulfilled by O-RAN. It means that there is no need to repeat those requirements in this document.
TR 33.818, clauses 5.2.5 and 5.3	It describes the generic assets, threats and requirements of 3GPP/ETSI NFV virtualized network products.	Yes	
TR 33.848, clause 5	It considers the consequences of virtualization on 3GPP architectures, in order to identify threats and subsequent security requirements relating to ETSI-defined interfaces and Security functional requirements related to	Yes	

	Virtualization layer, hardware and resource isolation.		
TS 33.501	It describes the security architecture and procedures for 5G system including gNodeB	Yes	
TS 33.511	It describes the security requirements for the next generation Node B (gNodeB) network product class	Yes	

In addition, O-RAN also needs to consider the security requirements related to the additional specific O-RAN interfaces and components. As a result, chapter §6 focus on the O-RAN security principles.

In future versions of the document, security requirements, recommendations and countermeasures will be derived from security principles.

Chapter 4 Roles-Assumptions-Assets

4.1 Stakeholders roles and responsibilities

The main stakeholders managing and using the O-RAN system are the following:

Table 4-1 : Roles and reponsibilities

Role	Description
Mobile Network Operator (MNO)	Who offers network services and has a license to operate in allocated spectrum.
Orchestrator	Who is in charge of operating and orchestrating the O-RAN services. The MNO could be the orchestrator.
HW/ Network vendor	Who is in charge of: • Providing the network infrastructure including servers to run SDN controller, switches, routers, gateways, radio hardware, etc. • Installation, maintenance or replacement of the hardware/network device • Providing capability and procedures to securely configure the hardware/network device • Providing capability for the hardware/network device to generate log events • Providing capability for log files to be sent to an externalized log analysis system provided by the MNO • Providing a process for users, including security researchers, to submit bug reports (e.g., using an issue tracker or a mailing list) • Testing according to 3GPP and O-RAN test plans. Testing should include security tests of the device and its interfaces • Setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the hardware/network device including firmware • Maintenance of the firmware that includes providing patches for bugs and vulnerabilities
HW/ Network administrator	Who is in charge of: • Configuration of the hardware/network device • Enabling collection of log events • Collection and analysis of log events generated by the hardware/network device • Deploying firmware patches in compliance with HW/ Network vendors deployment guidance • Monitoring, identifying and notifying HW/ Network vendors on discovered vulnerabilities • Regular testing of hardware/network configuration The MNO could be the HW/ Network administrator.
NF vendor	Who is in charge of:

	• Developing and providing NFs (e.g. VNF, CNF, PNF) for Near-RT RIC, O-CU-CP, O-CU-UP, O-DU, etc. • Providing capability and procedures to securely configure the NF • Setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the NF • Setting up a patch development, testing and delivery processes • Maintenance of the NF that includes providing patches for bugs and vulnerabilities • Providing capability for NF to generate log events • Providing capability for log files to be sent to an externalized log analysis system provided by the MNO • Testing according to 3GPP and O-RAN test plans. Testing should include security tests of the NF and its interface • Providing a process for users, including security researchers, to submit bug reports (e.g., using an issue tracker or a mailing list)
NF administrator	Who is in charge of: • Deploying patches in compliance with NF vendors deployment guidance • Monitoring, identifying and notifying NF vendors on discovered vulnerabilities • Securely configuring the NF • Regular testing of the NF configuration • Enabling collection of log events • Analyzing log events generated by the software The MNO could be the NF administrator.
Virtualization/Containerization hardware infrastructure provider	Who is in charge of: • Provides virtualized/containerized infrastructure comprising computing resources (e.g., from computing platforms), storage and network. • Providing capability to securely configure the virtualization/containerization hardware infrastructure • Setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the virtualization/containerization hardware infrastructure • Maintenance of the security of hardware infrastructure • Providing capability for the hardware infrastructure to generate log events • Providing capability for log files to be sent to an externalized log analysis system provided by the MNO • Providing a process for users, including security researchers, to submit bug reports (e.g., using an issue tracker or a mailing list)
Virtualization/Containerization hardware infrastructure administrator	Who is in charge of: • Deploying the Virtualization/Containerization hardware infrastructure in compliance with providers deployment guidance • Monitoring, identifying and notifying Virtualization/Containerization hardware infrastructure providers on discovered vulnerabilities

	• Securely configuring the Virtualization/Containerization hardware infrastructure • Regular testing of the Virtualization/Containerization hardware infrastructure configuration • Enabling collection of log events • Analyzing log events generated by the Virtualization/Containerization hardware infrastructure The MNO could be the Virtualization/Containerization hardware infrastructure administrator.
Virtualization/Containerization software infrastructure provider	Who is in charge of: • Provides virtualized/containerized infrastructure services and designs, builds, and operates virtualization/containerization infrastructure(s). The infrastructure comprises software of compute nodes such as hypervisors, host operating systems, and container run-time systems. • Providing capability to securely configure the virtualization/containerization software infrastructure • Setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the virtualization/containerization software infrastructure • Setting up a patch development, testing and delivery processes • Maintenance of the software infrastructure that includes providing patches for bugs and vulnerabilities • Providing capability for the software infrastructure to generate log events • Providing capability for log files to be sent to an externalized log analysis system provided by the MNO • Providing a process for users, including security researchers, to submit bug reports (e.g., using an issue tracker or a mailing list)
Virtualization/Containerization software infrastructure administrator	Who is in charge of: • Deploying patches in compliance with Virtualization/Containerization software infrastructure providers deployment guidance • Monitoring, identifying and notifying Virtualization/Containerization software infrastructure providers of discovered vulnerabilities • Securely configuring the Virtualization/Containerization software infrastructure • Regular testing of the Virtualization/Containerization software infrastructure configuration • Enabling collection of log events • Analyzing log events generated by the Virtualization/Containerization software infrastructure The MNO could be the Virtualization/Containerization software infrastructure administrator.
System integrator	Who is in charge of: • Appropriately integrating O-RAN HW and SW components. SW components are integrated, in most cases remotely. • Ensuring that those components function together as expected • Securely configuring (system level) the O-RAN system

	• Testing patches after deployment to ensure that they don't break other parts of O-RAN system or even expose new vulnerabilities The MNO could be the integrator.
System tester	Tester of the O-RAN system to ensure quality, security, functionality and performance. The MNO could be the system tester.
Other administrators	Identity Admin: • Manages (Add, Modify, Delete) administrator accounts • Configures general settings for administrator accounts (password policy, etc.) RBAC Admin • Generates RBAC policies and permissions on admin access System Admin • Monitors network traffic for any suspicious activity • Performs risk assessment and defends against zero-day malware • Audits the O-RAN system • Triggers the update of O-RAN components on the latest security patches • Runs regular backups • Regularly performs analysis of log data PKI Admin • Manage and secure private keys and certificates

Note: The operation, administration and orchestration of the O-RAN system can be split across multiple companies or roles.

Note: Compared to a traditional cellular network, the O-RAN communication environment has such characteristics as highly scalable, open and heterogeneous. Many O-RAN usage scenarios are accomplished effectively through the cooperation among mobile operators, vendors, etc. Therefore, a trust management mechanism becomes crucially important to realize trustworthy collaboration among the O-RAN stakeholders.

4.2 Assumptions and prerequisites

This section contains the list of minimum prerequisites and assumptions for equipment, software vendors, users and the physical environment needed to implement and successfully operate the O-RAN system.

- The operational environment of the O-RAN system must provide reliable timestamps for the generation of audit records, etc.
- Administrators, integrators, operators and orchestrators must be trustworthy, and trained such that they are capable of securely managing the O-RAN system and following the instructions provided by O-RAN Alliance as well as the provided guidance by vendors and service providers.
- Log files, secrets and credentials stored in external systems and related to O-RAN shall be protected. They shall be access controlled so only privileged users have access to those secrets/credentials.

4.3 Critical assets

The following table gives the list of critical assets to be protected within the O-RAN system. For each asset, the protection level is proposed. The table only considers critical assets, components and interfaces introduced by O-RAN Alliance.

1 **Table 4-2 : Critical assets**

Asset ID	Asset Description	Component	Interface	When		Protection Level				
				At rest	In transit	Confidentiality	Integrity	Availability	Replay	Authenticity
Data & Interfaces										
ASSET-D-01	Critical S-Plane data such as: - Data flow for synchronization and timing information between nodes - PTP (e.g. ANNOUNCE message) transported over Fronthaul that interconnects multiple O-RUs and O-DUs. - Timing configuration (LLS C1, C2, C3, C4) and topology	O-DU, O-RU	Fronthaul CUS-Plane		x		x		x	x
				x			x	x		
ASSET-D-02	Critical Management-Plane data transported over the Fronthaul interface such as: maintenance and monitoring signals, data collected related to O-RU operations, logs (troubleshooting, trace)	O-DU, O-RU, SMO	Fronthaul M-Plane		x	x	x		x	x
				x		x	x	x		
ASSET-D-03	Critical Management-Plane data transported over the O1 interface such as: - Observables (events and counters) and network status provided over O1 to non-RT RIC from Near-RT RIC, O-CU and O-DU. - The non-RT RIC uses the O1 observables (Feedback on the fulfilment of A1 policies in the near-RT RIC) to continuously evaluate the impact of the A1 policies towards fulfillment of the RAN Intent. - Managed Element Telemetry to monitor the application behavior (from O-Cloud).	Near-RT RIC, Non-RT RIC, O-CU, O-DU, SMO	O1		x	x	x		x	x
				x		x	x	x		
ASSET-D-04	Critical C-Plane data such as: - Scheduling information, FFT size, CP length, Subcarrier spacing, UL PRACH scheduling - DL and UL Beamforming commands (e.g., beam index) and scheduling - LBT Configuration parameters such as lbtHandle, lbtDeferFactor, lbtBackoffCounter, lbtOffset, MCOT, lbtMode, sfnSf, lbtCWconfig_H, lbtCWconfig_T, lbtTrafficClass. - LBT DL indication parameters such as lbtHandle, lbtResult, initialPartialSFs, bufferError, lbtCWR_Result	O-DU, O-RU	Fronthaul CUS-Plane		x	x	x		x	x
				x			x	x		
ASSET-D-05	Critical Fronthaul U-Plane data such as:	O-DU, O-RU			x	x	x		x	x

Asset ID	Asset Description	Component	Interface	When		Protection Level				
				At rest	In transit	Confidentiality	Integrity	Availability	Replay	Authenticity
	- Use data (i.e. DNS, PUSCH, PDSCH, etc.), - Control channel data (PDCCH, PUCCH, etc.), - PRACH data		Fronthaul CUS-Plane	x		x	x	x		
ASSET-D-06	Reference signals, synchronization signal and channels in downlink and uplink between O-RU and UE	O-RU	Radio		x	x	x		x	x
ASSET-D-07	A1 policies that are provided to the near-RT RIC over the A1 interface to guide the RAN performance towards the overall goal expressed in RAN Intent. The A1 policies are declarative policies that contain statements on policy objectives and policy resources applicable to UEs and cells. A1 policies are created, modified and deleted by the non-RT RIC.	Near-RT RIC, Non-RT RIC	A1		x	x	x			x
ASSET-D-08	A1 Enrichment Information that is collected or derived at SMO/non-RT RIC either from non-network data sources or from network functions themselves and provided over the A1 interface to be utilized by near-RT RIC, e.g. an ML model, to improve its performance. Discovery and request of A1 Enrichment Information from near-RT RIC to non-RT RIC External Enrichment Information that is provided by an O-RAN external information source to near-RT RIC over A1	Near-RT RIC, Non-RT RIC	A1		x	x	x			x
ASSET-D-09	Data transported over the O1 interface such as: - Near real-time information (e.g. UE basis, 2Cell basis). - The persistent configuration used by the near-RT RIC to control the RAN. - Identifiers of E2 nodes. - xApp-related messages. - Control signaling information. - Policies used by the Near-RT RIC to monitor, suspend/stop, override or control the behavior of E2 node. - NEAR-RT RIC services messages (REPORT, INSERT, CONTROL and POLICY).	O-DU, O-CU, Near-RT RIC	E2		x	x	x		x	x

Asset ID	Asset Description	Component	Interface	When		Protection Level				
				At rest	In transit	Confidentiality	Integrity	Availability	Replay	Authenticity
	- Interface Management messages (E2 Setup, E2 Reset, E2 Node Configuration Update, Reporting of General Error Situations). - Near-RT RIC Service Update messages.									
ASSET-D-10	Database holding data from xApp applications and E2 Node	Near-RT RIC	-	x		x	x	x		x
ASSET-D-11	E2 Node data (e.g. configuration information (cell configuration, supported slices, PLMNs, etc.), network measurements, context information, etc.)	E2 nodes	-	x			x	x		
ASSET-D-12	O-Cloud Inventory consists of the Physical Infrastructure (O-Cloud Node Identifier, Pool Identifier, Pool Location Identifier, and Use Identifier) used to create the O-Cloud, the logical Clouds which it provides as interfaces for deployments, and the inventory of deployments (deployment ID and descriptor) on the cloud	SMO, O-CLOUD	O2		x	x	x		x	x
ASSET-D-13	It includes: - Telemetry information of O-Cloud deployments in the network for analyzing the O-Cloud's state and health, and for delivering on service monitoring goals. It consists of fault, performance and configuration data: - Deployment Telemetry to monitor the number of deployment instances an O-Cloud has at that moment and how many were expected, how the on-progress deployment is going, and health checks. Additional Deployment Telemetry metrics like CPU, network, and memory usage can also be collected. - - Infrastructure Telemetry to monitor the health of the O-Cloud Infrastructure components. Network Operations are interested in discovering if all the components in the O-Cloud Infrastructure are working properly and at what capacity, how many deployments are running on each node, and the resource utilization of the O-Cloud Infrastructure.	SMO, O-CLOUD	O2		x	x	x		x	x
ASSET-D-14	O-Cloud Provisioning information (Affinity, Anti-Affinity, Quorum Diversity Rules, capabilities, capacity and availability) O-Cloud software management information: catalog of authorized software and its version	SMO, O-CLOUD	O2		x	x	x		x	x
ASSET-D-15	O-RAN Cloudified Network Function Software Image including the underlying software executable image, image properties/metadata such as data files, SoftwareImageId, Vendor, and Version	O-CLOUD	-	x			x	x		

Asset ID	Asset Description	Component	Interface	When		Protection Level				
				At rest	In transit	Confidentiality	Integrity	Availability	Replay	Authenticity
ASSET-D-16	X.509 certificates in O-RAN network such as those used for SMO, O-CU-CP, O-CU-UP, O-DU, O-RU, Near-RT RIC, Non-RT RIC, O-CLOUD, NetCONF (O1, Fronthaul)	All	O1, Fronthaul, O2, E2, A1	x			x	x		x
ASSET-D-17	Security private keys in O-RAN network such as those used for SMO, O-CU-CP, O-CU-UP, O-DU, O-RU, Near-RT RIC, Non-RT RIC, O-CLOUD, NetCONF (O1, Fronthaul)	All	O1, Fronthaul, O2, E2, A1	x		x	x	x		
ASSET-D-18	O-RAN components associated and configuration data, such as: - Software version information, identifier, IP address, port number, network layer parameters, time of request, previous behavior, etc. - The security related parameters (such audit records, lists of algorithms which are allowed for usage, file management, hash values, etc.).	All	-	x		x	x	x		
ASSET-D-19	Cryptographic keys: KgNB, KRRC-enc, KRRC-int, KUP-int, and KUP-enc (Hierarchy of cryptographic key derived from Anchor Key. (as defined in ETSI TS 133 501 section 6.2.)	O-CU	-	x		x	x	x		
ASSET-D-20	Credentials (Administrators): account information and passwords on SMO, O-CU-CP, O-CU-UP, O-DU, O-RU, Near-RT RIC, Non-RT RIC, O-Cloud used in O-RAN network	All		x		x	x	x		
ASSET-D-21	3GPP application related data such as subscription data, session data, call control related information etc.	O-CU		x	x	x	x	x	x	x
ASSET-D-22	Inter- and intra-slice UE priority [16]	O-CU, O-DU	-	x	x		x	x		
ASSET-D-23	Patches for vulnerable SW components	All	-		x		x	x		x
ASSET-D-24	NETCONF Configuration Access Control Model datastores	All		x		x	x	x		x
ASSET-D-25	Training or test data: data sets collected externally or internally from the Near-RT RIC, O-CU and O-DU and passed to the ML training hosts in a ML system.	Near-RT RIC, Non-RT RIC, xAPPs, rAPPs	A1, O1, E2		x	x	x		x	x
				x		x	x	x		x
ASSET-D-26	The trained ML model which includes intellectual property, numerous configured hyperparameters and millions of learned parameters.	Near-RT RIC, Non-RT RIC, xAPPs, rAPPs		x		x	x	x		
ASSET-D-27	The ML prediction results built into the model (e.g. expected outcomes)	Near-RT RIC, Non-RT RIC, xAPPs, rAPPs				x	x	x		

Asset ID	Asset Description	Component	Interface	When		Protection Level				
				At rest	In transit	Confidentiality	Integrity	Availability	Replay	Authenticity
ASSET-D-28	The behavior of the ML system including tasks for data collection, data wrangling, pipeline management, model retraining, and model deployment.	Near-RT RIC, Non-RT RIC, xAPPs, rAPPs		At runtime		x	x	x		
ASSET-D-29	Security event log files generated by O-RAN components	All		x	x		x	x		x
ASSET-D-30	O-RAN specific several UE IDs	Near-RT RIC, Non-RT RIC, SMO	A1, E2, O1		x	x	x		x	x
				x		x	x	x		
Components (logical, virtual, physical)										
ASSET-C-01	Logical module: Service Management and Orchestration (SMO)			x			x	x		x
ASSET-C-02	Near-RT RIC software			x			x	x		x
ASSET-C-03	O-CU-CP software			x			x	x		x
ASSET-C-04	O-CU-UP software			x			x	x		x
ASSET-C-05	O-DU software			x			x	x		x
ASSET-C-06	O-RU software			x			x	x		x
ASSET-C-07	O-eNB			x			x	x		x
ASSET-C-08	O-Cloud			x			x	x		x
ASSET-C-09	xApps			x			x	x		x
ASSET-C-10	rApps			x			x	x		x
ASSET-C-11	Non-RT RIC software			x			x	x		x
ASSET-C-12	ML components deploying machine learning such as: ML training and interference hosts, ML applications (xAPPS, rAPPs)			x			x	x		x
ASSET-C-12	PNF NF equipment			x			x	x		x

Chapter 5 Threat model

As the industry evolves towards RAN virtualization, it is important that a risk-based approach is taken to adequately address O-RAN security risks. Building upon the foundation set forth by 3GPP, O-RAN is standardized by the O-RAN Alliance with new functions and open, interoperable interfaces. With any nascent technology, including O-RAN, security should be built upon security-by-design using a risk-based approach, with consideration of potential zero-day attacks. The O-RAN architecture [13] has security risks beyond those in a 3GPP architecture due to its expanded threat surface from new functions, additional interfaces, and the Lower Layer Split (LLS). The disaggregation of hardware and software, virtualization, and use of open source components also present security risks that must be addressed.

5.1 Threat surface

The O-RAN architecture [13] introduces new functions and interfaces. The introduction of additional interfaces and nodes, and the decoupling of hardware and software, expands the threat and attack surface of the network. Threat surfaces may be divided into 6 main groups:

- Additional functions: SMO, Non-Real-Time RIC, Near-Real-Time RIC
- Additional open interfaces: A1, E2, O1, O2, Open Fronthaul
- Modified architecture: Lower Layer Split (LLS) 7-2x
- Decoupling increases threat to Trust Chain
- Containerization and Virtualization: Disaggregation of software and hardware
- Exposure to public exploits may be increased due to use of Open Source Code

The following entry points are considered:

- API between planes which facilitate the propagation of threats
- Threats coming from inside the O-RAN system
- Threats coming from outside the O-RAN system

5.2 Threat agent

Threat agents can be categorized as follows:

- Cyber-criminals: Represents individuals who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.
- Insiders: Represents malicious attacks perpetrated on a network or computer system by a person with authorized system access.
- Hacktivists: Represents actors that perform cyber-attacks to achieve political or social gains.
- Cyber-terrorists: Represents actors that their sole aim of violence against clandestine agents and subnational groups through the compromise of O-RAN infrastructures.
- Script kiddies: Represents actors that do not poses deep technical expertise or resources to perform sophisticated attacks.
- Nation-State: actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information. They may be part of a state apparatus or receive direction, funding, or technical assistance from a nation-state.

5.3 Potential vulnerabilities

This document addresses the following potential security vulnerabilities that could be exploited through attacks against Confidentiality, Integrity, and Availability:

- O-RAN specific vulnerabilities
    - Unauthorized access to O-DU, O-CU-CP, O-CU-UP and RU to degrade RAN performance or execute broader network attack (Availability)
    - Unprotected synchronization and control plane traffic on Open Fronthaul Interface (Integrity and Availability)
    - Disable over-the-air ciphers for eavesdropping (Confidentiality)
    - Near-RT RIC conflicts with O-gNB (Availability)
    - x/rApps conflicts (Availability)
    - x/rApps access to network and subscriber data (Confidentiality)
    - Unprotected management interface (Confidentiality, Integrity, Availability)
    - CP UL or DL messages can be injected for attack on UP (Availability)
- General vulnerabilities
    - Decoupling of functions without hardware root of trust and software trust chain (Integrity)
    - Exposure to public exploits from use of Open Source code (Confidentiality, Integrity, Availability)
    - Misconfiguration, poor isolation or insufficient access management in the O-Cloud platform (Confidentiality, Integrity, Availability)

5.4 Threats

Threats can be grouped in seven categories:

- Threats against O-RAN system
- Threats against O-CLOUD
- Threats to open source code
- Physical Threats
- Threats against 5G radio networks
- Threats against ML system

The threat analysis is carried out using a well-defined structure to present each threat cases and simplify the risk analysis associated with each threat. In the following subsections, only a unique ID, title and description of each threat are given:

Threat ID	Unique identification per Threat (e.g. T-XX-01)
Threat title	Title of the threat
Threat description	Description of the Threat

At the end of this chapter a matrix is provided depicting the mapping between threats and the following elements:

Threat agent	An individual or group that can manifest a threat
Vulnerability	What vulnerabilities can the threat exploits?
Threatened Assets	Impacted Asset(s)
Affected Components	The list of Components impacted by that Threat

The template of the matrix is as follows:

Threat ID	Threat title	Threat agent	Vulnerability	Threatened Asset	Affected Components

5.4.1 Threats against O-RAN system

5.4.1.1 Common among O-RAN components

The O-RAN system architecture introduces the following common threats among its components:

Threat ID	T-O-RAN-01
Threat title	An attacker exploits insecure designs or lack of adoption in O-RAN components
Threat description	Unauthenticated/unauthorized access to O-RAN components could possibly be achieved via the different O-RAN interfaces, depending upon the design of the hardware-software O-RAN system and how different functions are segregated within the O-RAN system. O-RAN components might be vulnerable if: • Outdated component from the lack of update or patch management, • Poorly design architecture, • Missing appropriate security hardening, • Unnecessary or insecure function/protocol/component. An attacker could, in such case, either inject malwares and/or manipulate existing software, harm the O-RAN components, create a performance issue by manipulation of parameters, or reconfigure the O-RAN components and disable the security features with the purpose of eavesdropping or wiretapping on various CUS & M planes, reaching northbound systems, attack broader network to cause denial-of-service, steal unprotected private keys, certificates, hash values, or other type of breaches. In addition, O-RAN components could be software providing network functions, so they are likely to be vulnerable to software flaws: it could be possible to bypass firewall restrictions or to take advantage of a buffer overflow to execute arbitrary commands, etc.

Threat ID	T-O-RAN-02
Threat title	An attacker exploits misconfigured or poorly configured O-RAN components
Threat description	Unauthenticated/unauthorized access to O-RAN components could possibly be achieved via the different O-RAN interfaces, depending upon the configuration of the hardware-software O-RAN system. O-RAN components might be vulnerable if: • Errors from the lack of configuration change management, • Misconfigured or poorly configured O-RAN components,

	• Improperly configured permissions, • Unnecessary features are enabled (e.g. unnecessary ports, services, accounts, or privileges), • Default accounts and their passwords still enabled and unchanged, • Security features are disabled or not configured securely. An attacker could, in such case, either inject malwares and/or manipulate existing software, harm the O-RAN components, create a performance issue by manipulation of parameters, or reconfigure the O-RAN components and disable the security features with the purpose of eavesdropping or wiretapping on various CUS & M planes, reaching northbound systems, attack broader network to cause denial-of-service, steal unprotected private keys, certificates, hash values, or other type of breaches.

1

Threat ID	T-O-RAN-03
Threat title	Attacks from the internet exploit weak authentication and access control to penetrate O-RAN network boundary
Threat description	Web servers serving O-RAN functional and management services should provide adequate protection. An attacker that have access to the uncontrolled O-RAN network could: • Bypass the information flow control policy implemented by the firewall, • And/or attack O-RAN components in the trusted networks by taking advantage of particularities and errors in the design and implementation of the network protocols (IP, TCP, UDP, application protocols), • Use of incorrect or exceeded TCP sequence numbers, • Perform brute force attacks on FTP passwords, • Use of improper HTTP user sessions, • Etc. The effects of such attacks may include: • An intrusion, meaning unauthorized access to O-RAN components, • Blocking, flooding or restarting an O-RAN component causing a denial of service, • Flooding of network equipment, causing a denial of service, • Etc.

2

Threat ID	T-O-RAN-04
Threat title	An attacker attempts to jam the airlink signal through IoT devices
Threat description	DDoS attacks on O-RAN systems: The 5G evolution means billions of things, collectively referred to as IoT, will be using the 5G O-RAN. Thus, IoT could increase the risk of O-RAN resource overload by way of DDoS attacks. Attackers create a botnet army by infecting many (millions/billions) IoT devices with a “remote-reboot” malware. Attackers instruct the malware to reboot all devices in a specific or targeted 5G coverage area at the same time.

3

Threat ID	T-O-RAN-05
Threat title	An attacker penetrates and compromises the O-RAN system through the open O-RAN’s Fronthaul, O1, O2, A1, and E2
Threat description	O-RAN’s Fronthaul, O1, O2, A1, and E2 management interfaces are the new open interfaces that allow software programmability of RAN. These interfaces may not be secured to industry best practices.

	O-RAN components might be vulnerable if: • Improper or missing authentication and authorization processes, • Improper or missing ciphering and integrity checks of sensitive data exchanged over O-RAN interfaces, • Improper or missing replay protection of sensitive data exchanged over O-RAN interfaces, • Improper prevention of key reuse, • Improper implementation, • Improperly validate inputs, respond to error conditions in both the submitted data as well as out of sequence protocol steps. An attacker could, in such case, cause denial-of-service, data tampering or information disclosure, etc. Note: O-RAN interfaces allow use of TLS or SSH. Industry best practices mandate the use of TLS (v1.2 or higher) or SSH certificate-based authentication. An implementation that implement TLS version lower than 1.2 or a SSH password authentication, may become the key source of vulnerability that a malicious code will exploit to compromise the O-RAN system.

1

Threat ID	T-O-RAN-06
Threat title	An attacker exploits insufficient/improper mechanisms for authentication and authorization to compromise O-RAN components
Threat description	O-RAN management and orchestration should not be used without appropriate authentication and authorization and authorization checks. O-RAN components might be vulnerable if: • Unauthenticated access to O-RAN functions, • Improper authentication mechanisms, • Use of Predefined/ default accounts, • Weak or missing password policy, • Lack of mutual authentication to O-RAN components and interfaces, • Failure to block consecutive failed login attempts, • Improper authorization and access control policy. An attacker could, in such case, either inject malwares and/or manipulate existing software, harm the O-RAN components, create a performance issue by manipulation of parameters, or reconfigure the O-RAN components and disable the security features with the purpose of eavesdropping or wiretapping on various CUS & M planes, reaching northbound systems, attack broader network to cause denial-of-service, steal unprotected private keys, certificates, hash values, or other type of breaches.

2

Threat ID	T-O-RAN-07
Threat title	An attacker compromises O-RAN monitoring mechanisms and log files integrity and availability
Threat description	Improper / missing controls for protection of security event log files generated by O-RAN components and the lack of security events logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred do not allow a correct and rapid audit in case of security incident occurrence. Security restoration is delayed. Compromise of availability and integrity of security event log files could conduct to delays, wrong audit results, delays in security restoration, threats persistence.

3

Threat ID	T-O-RAN-08
Threat title	An attacker compromises O-RAN data integrity, confidentiality and traceability
Threat description	O-RAN components may not be secured to industry best practices. Adequate security controls are needed for protecting sensitive data stored, processed and transferred by O-RAN components. O-RAN components might be vulnerable if: • Improper or missing ciphering of sensitive data in storage or in transfer, • Improper or missing integrity mechanisms to protect sensitive data in storage or in transfer, • Presence of active function(s) that reveal confidential internal data in the clear to administrators. Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. • No traceability (logging) of access to personal data. An attacker could, in such case, cause denial-of-service, data tampering, information disclosure, spoofing identity, elevation of privilege, etc.

Threat ID	T-O-RAN-09
Threat title	An attacker compromises O-RAN components integrity and availability
Threat description	Overload situation could appear in the case of DoS attack or increased traffic. Inability to deal with such events affects availability of information or security functionalities of O-RAN components. O-RAN components may boot from unauthorized memory devices. Inability to deal with such events affects integrity of information or security functionalities of O-RAN components. Insufficient assurance of O-RAN software package integrity could affect CIA of data, services, hardware and policies during installation or upgrade phases for O-RAN components. An attacker could, in such case, cause denial-of-service, data tampering, information disclosure, spoofing identity, etc.

5.4.1.2 Threats against the fronthaul interface and M-S-C-U planes

The LLS architecture and the fronthaul interface introduce the following threats:

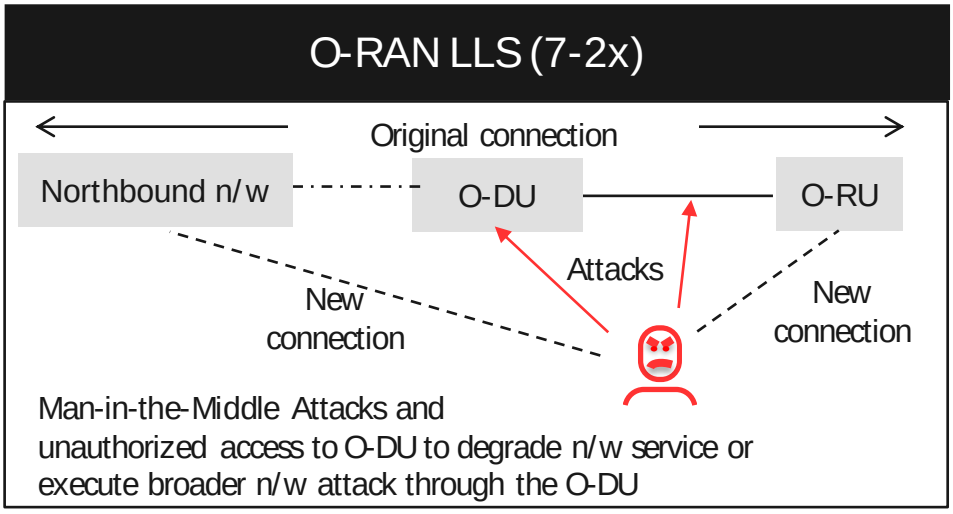

Figure 5-1 : Threats and Vulnerabilities for O-RAN LLS 7-2x

Threat ID	T-FRHAUL-01
Threat title	An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface [12]
Threat description	When having two different vendors, the O-RU and the O-DU needs to be managed as different entities and may have heterogeneous security levels. Instead, the O-DU will have to bridge the management traffic between the management system and the O-RU. Hence the possibilities to reach the northbound systems beyond the O-DU through the Open Fronthaul interface become a possible attack vector in this split architecture.

1

Threat ID	T-MPLANE-01
Threat title	An attacker attempts to intercept the Fronthaul (MITM) over M Plane
Threat description	The High bit rate Fronthaul interface impose strict performance requirements ((bandwidth, latency, fronthaul transport link length, etc.) that limit the use of some security features, due to the increased processing delay. This opens the risk of Man-in-the-Middle (MITM) attacks over the fronthaul interface or O1 to intercept the M plane. For the transported Management-Plane data over the fronthaul interface or O1, an Attacker could potentially do threats, such as passive wiretapping and denial of service, but would need to break M-Plane Security prior to gain OAM access.

2

Threat ID	T-SPLANE-01
Threat title	DoS attack against a Master clock
Threat description	An attacker can attack a master clock by sending an excessive number of time protocol packets or impersonate a legitimate clock, a slave, or an intermediate clock, by sending malicious messages to the master, thus degrading the victim's performance. The attacker may be residing either within the attacked network (insider) or on an external network connected to the attacked network. This attack results in a situation where the clock service is interrupted completely or the timing protocol is operational but slaves are being provided inaccurate timing information due the degraded performance of the Master clock. This degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell. A cell outage caused by misaligned time, may further impact performance in connected neighboring cells.

3

Threat ID	T-SPLANE-02
Threat title	MITM random delay attack against selective PTP messages
Threat description	An attacker acting as MITM can introduce random packet delay on PTP sync messages and/or PTP delay-req/resp messages (in between master and slaves), which causes inaccurate PTP offset calculation, thus the clocks may not be synchronized properly. The attacker has to be residing within the attacked network (insider) for this attack. This attack results in a situation where the clock service is operational but slaves are being served with inaccurate timing information.

4

Threat ID	T-CPLANE-01
Threat title	Spoofing of DL/UL C-plane messages
Threat description	The lack of authentication could allow an adversary to inject DL/UL C-plane messages that falsely claim to be from the associated O-DU. As a result, it would impact the O-RU to process the corresponding U-Plane packets, leading to temporarily limited cell performance (or even DoS) on cells served by the O-RU and in addition a consequential threat to all O-RUs parented to that O-DU might exist.

5

Threat ID	T-CPLANE-02

Threat title	DoS Attack against O-DU C-plane
Threat description	Due to the clear-text nature of eCPRI messages used for the Open Fronthaul C-Plane, an attacker can launch a volumetric DoS attack with bad or unauthenticated eCPRI Real-time control data messages (adopted for C-Plane communication) against the O-DU C-Plane, causing O-DU performance degradation and potentially its overall service interruption, which could further cascade to all its serving O-RUs.

Threat ID	T-UPLANE-01
Threat title	An attacker attempts to intercept the Fronthaul (MITM) over U Plane
Threat description	The High bit rate Fronthaul interface impose strict performance requirements ((bandwidth, latency, fronthaul transport link length, etc.) that limit the use of some security features, due to the increased processing delay. This opens the risk of Man-in-the-Middle (MITM) attacks over the fronthaul interface to intercept the U-Plane. For the transported U-Plane data an attacker could potentially do threats, such as passive wiretapping and denial of service, but would need to break PDCP Security prior to any content access. 3GPP defines UP integrity protection algorithms in their specifications but many of the OEMs have not implemented them because of impact on the user experience (e.g. download and upload data throughputs). Enabling UP integrity protection requires considerable compute resources and adds overhead that directly impacts the maximum throughputs that can be measured on the user device. The integrity protection is enabled on the Control Plane messages but that still leaves the user's data traffic vulnerable because the Control Plane and User Plane are segregated. For example, the lack of UP integrity could enable a rogue base station to manipulate the user data messages (i.e. DNS) and redirect a user to a malicious website.

5.4.1.3 Threats against O-RU

The O-RU introduces the following threats:

Threat ID	T-ORU-01
Threat title	An attacker stands up a rogue O-RU
Threat description	The idea is to 'fool' O-DU or UE into associating to this rogue O-RU over the legitimate O-RUs. False O-RUs or SUPI/5G-GUTI catchers are able to retrieve the subscriber identity by forcing a device to attach to the Rogue O-RU while sniffing the unencrypted traffic over the air. This opens the door to subscriber's identity interception/disclosure and unauthorized user tracking attacks. SUPI/5G-GUTI catching attacks can be used to reveal the identity of a subscriber by catching the SUPI/5G-GUTI of the subscriber's User Equipment (UE) and location of a device) to enable unauthorized tracking of user movements and activities.

5.4.1.4 Threats against Near-RT RIC

Near-Real-Time (RT) RIC introduces the following threats:

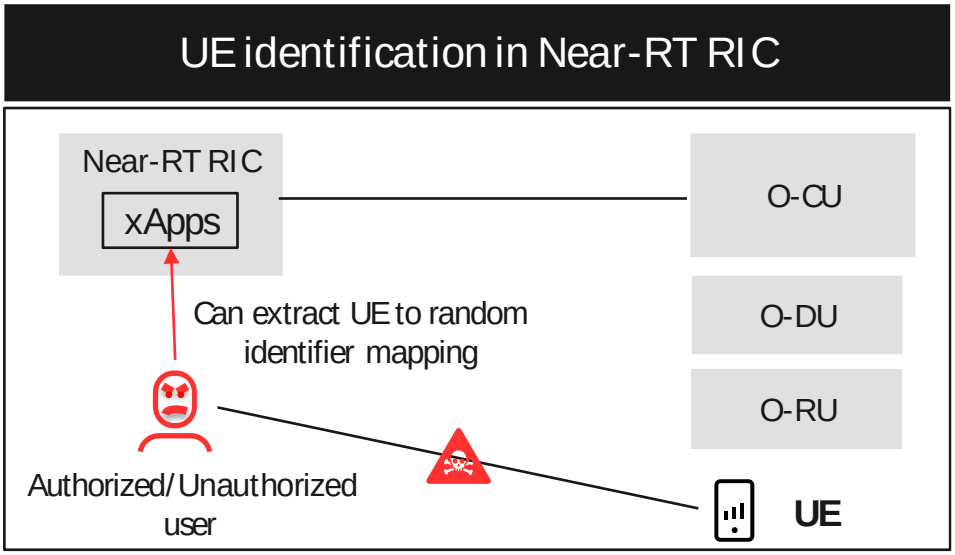

Figure 5-2 : UE Identification in Near-RT-RIC

Threat ID	T-NEAR-RT-01
Threat title	Malicious xApps can exploit UE identification, track UE location and change UE priority [12]
Threat description	xApps in the Near-RT-RIC have the capability to manipulate behavior of a certain cell, a group of UEs, and a specific UE. A malfunctioning or unavailable root of trust could potentially cause issues on the network and compromise RAN performance, privacy, etc. For example, the xApp could track a certain subscriber or impact service for a subscriber or a dedicated area. In addition, an xApp can receive order via A1 to control a certain UE and if a malfunctioning xApp receives an order to prioritize this UE, then the owner of the malfunctioning xApp knows a VIP that they want to track is in a certain area. With this command exposure, the attacker can obtain a rough location of a very important person and change the order from prioritize to deprioritize for a UE. Further, E2 interface exposes UE identification that can be exploited by a malicious xApp. As the E2 interface (similar to A1 interface) can point out a certain UE in the network, this will create a correlation between the randomized (anonymized) UE identities between the RAN nodes. For example, a xApp can potentially be used as a “sniffer” for UE identification. The additional challenge for the Near-RT RIC / E2 compared to the Non-RT RIC / A1 is that more frequent signaling is expected over the E2 interface to enable near-real-time operation. Therefore, the UE identifier will be exchanged more frequently over the E2 than over the A1.

5.4.1.5 Threats against Non-RT RIC

Threats against Non-RT RIC include:

Threat ID	T-NONRTRIC-01
Threat title	An attacker penetrates the non-RT RIC to cause a denial of service or degrade the performance
Threat description	An attacker penetrates the non-RT RIC through A1/O1 interfaces or from external sources through SMO and attempts to trigger a Denial of Service or degrade the performance of non-RT RIC so that non-RT RIC would not be liable for ensuring: • The monitoring or tracing of the network to understand the effect of the A1 policy on performance in Near-RT RIC • The update of A1 policy and E2 control or policy • The exposure and secure delivery of A1 Enrichment Information to near-RT RIC • The setup of access control rules and the selection of which Enrichment Information ID (EiId) are exposed to a near-RT RIC • The allocation of the control plane (RRC) and the user plane for different services

	• Etc.

Threat ID	T-NONRTRIC-02
Threat title	UE sniffing in the Non-RT RIC
Threat description	As the A1 interface can point out a certain UE in the network, this will create a correlation between the randomized (anonymized) UE identities between the RAN nodes. For example, a rApp can potentially be used as a "sniffer" for UE identification. The additional challenge for the Non-RT RIC / A1 is that signaling is expected over the A1 interface to enable non-real-time operation. Therefore, the UE identifier will be exchanged over the A1.

5.4.1.6 Threats against xApps

xApps introduce the following threats:

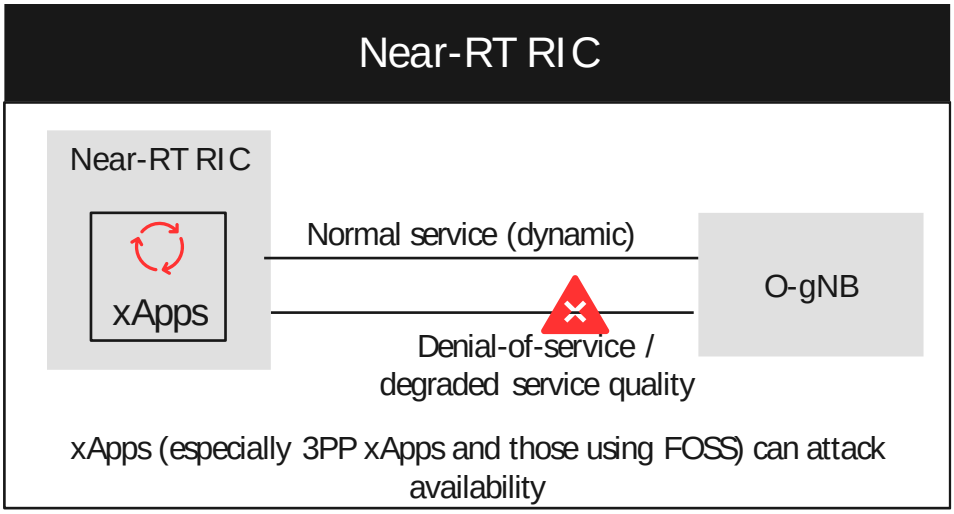

Figure 5-3 : Near-RT-RIC and xApps conflict with gNB

Threat ID	T-xApp-01
Threat title	An attacker exploits xApps vulnerabilities and misconfiguration
Threat description	Vulnerabilities can potentially exist in any xApp if it stems from an untrusted or unmaintained source. If attackers can find exploitable xApp, they can disrupt the offered network service and potentially take over another xApp or the whole near-RT RIC. The actual consequences may vary. For example, an attacker may gain the ability to alter data transmitted over A1 or E2 interfaces, extract sensitive information, etc. Malicious xApps impact near-RT RIC functions in the purpose of performance degradation, DoS, etc. xAPPs have the capability to manipulate behavior of a certain cell, a group of UEs, and a specific UE. A malfunctioning xApp could potentially track a certain subscriber or impact service for a subscriber or a dedicated area [12]

Threat ID	T-xApp-02
Threat title	Conflicting xApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS [12]

Threat description	Conflicting xApps unintentionally or maliciously impact O-RAN system functions such as mobility management, admission controls, bandwidth management and load balancing in the purpose of performance degradation. There is no clear functional split between the Near-RT RIC and the O-gNB. The functional split depends on the available xApps and the capabilities exposed by the O-gNB. This creates possible conflicts between the decisions taken by the Near-RT RIC and the O-gNB that could lead to instability in the network, which introduces vulnerabilities that could be exploited by threat actors. For example, a threat actor can utilize a malicious xApp that intentionally triggers RRM decisions conflicting with the O-gNB internal decisions to create denial of service.

Threat ID	T-xApp-03
Threat title	An attacker compromises xApp isolation
Threat description	An attacker can exploit weaknesses and vulnerabilities to compromise xApp isolation and to break out of xApp confinement. For example, attacker can use the underlying system vulnerabilities to easily breach isolation and confinement. Adversary can use side effects resulting from a shared resource usage to deduce information from co-hosted xApps. Gaining unauthorized access to the underlying system provides new opportunities to exploit vulnerabilities in other xApps or O-RAN components to intercept and spoof network traffic, to degrade services (DoS), etc.

5.4.1.7 Threats against rApps

Threats against rApps include:

Threat ID	T-rApp-01
Threat title	An attacker exploits rApps vulnerabilities and misconfiguration
Threat description	Vulnerabilities can potentially exist in any rApp if it stems from an untrusted or unmaintained source. If attackers can find exploitable rApp, they can disrupt the offered network service and potentially take over another rApp or the whole non-RT RIC. The actual consequences may vary. For example, an attacker may gain the ability to alter data transmitted over A1 interface, extract sensitive information, etc. Malicious rApps impact non-RT RIC functions such as AI/ML model training, A1 policy management, Enrichment information management, Network Configuration Optimization in the purpose of performance degradation, DoS, enrichment data sniffing (UE location, trajectory, navigation information, GPS data, etc.), etc. rApps have the capability to manipulate behavior of a certain cell, a group of UEs, and a specific UE. A malfunctioning rApp could potentially track a certain subscriber or impact service for a subscriber or a dedicated area.

Threat ID	T-rApp-02
Threat title	An attacker bypasses authentication and authorization
Threat description	Usually the rApp management is exposed to the tenant in a web front-end or REST API. In case these interfaces contain software vulnerabilities or implement authentication and authorization insufficiently, an attacker would be able to gain access to the rApp and pose as a tenant. It is also possible that an attacker gains the ability to submit requests without prior authentication and authorization in order to manipulate configurations, access logs, implement back doors, etc.

Threat ID	T-rApp-03
Threat title	An attacker compromises rApp isolation

Threat description	Adversary can exploit weaknesses and vulnerabilities to compromise rAPP isolation and to break out of rApp confinement. For example, attacker can use the underlying system vulnerabilities to easily breach isolation and confinement. Adversary can use side effects resulting from a shared resource usage to deduce information from co-hosted rApps. Gaining unauthorized access to the underlying system provides new opportunities to exploit vulnerabilities in other rApps or O-RAN components to intercept and spoof network traffic, to degrade services (DoS), etc.

Threat ID	T-rAPP-04
Threat title	Conflicting rApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS
Threat description	rApps in the Non-RT RIC can be provided by different vendors. For example, one vendor can provide the rApp for Carrier license scheduling and another vendor provide the rApp for energy saving, etc. This creates the risk that different rApps will take conflicting decisions at the same instance in time for the same user. Such conflicts between rApps include: • Direct conflicts: different rApps request change for the same parameter. • Indirect conflicts: different rApps request change to different parameters that will create opposite effects. • Implicit conflicts: different rApps request change to different parameters that are not creating any obvious opposite effect but result in an overall network performance degradation, instabilities, etc. These conflicts are difficult to mitigate since dependencies are impossible to observe.

5.4.1.8 Threats against PNF

As mentioned before in this document, the NFs could be either VNF, CNF or PNF. Vulnerabilities of a PNF could be used as a starting point for an attack against VNFs/CNFs.

Threat ID	T-PNF-01
Threat title	An attacker compromises a PNF to launch reverse attacks and other attacks against VNFs/CNFs
Threat description	A lack of security policies to protect mixed PNF-VNF/CNF deployments could be used to perform attacks against VNFs/CNFs, potentially taking advantage of legacy security used by PNFs and not provided by the virtualization/containerization layer. Attackers could use insecure interfaces as injection points and for reverse attack.

5.4.1.9 Threats against SMO

Threats against SMO include:

Threat ID	T-SMO-01
Threat title	An attacker can exploit the improper/missing authentication weakness on SMO functions
Threat description	If the authentication of O-RAN external (e.g. AI/ML, EI, Human-Machine) or internal (e.g. over O1 or O2 interfaces, with Non-RT RIC) interfaces on SMO is not supported or not properly implemented, those interfaces without legal certificates, or pre-shared key could be able to establish a TLS connection with the SMO. The data stored in the SMO may be exposed to an attacker.

Threat ID	T-SMO-02
Threat title	An attacker can exploit the improper/missing authorization weakness on SMO functions
Threat description	A malicious external (e.g. AI/ML servers, EI sources, technician) or internal (E2 nodes, Near RT-RIC, O-Cloud, Non-RT RIC) entities without authorization or with an incorrect access token may invoke the SMO functions arbitrarily. The data related to that functions will be leaked to the attacker. In addition, an attacker can be able to perform certain actions, e.g. disclose O-RAN sensitive information or alter O-RAN components.

Threat ID	T-SMO-03
Threat title	Overload DoS attacks at SMO
Threat description	Overload situation could appear in the case of DoS attack or increased traffic. Inability to deal with such events affects availability of SMO data and functions.

5.4.2 Threats against O-CLOUD

Due to O-RAN security and privacy concerns, a trust relationship must be built and maintained between the different actors involved in providing and managing the O-Cloud infrastructure. The role of trust is essential and vital to prevent or correct any potential issue that may arise from the following challenges:

- SW decoupled from dedicated HW
- Another organization may share the same HW
- 3-party organization may be managing the infrastructure
- Use of open source components

Relevant threats against O-CLOUD described in this section are selected from the following existing studies on virtualization and containerization security:

- 3GPP TS 33.818 [17]: “Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products”.
- NIST SP 800-190 - Application Container Security Guide [18]
- ENISA - Security aspects of virtualization [19]
- CSA - Best Practices for Mitigating Risks in Virtualized Environments [20]
- Fraunhofer AISEC - threat analysis of container-as-a-service for network function virtualization [21]

Five types of threats are considered:

- Compromise of VNF/CNF images and embedded secrets
- Weak orchestrator configurations, access controls and isolation
- Misuse of a VM/CN to attack other VM/CN, hypervisor/container engine, other hosts (memory, network, storage), etc.
- Spoofing and eavesdropping on network traffic to access all O-RAN network data processed in the workload
- Compromise auxiliary/supporting network services

Other threats involving the O-Cloud including hypervisor/container engine and host hardware are not considered. For an exhaustive security analysis on the virtualization/containerization technologies, please refer to the above documentation, and others.

Virtualization and containerization technologies in O-RAN introduce the following relevant threats:

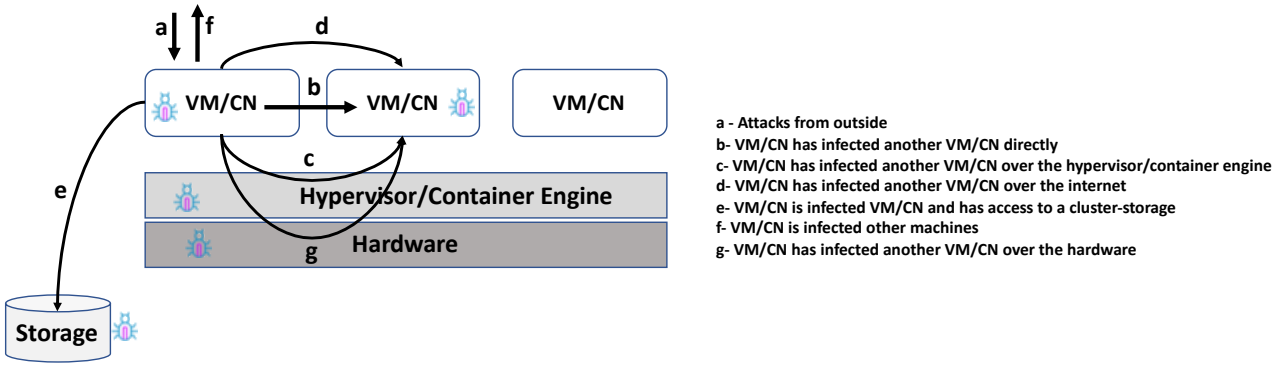

Figure 5-4 : Threats against O-Cloud

Threat ID	T-OCLOUD-01
Threat title	An attacker compromises VNF/CNF images and embedded secrets
Threat description	Because images are effectively static archive modules that include all the components used to run a given O-RAN VNF/CNF, modules within an image may be having vulnerabilities, introducing malware, missing critical security updates or are otherwise outdated. Thus, could be used to attack other VMs/CNs or hosts within the environment. In addition, images may also have configuration defects. For example, an image may not be configured with a specific user account to "run as" and thus run with greater privileges than needed. Because images are just collections of files packaged together, malicious files could be included intentionally or inadvertently within them. Thus, could be used to attack other VMs/CNs or hosts within the environment. Many O-RAN VNFs/CNFs require secrets to enable authentication, access control and secure communication between components. For example, an O-RAN VNF/CNF may need a username and password to connect to a backend server/database. Other examples of embedded secrets include connection strings, SSH private keys, and X.509 private keys. When an O-RAN VNF/CNF is packaged into an image, these secrets can be embedded directly into the image file system. However, this practice creates a security risk because anyone with access to the image can easily parse it to learn these secrets. In addition, insufficient authentication and authorization can lead to intellectual property loss and expose significant technical details about an O-RAN VNF/CNF image to an attacker. Even more critically, because registries of images are typically trusted as a source of valid, approved software, compromise of a registry can potentially lead to compromise of downstream VMs/CNs and hosts. Images often contain sensitive components like an organization's proprietary software, and embedded secrets and administrator credentials. If connections to registries are performed over insecure channels, man-in-the-middle attacks could intercept network traffic and therefore the contents integrity and confidentiality of images may be compromised. There is also an increased risk of man-in-the-middle attacks that could intercept network traffic intended for registries and steal developer or administrator credentials within that traffic. Thus, could be used to provide fraudulent or outdated images to orchestrators, etc.

Threat ID	T-OCLOUD-02
Threat title	An attacker exploits weak orchestrator configuration, access control and isolation
Threat description	A single orchestrator may run many different VMs/CNs, each managed by different teams, and with different sensitivity levels. If the access provided to users and groups is not scoped to their specific needs, a malicious or careless user could affect or subvert the operation of another VM/CN managed by the orchestrator. Malicious traffic from different VMs/CNs sharing the same virtual networks may be possible if VMs/CNs of different sensitivity levels are using the same virtual network with a poorly isolation of inter-VM/CN network traffic. For example, if VM1/CN1 is compromised, attackers may be able to use shared networks to attack VM2/CN2.The primary "data" to protect is the images and containers, which may hold app files, data files, etc. The secondary data to protect is container data within shared host resources such as memory, storage, and network interfaces. Weak orchestrator configurations can expose the orchestrator, VMs/CNs and other hosts to increased risk. Examples of possible consequences include:

	• Unauthorized hosts joining the O-CLOUD infrastructure and running VMs/CNs • The compromise of a single VM/CN host implying compromise of the entire VMs/CNs —for example, if the same key pairs used for authentication are shared across all VMs/CNs • Communications between the orchestrator, administrators, and hosts being unencrypted and unauthenticated

Threat ID	T-OCLOUD-03
Threat title	Misuse of a VM/CN to attack other VM/CN, hypervisor/container engine, other hosts (memory, network, storage), etc.
Threat description	An attacker may be able to exploit vulnerabilities to compromise the runtime VM/CN, and then alter that VM/CN so it allows the attacker to access other VMs/CNs, monitor VM/CN to VM/CN, communications, attack the O-Cloud infrastructure/services, etc. If a VM/CN is compromised and acting maliciously, it can be used to scan the network it is connected to in order to find other weaknesses for an attacker to exploit. An attacker can launch a noisy neighbor attack against the shared O-Cloud infrastructure to cause the O-RAN system performance degradation and/or its services disruption by depriving the resources required by various O-RAN running functions. Insecure VM/CN runtime configuration by the administrator can lower the security of the O-RAN system. It may expose VMs/CNs and the hypervisor/container engine to increased risk from a compromised VM/CN. For example, it could be used to elevate privileges and attack VMs/CNs, the O-Cloud infrastructure/services, etc. VMs/CNs may be compromised due to flaws in the O-RAN VNFs/CNFs they run. For example, an O-RAN VNF/CNF may be vulnerable to cross-site scripting (SQL) injection and buffer overflow vulnerabilities. An attacker hack into VM/CN, get its administrator privileges, then he can steal all tenant's token and the administrator rights of the whole O-RAN system. For example, an attacker can steal other VMs/CNs ' private key from one VM/CN.

Threat ID	T-OCLOUD-04
Threat title	Spoofing and eavesdropping on network traffic
Threat description	The container engine (in case of container) or hypervisor (in case of VM) has access to all RAM memory, disk volumes mounted on virtual machines, and containers. This means that a malicious VM/CN or hypervisor/container engine can get access to all O-RAN network data processed in the workloads. If VMs/CNs are given direct access to the underlying network stack. It allows other VMs/CNs to intercept and spoof network traffic destined for co-hosted VMs/CNs. Secondly, direct access to the underlying network would allow attackers to gain valuable information on the internal network traffic.

Threat ID	T-OCLOUD-05
Threat title	An attacker compromises auxiliary/supporting network and security services
Threat description	In addition to the main functionality of the VNF/CNF itself, administrators may deploy additional network services with their VMs/CNs. These services can be built for example to allow monitoring, remote configuration, remote access services such as SSH, etc. If these network services are directly accessible over the Internet (or from another administrator), they provide an additional entry point for attackers. For example, attackers can try to guess access credentials or exploit known vulnerabilities in the network services. Once an attacker gained access to the VM/CN through these services, additional attacks become possible.

5.4.3 Threats to open source code

Open source introduces the following threats:

Threat ID	T-OPENSRC-01
Threat title	Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack
Threat description	The O-RAN Software Community is a Linux Foundation project, supported and funded by O-RAN to lead the implementation of the O-RAN specifications in Open Source. Industry has recognized that Open Source code introduces security risks. Open Source vulnerabilities are publicly available on the National Vulnerability Database (NVD). While this is intended for developers to disclose vulnerabilities, it is also used by hackers to exploit those vulnerabilities. Vulnerabilities frequently propagate as developers re-use free open source code enabling backdoors to attacks. There have been notable vulnerabilities from downloading open source libraries and dependencies, as well as supply chain risks when downloading Open Source code from untrusted repositories. Some O-RAN vendors and operators may not have accurate inventories of open-source software dependencies used by their different applications, or a process to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open-source. Some O-RAN vendors may not have a lack of consistent Supply Chain traceability and security, and a lack of coding best practices conflicts with Security-by-Design principles. Developers may use modules with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack. Attackers can exploit a vulnerability on the open source code and infects a hypervisor, operating system, VM or container with a malware.

Threat ID	T-OPENSRC-02
Threat title	A trusted developer intentionally inserts a backdoor into an open source code O-RAN component
Threat description	A trusted developer intentionally inserts a backdoor by injecting a few lines of malicious code into an open source code component to be used within the O-RAN system. A software project team picks up and uses the infected open source code and the development team's tools for vetting and testing the component do not detect the malicious code. Unknowingly they have introduced a vulnerability into their O-RAN software code. The vulnerability has gone undetected and the threat actor is able to compromise the software through the inserted vulnerability. The resulting effect on the O-RAN system can take a variety of forms, from being annoying to impacting system performance (DoS) to the loss of sensitive data.

5.4.4 Physical Threats

The use of hardware introduces the following threats:

Threat ID	T-PHYS-01
Threat title	An intruder into a site gains physical access to O-RAN components to cause damage or access sensitive data
Threat description	Physical attacks on the O-RAN deployment that stores or processes keys, user plane data, control plane data and management data in cleartext. O-RAN physical components might be vulnerable if: • Improper physical security protection of data centers, PNFs, operation areas, etc. • Improper protection to power outages (power supply) • Improper protection against environmental disasters • Improper maintenance and monitoring of hardware parameters • Hardware backdoor Attackers try to modify the O-RAN components settings and configurations via local access. Physical access to O-RAN components thanks to unsecured management ports and consoles (such as JTAG, serial consoles or dedicated management ports), relaxed administrator credentials management, unsecured HW

	and SW configuration/management could allow an attacker to inject malwares and/or manipulate existing software, steal unprotected private keys, certificates, hash values, disable security features, create a performance issue by manipulation of parameters with the purpose of eavesdropping or wiretapping on various CUS & M planes, reaching the network beyond the O-RAN or with the purpose of gaining access to the O-RAN components, denial of service, intrusion and replay attacks or other type of breaches.

Threat ID	T-PHYS-02
Threat title	An intruder into the exchange over the Fronthaul cable network attempts to gain electronic access to cause damage or access sensitive data
Threat description	O-RU and O-DU may be located at different premises and connected through a cable network to support the fronthaul link. Attackers can gain access to, or control over, data traffic through breaching terminals in the cable landing sites (O-RU or O-DU).

5.4.5 Threats against 5G radio networks

Threats against 5G radio networks include:

Threat ID	T-RADIO-01
Threat title	Disruption through radio Jamming[1], Sniffing[2] and Spoofing[3]
Threat description	Like for any wireless technology, disruption through radio jamming is possible by analyzing the physical downlink and uplink control channels and signals. 5G radio network is vulnerable to: • Jamming Vulnerability of Reference Signals • Jamming Vulnerability of Synchronization Signal • Jamming Vulnerability of the PBCH • Sniffing and Spoofing Vulnerability of the PBCH • Jamming Vulnerability of PDCCH • Jamming Vulnerability of Physical Uplink Control Channel • Jamming Vulnerability of Physical Random-Access Channel Note: The O-RAN OEMs need to develop new intelligence that can proactively alert the operator when this attack is initiated so that the operator can take appropriate actions to mitigate. Note: In the scenario of RF spoofing, the UE needs to be able to validate the legitimacy of the O-RU as being one owned and operated by the operator. 3GPP has proposed in a study to use Digital Signatures to mitigate this threat but there has been no agreement on this to date. The O-RAN OEMs need to develop new intelligence that can proactively alert the operator when this attack is initiated so that the operator can take appropriate actions to mitigate.

Threat ID	T-RADIO-02

[1] Radio jamming is the deliberate jamming, blocking or creating interference with authorized wireless network. A radio jammer is a transmitter that tunes to the same frequency as the opponents' receiving equipment and with the same type of modulation, with enough power to override any signal at the receiver.

[2] Radio Sniffing technique helps to decode all sorts of essential network configuration details easily with low-cost software radios. Sniffing information can aid attackers in optimizing and crafting attacks.

[3] RF spoofing refers to transmitting a fake signal meant to pretense as an actual signal.

Threat title	DoS attacks on cognitive radio networks [22]
Threat description	Cognitive radio (CR) technology, which is designed to enhance spectrum utilization, depends on the success of opportunistic access, where unlicensed secondary users (SUs) exploit spectrum void unoccupied by primary users (PUs) for transmissions. To realize DoS attacks, malicious users (MUs) target the critical functionalities for CR ecosystems, including spectrum sensing, agile radio, and light-handed regulation since once these functionalities fail, SUs are not able to communicate effectively. For example, MUs can directly jam the victim by injecting interference or deceive SUs into believing that there is a PU by emulating the signal characteristics of the PU, thereby evacuating the occupied spectrum. Moreover, the liability rule is vulnerable to the selfish and greedy users aiming to maximize their own private benefits. Since complying with the rule results in less transmission opportunities, such SUs may not want to invest efforts to follow the rule and thus will transmit simultaneously with Pus.

5.4.6 Threats against ML system

This section provides the relevant threats against the ML system implemented in O-RAN architecture. The threats listed here below are generic to cover the ML model and not refined at ML components (training and inference hosts) due to the various deployment scenarios that are considered for ML architecture/framework in O-RAN. The deployment scenarios are:

1. Scenario 1.1: SMO/Non-RT RIC acts as both the ML training and inference host.
2. Scenario 1.2: Non-RT RIC acts as the ML training host and the Near-RT RIC as the ML inference host
3. Scenario 1.3: Non-RT RIC acts as the ML training host and the O-CU/O-DU as the ML inference host

The involved components and interfaces within each scenario are:

- Scenario 1.1: SMO/Non-RT RIC, Near-RT RIC, O-CU, O-DU, O-RU, SMO internal/O1/A1 interfaces
- Scenario 1.2: SMO/Non-RT RIC, Near-RT RIC, O-CU, O-DU, O-RU, O1/O2/A1/E2 interfaces
- Scenario 1.3: SMO/Non-RT RIC, O-CU, O-DU, O-RU, O1/O2 interfaces

Threat ID	T-ML-01
Threat title	Poisoning the ML training data (Data poisoning attacks)
Threat description	An attacker gains access to the training set of a machine learning model and alters the data (e.g. datasets that are assembled to train, test, and validate an ML system) before the training begins without the knowledge of the machine learning engineers. The training data will already be tampered with and has lost its original quality which will result in modeling on wrong data. Hence, the ML model will no longer be a reliable one since it was trained on bad data and therefore modelling, decisions, predictions, model classifications, detections, etc. will surely not be appropriate. Also, another scenario can be in a situation where a model is online and continues to learn during operational use, modifying its behavior over time. In this case, an attacker can feed the model with bad data and the model can learn from this bad data, and as a result, negatively impact its performance and retrain the ML system to do the wrong thing.

Threat ID	T-ML-02
Threat title	Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy)
Threat description	An attacker can illegally access a machine learning model and alter its parameters and thereby influence how it produces results. This can lead to wrong prediction and might result in catastrophic decisions if the results of the predictions were being used to make key business decisions. Also, an attacker can extract sensitive or confidential data that, through training, are built right into the ML model.

Threat ID	T-ML-03
Threat title	Transfer learning attack
Threat description on	A transfer learning attack is a risk when an ML system is built by fine-tuning a pretrained model that is widely available. An attacker could use the public model as a cover for their malicious ML behavior.

For more information about ML security risks and controls, see the risk analysis of ML systems released by BIML [23].

5.5 Coverage matrix of threats

From the above threats, a threat inventory for the O-RAN system is developed to provide a mapping between threats, vulnerabilities and assets. Threats have been grouped into two categories:

1. 'O-RAN specific' comprises threats directly relating to O-RAN components and interfaces
2. 'General' covers threats relating to physical, open source, virtualization, IoT and radio aspects

The threat inventory provides all details of each individual threat: Threat agents, vulnerabilities, threatened assets and affected components.

1

Table 5-1 : O-RAN Threat Inventory

Threat ID	Threat title	Threat agent	Vulnerability	Threatened Asset	Affected Components
O-RAN specific threats					
T-O-RAN-01	An attacker exploits insecure designs or lack of adaption in O-RAN components	All	• Outdated component from the lack of update or patch management • Poorly design architecture • Missing appropriate security hardening • Unnecessary or insecure function/protocol/component	All	All
T-O-RAN-02	An attacker exploits misconfigured or poorly configured O-RAN components	All	• Errors from the lack of configuration change management • Misconfigured or poorly configured O-RAN components • Improperly configured permissions • Unnecessary features are enabled (e.g. unnecessary ports, services, accounts, or privileges) • Default accounts and their passwords still enabled and unchanged • Security features are disabled or not configured securely	All	All
T-O-RAN-03	Attacks from the internet to penetrate O-RAN network boundary	All	Errors in the design and implementation of the network protocols (HTTP, P, TCP, UDP, application protocols)	All	All
T-O-RAN-04	An attacker attempts to jam the airlink signal through IoT devices	All	Failure to address overload situations	ASSET-D-06, ASSET-D-18	O-RU, airlink with UE, O-DU
T-O-RAN-05	An attacker penetrates and compromises the O-RAN system through the open O-RAN's Fronthaul, O1, O2, A1, and E2	All	• Improper or missing authentication and authorization processes • Improper or missing ciphering and integrity checks of sensitive data exchanged over O-RAN interfaces • Improper or missing replay protection of sensitive data exchanged over O-RAN interfaces • Improper prevention of key reuse	All	rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC
T-O-RAN-06	An attacker exploits insufficient/improper mechanisms for authentication and authorization to compromise O-RAN components	All	• Unauthenticated access to O-RAN functions • Improper authentication mechanisms • Use of Predefined/ default accounts • Weak or missing password policy • Lack of mutual authentication to O-RAN components and interfaces • Failure to block consecutive failed login attempts • Improper authorization and access control policy	All	All
T-O-RAN-07	An attacker compromises O-RAN monitoring mechanisms and log files integrity and availability	All	• Lack of security event logging • Insufficient protection of log files	ASSET-D-29	All
T-O-RAN-08	An attacker compromises O-RAN data integrity, confidentiality and traceability	All	• Improper or missing ciphering of sensitive data in storage or in transfer • Improper or missing integrity mechanisms to protect sensitive data in storage or in transfer • Presence of active function(s) that reveal confidential internal data • No traceability (logging) of access to personal data	ASSET-D-01 to ASSET-D-29	All
T-O-RAN-09	An attacker compromises O-RAN components integrity and availability	All	• Improper handling of overload situations • Unrestricted boot memory devices • Lack of / improper mechanisms for Network Product software package integrity validation	ASSET-C-01 to ASSET-C-12	All
T-FRHAUL-01	An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface	All	Heterogeneous security levels between O-RU and O-DU provided by different vendors	ASSET-D-01, ASSET-D-02, ASSET-D-04, ASSET-D-05	rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC
T-MPLANE-01	An attacker attempts to intercept the Fronthaul (MITM) over M Plane	All	Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements	ASSET-D-02, ASSET-D-03	Near-RT RIC, Non-RT RIC, O-CU, O-DU, SMO
T-SPLANE-01	DoS attack against a Master clock	All	• Improper process to monitor and manage the performance of the Master clock • ANNOUNCE messages can be sent publicly in clear text	ASSET-D-01	O-DU, O-RU

Threat ID	Threat title	Threat agent	Vulnerability	Threatened Asset	Affected Components
T-SPLANE-02	MITM random delay attack against selective PTP messages	All	• Inaccurate timing information • Improper synchronization between clocks • ANNOUNCE messages can be sent publicly in clear text	ASSET-D-01	O-DU, O-RU
T-CPLANE-01	Spoofing of DL/UL C-plane messages	All	Lack of authentication could allow an adversary to inject own DL/UL C-plane messages	ASSET-D-04	O-DU, O-RU
T-CPLANE-02	DoS Attack against O-DU C-plane	All	Clear-text nature of eCPRI messages used for the Open Fronthaul C-Plane	ASSET-D-04	O-DU, O-RU
T-UPLANE-01	An attacker attempts to intercept the Fronthaul (MITM) over U Plane	All	Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements	ASSET-D-05	O-DU, O-RU
T-ORU-01	An attacker stands up a rogue O-RU	All	False O-RUs	ASSET-D-06, ASSET-D-18, ASSET-D-22	O-RU
T-NEAR-RT-01	Malicious Apps can exploit UE identification, track UE location and change UE priority	All	Malicious xApps may be used to gain access to UE identification location and priority	ASSET-D-21, ASSET-D-22	Near-RT RIC, UE, xApps
T-NONRTRIC-01	An attacker penetrates the non-RT RIC to cause a denial of service or degrade the performance	All	Improper or missing authentication and authorization processes on the Non-RT RIC or SMO	ASSET-D-03, ASSET-D-07, ASSET-D-08	Non-RT RIC, rApps
T-NONRTRIC-02	UE sniffing in the Non-RT RIC	All	Malicious rApps may be used to gain access to UE identification	ASSET-D-21, ASSET-D-22	Non-RT RIC, rApps, UE
T-xAPP-01	An attacker exploits xApps vulnerabilities and misconfiguration	All	xApp stems from an untrusted or unmaintained source	ASSET-C-03, ASSET-C-07, ASSET-C-08, ASSET-C-09, ASSET-C-10	O-CU, Near-RT RIC, xApps
T-xAPP-02	Conflicting xApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS	All	• xApps may be misconfigured or compromised • Failing or misconfigured authentication and authorization in xApp	ASSET-C-03, ASSET-C-07, ASSET-C-08, ASSET-C-09, ASSET-C-10	O-CU, Near-RT RIC, xApps
T-xAPP-03	An attacker compromises xApp isolation	All	Vulnerabilities in the underlying system hosting xApps	ASSET-C-03, ASSET-C-07, ASSET-C-08, ASSET-C-09, ASSET-C-10	O-CU, Near-RT RIC, xApps
T-rAPP-01	An attacker exploits rApps vulnerabilities and misconfiguration	All	rApp stems from an untrusted or unmaintained source	ASSET-D-03, ASSET-D-07, ASSET-D-08, ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28	rApps, UE, Non-RT RIC, Near-RT RIC, xApps
T-rAPP-02	An attacker bypasses authentication and authorization	All	rApp management is exposed to the tenant in a web front-end or REST API. These interfaces may contain software vulnerabilities or implement authentication and authorization insufficiently.	ASSET-D-03, ASSET-D-07, ASSET-D-08, ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28	rApps, Non-RT RIC, Near-RT RIC, xApps
T-rAPP-03	An attacker compromises rApp isolation	All	Vulnerabilities in the underlying system hosting rApps	ASSET-D-03, ASSET-D-07, ASSET-D-08, ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28	rApps, Non-RT RIC, Near-RT RIC, xApps
T-rAPP-04	Conflicting rApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS	All	• rApps may be misconfigured or compromised • Failing or misconfigured authentication and authorization in rApp	ASSET-D-03, ASSET-D-07, ASSET-D-08, ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28	rApps, Non-RT RIC, Near-RT RIC, xApps
T-PNF-01	An attacker compromises a PNF to launch reverse attacks and other attacks against VNFs/CNFs	All	Mixed PNF-VNF/CNF deployments	All	All
T-SMO-01	An attacker can exploit the improper/missing authentication weakness on SMO functions	All	Improper/missing authentication on SMO functions	ASSET-D-02, ASSET-D-03, ASSET-D-07, ASSET-D-08, ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-16, ASSET-D-17, ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28; ASSET-D-20, ASSET-D-30	All
T-SMO-02	An attacker can exploit the improper/missing authorization weakness on SMO functions	All	Improper/missing authorization on SMO functions	ASSET-D-02, ASSET-D-03, ASSET-D-07, ASSET-D-08, ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-16, ASSET-D-17, ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28; ASSET-D-20, ASSET-D-30	All
T-SMO-03	Overload DoS attacks at SMO	All	Failure to address overload situation	ASSET-D-02, ASSET-D-03, ASSET-D-07, ASSET-D-08, ASSET-D-12, ASSET-D-13,	SMO

Threat ID	Threat title	Threat agent	Vulnerability	Threatened Asset	Affected Components
				ASSET-D-14, ASSET-D-16, ASSET-D-17, ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28; ASSET-D-20, ASSET-D-30	
General threats					
T-OCLOUD-01	An attacker compromises VNF/CNF images and embedded secrets	All	Images may introduce malware, missing critical security updates or are otherwise outdated, configuration defects, insufficient authentication and authorization, lack of or insufficient cryptographic protection	ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-20, ASSET-D-23	O-Cloud
T-OCLOUD-02	An attacker exploits weak orchestrator configuration, access control and isolation	All	• VMs/CNs of different sensitivity levels are using the same virtual network with a poorly isolation of inter-VM/CN network traffic • Weak orchestrator configurations	ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-24, ASSET-D-29	All
T-OCLOUD-03	Misuse of a VM/CN to attack other VM/CN, hypervisor/container engine, other hosts (memory, network, storage), etc.	All	• Compromised VM/CN • Insecure VM/CN runtime configuration • Flaws in the O-RAN VNFs/CNFs	ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-24, ASSET-D-29	All
T-OCLOUD-04	Spoofing and eavesdropping on network traffic	All	Malicious VM/CN or hypervisor/container engine	ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-24, ASSET-D-29	All
T-OCLOUD-05	An attacker compromises auxiliary/supporting network and security services	All	Insecure authentication to auxiliary/supporting network and security services	ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-24, ASSET-D-29	All
T-OPENSRC-01	Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	All	• Inaccurate inventories of open-source software • Lack of consistent Supply Chain traceability and security • Lack of coding best practices • Modules with known vulnerabilities and untrusted libraries	All	All
T-OPENSRC-02	A trusted developer intentionally inserts a backdoor into an open source code O-RAN component	All	Bugs in open source software caused by mistakes and human error	All	All
T-PHYS-01	An intruder into a site gains physical access to O-RAN components to cause damage or access sensitive data	All except Script kiddies	• Improper physical security protection of data centres, PNFs, operation areas, etc. • Improper protection to power outages (power supply) • Improper protection against environmental disasters • Improper maintenance and monitoring of hardware parameters • Hardware backdoor	All	All
T-PHYS-02	An intruder into the exchange over the Fronthaul cable network attempts to gain electronic access to cause damage or access sensitive data	All except Script kiddies	Physical access to the open Fronthaul cable network	ASSET-D-01, ASSET-D-02, ASSET-D-04, ASSET-D-05	O-RU, O-DU
T-RADIO-01	Disruption through radio jamming, sniffing and spoofing	All except Script kiddies	Weakness of wireless cellular communications	ASSET-D-06	UE, O-RU, O-DU
T-RADIO-02	DoS attacks on cognitive radio networks	All except Script kiddies	Weakness of wireless cellular communications	ASSET-D-06	UE, O-RU, O-DU
T-ML-01	Poisoning the ML training data (Data poisoning attacks)	All	Lack of or improper access control to the ML model	ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28	Near-RT RIC, Non-RT RIC, xAPPs, rApps
T-ML-02	Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy)	All	Lack of or improper access control to the ML model	ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28	Near-RT RIC, Non-RT RIC, xAPPs, rApps
T-ML-03	Transfer learning attack	All	Use of pretrained public ML model	ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28	Near-RT RIC, Non-RT RIC, xAPPs, rApps

1

Chapter 6 Security principles

This chapter consists of a set of security principles that the O-RAN system should achieve. They provide high level and abstract statement of the intended solution to countering potential Threats. In the future, this chapter is expected to be normative, therefore these security principles will be developed and refined into security requirements, recommendations and potential countermeseares in order to clearly identify what is required (SHALL), recommended (SHOULD) or optional (MAY). In the current version, only 'SHOULD' is used within the security principles to make recommendations.

6.1 Principles (SP)

6.1.1 SP-AUTH Mutual Authentication

- Mutual authentication SHOULD be established to allow the O-RAN system verifying who performs what, thus possible to detect fake base stations, unauthorized or malicious components, malicious applications and malicious users/administrators. To authenticate each component, a unique identifier and one or more credentials that SHOULD be kept secret are needed.

6.1.2 SP-ACC Access Control

- The O-RAN system SHOULD forbid unauthorized administrators or components to access O-RAN resources or services anytime and anywhere. Access controls are required for:
    - Network Access Controls for filtering unauthorized/unexpected traffic in the O-RAN components over their interfaces.
    - Access controls to restrict access to component configurations.
    - Access controls for hardware to maintain the trust chain.

6.1.3 SP-CRYPTO Secure cryptographic, key management and PKI

- Well-known, standardized, secure and unbroken cryptographic schemes and protocols SHOULD be used. Proprietary schemes and protocols SHOULD be avoided.
- A secure key management of O-RAN keys (KgNB, KRRC-enc, KRRC-int, KUP-int, and KUP-enc, ksn) SHOULD be implemented to manage all the steps of key lifecycle: key generation using an appropriate level of entropy from a reliable source, secure key storage, key rotation and revocation, secure key destruction, etc.
- Reliable PKI for authentication and data encryption SHOULD be used. Public CAs SHOULD be supported. The certificates SHOULD be issued by a trusted or rooted Certificate Authority (CA). The CA implements the Certificate Policy which specifies the rules and policies about who may or may not receive a Certificate. Relying parties can access the Certificate Policy to determine what validation/verification checks were performed prior to certificate issuance.
- Each O-RU SHOULD be configured with lists of algorithms which are allowed for usage. There SHOULD be one list for integrity algorithms, and one for ciphering algorithms. These lists SHOULD be ordered according to a priority decided by the operator.

6.1.4 SP-TCOMM Trusted Communication

- Integrity, confidentiality, availability, authenticity and replay protection of resources SHOULD be ensured in transit (see 'Critical Assets) over O-RAN interfaces according to industry best practices.

6.1.5 SP-SS Secure storage

- Integrity, confidentiality, availability protection of resources SHOULD be ensured at rest (see 'Critical Assets) according to industry best practices. Special attention SHOULD be paid to the protection of private keys, certificates and hash-values at rest.

6.1.6 SP-SB Secure boot and self-configuration

- O-RAN components SHOULD secure their underlying firmware and configuration to provide the opportunity for trust to be extended higher in the software stack. Verified platform firmware can, in turn, verify the operating system (OS) boot loader, which can then verify other software components all the way up to the OS itself, the hypervisor or container runtime layers and O-RAN components. The transitive trust SHOULD be consistent with the concept of the chain of trust (CoT)-a method where each piece of code in the boot process measures and checks the signature of the next stage of the boot process before the software boots.

- The secure boot process, signature verification and self-configuration SHOULD be securely and properly implemented for all O-RAN components to authenticate them before loading.

6.1.7 SP-UPDT Secure Update

- A secure update management process SHOULD be implemented for introducing a new component or software change into the O-RAN system. The process SHOULD consider the ability to update the cryptographic algorithms and to adapt to upcoming O-RAN security challenges. O-RAN vendors SHOULD constantly provide ongoing security monitoring and patches for all of O-RAN components. A timely update cycles if vulnerabilities are discovered SHOULD be in place.

6.1.8 SP-RECO Recoverability & Backup

- Recoverability process in terms of the capacity of recovery in case of denial of service SHOULD be implemented. An approach for detecting and mitigating DoS attacks SHOULD be in place.

- O-RAN vendors SHOULD define a recovery plan that resets the O-RAN components to a trustworthy state in case of a malfunction or an attack (e.g. DoS).

- Backup systems SHOULD be in place to allow data or component on the O-RAN to be secured. Backup systems SHOULD ensure a suitable level of data or component availability and reliability.

6.1.9 SP-OPNS Security management of risks in open source components

- Vendors using open source code SHOULD enhance its security by applying industry coding best practices. It is recommended that vendors practice a higher level of due diligence for exposure to public exploits when using Open Source code.

- A Software Bill of Materials (SBOM) SHOULD be maintained to understand which open source components are in use and where.

- Security Analysis (Audit, vulnerability scan, etc.) SHOULD be performed to ensure all identified components are free of security vulnerabilities.

- Because of the pull operation mode of the open source software, a proper policy and process SHOULD be in place for identifying and patching known issues with the open source components. Open source software components SHOULD be kept up to date and patched.

6.1.10 SP-ASSU Security Assurance

- Mobile networks are classified as critical infrastructure making security assurance especially more than relevant:

- Vendors SHOULD ensure and prove that its software or hardware meets 3GPP Security Assurance Specifications (SCAS).
- Vendors SHOULD ensure and prove that its software or hardware fulfils O-RAN security tests, requirements and recommendations provided by O-RAN alliance.
- Vendors SHOULD ensure and prove that their software or hardware meets the needs of many national and international cybersecurity regulations, such as the Cyber Act, GDPR, etc.
- Vendors SHOULD provide risk assessment, secure code review, penetration testing, vulnerability analysis and hardening guidelines for their O-RAN components.

6.1.11 SP-PRV Privacy

- In O-RAN, the privacy of end users SHOULD be considered. The privacy of end users can be divided into data privacy, identity privacy and personal information privacy. Most Communication services are to gather data and personal information around end users themselves, which may reveal information sensitive to their privacy. Adversaries would further extract more personal information about end users, such as UE priority, location information, trajectory, and preference.

6.1.12 SP-SLC Continuous security development, testing, logging, monitoring and vulnerability handling

- Continuous development and continuous integration (CD/CI) with continuous regression testing and software security auditing SHOULD be implemented.
- Relevant activities events SHOULD be logged and logs collected SHOULD be analyzed in real time for the identification of potential security attacks and for security auditing.
- Continuous monitoring SHOULD be implemented to verify that the wanted security state is maintained throughout the lifecycle of deployed O-RAN components.
- Vulnerability management SHOULD be in place with intelligence to continuously track, identify and remediate vulnerable applications. Vendors SHOULD keep track of any new vulnerabilities discovered and is ready to act on customer product security incidents and reported security issues affecting O-RAN components.

6.1.13 SP-ISO Robust Isolation

- In a multi-vendor environment, intra-domain host isolation SHOULD be enforced. In the same host, VMs, CNs, virtualization/container layer, CPU, storage, and network security isolation of resources SHOULD be ensured by implementing system security orchestration, segmentation, lifecycle management, time scheduling, monitoring and audit on the management, signaling, control and data planes, and the execution of virtualized O-RAN components.

6.1.14 SP-PHY Physical security

- The O-RAN system SHOULD be located at physically secure environment in a way that minimizes the risk of resource theft and destruction. It SHOULD support secure storage of sensitive data (cryptographic keys and configuration data), execution of sensitive functions (encryption/decryption, authentication), and execution of boot and update processes.
- Special attention SHOULD be paid to the site intrusion and physical access threats against O-RU sites. Consequently O-RU equipment SHOULD disable all unnecessary physical and logical ports, protocols and interfaces. In addition, secure physical connections to O-RU for O&M operations SHOULD be implemented (e.g. secure laptop with secure credentials).

6.1.15 SP-CLD Secure cloud computing and virtualization

- Defense methods SHOULD be implemented: virtual machine-based intrusion detection, virtual machine-based isolation, virtual machine-based kernel protection, virtual machine-based access control, and virtual machine-based trusted computing.

- To get a fully trusted virtualized application, all the layers in the stack from hardware to firmware to virtualized software SHOULD be trust, as it is impossible to protect a virtual machine or containers from the host system.

6.1.17 SP-ROB Robustness

- The O-RAN system SHOULD not only ensure the robustness of software or hardware resources, but also guarantee the robustness of the cognitive radio channel for meeting the QoS of communication services required by users. In some scenarios, the robustness of spectrum sensing SHOULD be enhanced when some sensing nodes (e.g. O-RU) are easily malfunctioned. Robustness is an essential consideration for overcoming the security threats caused by jamming, DoS or DDoS attacks.

6.2 Coverage Threats - Security principles

The table below illustrates how threats are covered by security principles. It outlines the list of security principles contributing to counter threats.

1 **Table 6-1 : Coverage Security principles-Threats**

SR	Threats																																											
	T-O-RAN-01	T-O-RAN-02	T-O-RAN-03	T-O-RAN-04	T-O-RAN-05	T-O-RAN-06	T-O-RAN-07	T-O-RAN-08	T-O-RAN-09	T-FRHAUL-01	T-MPLANE-01	T-SPLANE-01	T-SPLANE-02	T-CPLANE-01	T-CPLANE-02	T-UPLANE-01	T-ORU-01	T-NEAR-RT-01	T-NONRTRIC-01	T-NONRTRIC-02	T-xAPP-01	T-xAPP-02	T-xAPP-03	T-rAPP-01	T-rAPP-02	T-rAPP-03	T-rAPP-04	T-PNF-01	T-SMO-01	T-SMO-02	T-SMO-03	T-OCLOUD-01	T-OCLOUD-02	T-OCLOUD-03	T-OCLOUD-04	T-OCLOUD-05	T-OPENSRC-01	T-OPENSRC-02	T-PHYS-01	T-PHYS-02	T-RADIO-01	T-RADIO-02	T-ML-01	T-ML-02	T-ML-03
SP-AUTH			x			x				x	x	x	x	x	x	x			x		x	x	x	x	x	x	x		x			x	x	x	x	x							x	x	x
SP-ACC			x			x				x	x	x	x	x	x	x			x		x	x	x	x	x	x	x			x		x	x	x	x	x							x	x	x
SP-CRYPTO		x	x		x	x		x		x	x	x	x	x	x	x	x		x		x	x	x	x	x	x	x					x	x	x	x	x							x	x	x
SP-TCOMM					x			x		x	x	x	x	x	x	x	x																												
SP-SS							x	x																								x	x	x	x	x									
SP-SB		x																x		x	x	x	x	x	x	x	x	x				x	x	x	x	x							x	x	x
SP-UPDT	x																				x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x					x	x	x
SP-RECO				x					x												x	x	x	x	x	x	x				x	x	x	x	x	x							x	x	x
SP-OPNS									x									x		x												x	x	x	x	x	x	x							
SP-ASSU	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
SP-PRV								x										x		x																									
SP-SLC	x						x		x									x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x					x	x	x
SP-ISO		x																x		x	x	x	x	x	x	x	x					x	x	x	x	x							x	x	x
SP-PHY									x								x											x											x	x					
SP-CLD																		x		x	x	x	x	x	x	x	x					x	x	x	x	x							x	x	x
SP-ROB				x																																					x	x			

2

Note: In next future versions, this document will be consolidated and completed with

- Security requirements, countermeasures and recommendations,
- A risk assessment will be applied on some use cases defined by O-RAN.

Annex ZZZ : O-RAN Adopter License Agreement

BY DOWNLOADING, USING OR OTHERWISE ACCESSING ANY O-RAN SPECIFICATION, ADOPTER AGREES TO THE TERMS OF THIS AGREEMENT.

This O-RAN Adopter License Agreement (the "Agreement") is made by and between the O-RAN ALLIANCE and the entity that downloads, uses or otherwise accesses any O-RAN Specification, including its Affiliates (the "Adopter").

This is a license agreement for entities who wish to adopt any O-RAN Specification.

Section 1: DEFINITIONS

1.1 "Affiliate" means an entity that directly or indirectly controls, is controlled by, or is under common control with another entity, so long as such control exists. For the purpose of this Section, "Control" means beneficial ownership of fifty (50%) percent or more of the voting stock or equity in an entity.

1.2 "Compliant Implementation" means any system, device, method or operation (whether implemented in hardware, software or combinations thereof) that fully conforms to a Final Specification.

1.3 "Adopter(s)" means all entities, who are not Members, Contributors or Academic Contributors, including their Affiliates, who wish to download, use or otherwise access O-RAN Specifications.

1.4 "Minor Update" means an update or revision to an O-RAN Specification published by O-RAN ALLIANCE that does not add any significant new features or functionality and remains interoperable with the prior version of an O-RAN Specification. The term "O-RAN Specifications" includes Minor Updates.

1.5 "Necessary Claims" means those claims of all present and future patents and patent applications, other than design patents and design registrations, throughout the world, which (i) are owned or otherwise licensable by a Member, Contributor or Academic Contributor during the term of its Member, Contributor or Academic Contributorship; (ii) such Member, Contributor or Academic Contributor has the right to grant a license without the payment of consideration to a third party; and (iii) are necessarily infringed by a Compliant Implementation (without considering any Contributions not included in the Final Specification). A claim is necessarily infringed only when it is not possible on technical (but not commercial) grounds, taking into account normal technical practice and the state of the art generally available at the date any Final Specification was published by the O-RAN ALLIANCE or the date the patent claim first came into existence, whichever last occurred, to make, sell, lease, otherwise dispose of, repair, use or operate a Compliant Implementation without infringing that claim. For the avoidance of doubt in exceptional cases where a Final Specification can only be implemented by technical solutions, all of which infringe patent claims, all such patent claims shall be considered Necessary Claims.

1.6 "Defensive Suspension" means for the purposes of any license grant pursuant to Section 3, Member, Contributor, Academic Contributor, Adopter, or any of their Affiliates, may have the discretion to include in their license a term allowing the licensor to suspend the license against a licensee who brings a patent infringement suit against the licensing Member, Contributor, Academic Contributor, Adopter, or any of their Affiliates.

Section 2: COPYRIGHT LICENSE

2.1 Subject to the terms and conditions of this Agreement, O-RAN ALLIANCE hereby grants to Adopter a nonexclusive, nontransferable, irrevocable, non-sublicensable, worldwide copyright license to obtain, use and modify O-RAN Specifications, but not to further distribute such O-RAN Specification in any modified or unmodified way, solely in furtherance of implementations of an O-RAN Specification.

2.2 Adopter shall not use O-RAN Specifications except as expressly set forth in this Agreement or in a separate written agreement with O-RAN ALLIANCE.

Section 3: FRAND LICENSE

3.1 Members, Contributors and Academic Contributors and their Affiliates are prepared to grant based on a separate Patent License Agreement to each Adopter under Fair Reasonable And Non- Discriminatory (FRAND) terms and conditions with or without compensation (royalties) a nonexclusive, non-transferable, irrevocable (but subject to Defensive Suspension), non-sublicensable, worldwide patent license under their Necessary Claims to make, have made, use, import, offer to sell, lease, sell and otherwise distribute Compliant Implementations; provided, however, that such license shall not extend: (a) to any part or function of a product in which a Compliant Implementation is incorporated that is not itself part of the Compliant Implementation; or (b) to any Adopter if that Adopter is not making a reciprocal

grant to Members, Contributors and Academic Contributors, as set forth in Section 3.3. For the avoidance of doubt, the foregoing licensing commitment includes the distribution by the Adopter's distributors and the use by the Adopter's customers of such licensed Compliant Implementations.

3.2 Notwithstanding the above, if any Member, Contributor or Academic Contributor, Adopter or their Affiliates has reserved the right to charge a FRAND royalty or other fee for its license of Necessary Claims to Adopter, then Adopter is entitled to charge a FRAND royalty or other fee to such Member, Contributor or Academic Contributor, Adopter and its Affiliates for its license of Necessary Claims to its licensees.

3.3 Adopter, on behalf of itself and its Affiliates, shall be prepared to grant based on a separate Patent License Agreement to each Members, Contributors, Academic Contributors, Adopters and their Affiliates under Fair Reasonable And Non-Discriminatory (FRAND) terms and conditions with or without compensation (royalties) a nonexclusive, non-transferable, irrevocable (but subject to Defensive Suspension), non-sublicensable, worldwide patent license under their Necessary Claims to make, have made, use, import, offer to sell, lease, sell and otherwise distribute Compliant Implementations; provided, however, that such license will not extend: (a) to any part or function of a product in which a Compliant Implementation is incorporated that is not itself part of the Compliant Implementation; or (b) to any Members, Contributors, Academic Contributors, Adopters and their Affiliates that is not making a reciprocal grant to Adopter, as set forth in Section 3.1. For the avoidance of doubt, the foregoing licensing commitment includes the distribution by the Members', Contributors', Academic Contributors', Adopters' and their Affiliates' distributors and the use by the Members', Contributors', Academic Contributors', Adopters' and their Affiliates' customers of such licensed Compliant Implementations.

Section 4: TERM AND TERMINATION

4.1 This Agreement shall remain in force, unless early terminated according to this Section 4.

4.2 O-RAN ALLIANCE on behalf of its Members, Contributors and Academic Contributors may terminate this Agreement if Adopter materially breaches this Agreement and does not cure or is not capable of curing such breach within thirty (30) days after being given notice specifying the breach.

4.3 Sections 1, 3, 5 - 11 of this Agreement shall survive any termination of this Agreement. Under surviving Section 3, after termination of this Agreement, Adopter will continue to grant licenses (a) to entities who become Adopters after the date of termination; and (b) for future versions of O-RAN Specifications that are backwards compatible with the version that was current as of the date of termination.

Section 5: CONFIDENTIALITY

Adopter will use the same care and discretion to avoid disclosure, publication, and dissemination of O-RAN Specifications to third parties, as Adopter employs with its own confidential information, but no less than reasonable care. Any disclosure by Adopter to its Affiliates, contractors and consultants should be subject to an obligation of confidentiality at least as restrictive as those contained in this Section. The foregoing obligation shall not apply to any information which is: (1) rightfully known by Adopter without any limitation on use or disclosure prior to disclosure; (2) publicly available through no fault of Adopter; (3) rightfully received without a duty of confidentiality; (4) disclosed by O-RAN ALLIANCE or a Member, Contributor or Academic Contributor to a third party without a duty of confidentiality on such third party; (5) independently developed by Adopter; (6) disclosed pursuant to the order of a court or other authorized governmental body, or as required by law, provided that Adopter provides reasonable prior written notice to O-RAN ALLIANCE, and cooperates with O-RAN ALLIANCE and/or the applicable Member, Contributor or Academic Contributor to have the opportunity to oppose any such order; or (7) disclosed by Adopter with O-RAN ALLIANCE's prior written approval.

Section 6: INDEMNIFICATION

Adopter shall indemnify, defend, and hold harmless the O-RAN ALLIANCE, its Members, Contributors or Academic Contributors, and their employees, and agents and their respective successors, heirs and assigns (the "Indemnitees"), against any liability, damage, loss, or expense (including reasonable attorneys' fees and expenses) incurred by or imposed upon any of the Indemnitees in connection with any claims, suits, investigations, actions, demands or judgments arising out of Adopter's use of the licensed O-RAN Specifications or Adopter's commercialization of products that comply with O-RAN Specifications.

Section 7: LIMITATIONS ON LIABILITY; NO WARRANTY

EXCEPT FOR BREACH OF CONFIDENTIALITY, ADOPTER'S BREACH OF SECTION 3, AND ADOPTER'S INDEMNIFICATION OBLIGATIONS, IN NO EVENT SHALL ANY PARTY BE LIABLE TO ANY OTHER PARTY OR THIRD PARTY FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES RESULTING FROM ITS PERFORMANCE OR NON-PERFORMANCE UNDER THIS AGREEMENT, IN EACH CASE WHETHER UNDER CONTRACT, TORT, WARRANTY, OR OTHERWISE, AND WHETHER OR NOT SUCH PARTY HAD ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. O-RAN SPECIFICATIONS ARE PROVIDED "AS IS" WITH NO WARRANTIES OR CONDITIONS WHATSOEVER, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. THE O-RAN ALLIANCE AND THE MEMBERS, CONTRIBUTORS OR ACADEMIC CONTRIBUTORS EXPRESSLY DISCLAIM ANY WARRANTY OR CONDITION OF MERCHANTABILITY, SECURITY, SATISFACTORY QUALITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, ERROR-FREE OPERATION, OR ANY WARRANTY OR CONDITION FOR O-RAN SPECIFICATIONS.

Section 8: ASSIGNMENT

Adopter may not assign the Agreement or any of its rights or obligations under this Agreement or make any grants or other sublicenses to this Agreement, except as expressly authorized hereunder, without having first received the prior, written consent of the O-RAN ALLIANCE, which consent may be withheld in O-RAN ALLIANCE's sole discretion. O-RAN ALLIANCE may freely assign this Agreement.

Section 9: THIRD-PARTY BENEFICIARY RIGHTS

Adopter acknowledges and agrees that Members, Contributors and Academic Contributors (including future Members, Contributors and Academic Contributors) are entitled to rights as a third-party beneficiary under this Agreement, including as licensees under Section 3.

Section 10: BINDING ON AFFILIATES

Execution of this Agreement by Adopter in its capacity as a legal entity or association constitutes that legal entity's or association's agreement that its Affiliates are likewise bound to the obligations that are applicable to Adopter hereunder and are also entitled to the benefits of the rights of Adopter hereunder.

Section 11: GENERAL

This Agreement is governed by the laws of Germany without regard to its conflict or choice of law provisions.

This Agreement constitutes the entire agreement between the parties as to its express subject matter and expressly supersedes and replaces any prior or contemporaneous agreements between the parties, whether written or oral, relating to the subject matter of this Agreement.

Adopter, on behalf of itself and its Affiliates, agrees to comply at all times with all applicable laws, rules and regulations with respect to its and its Affiliates' performance under this Agreement, including without limitation, export control and antitrust laws. Without limiting the generality of the foregoing, Adopter acknowledges that this Agreement prohibits any communication that would violate the antitrust laws.

By execution hereof, no form of any partnership, joint venture or other special relationship is created between Adopter, or O-RAN ALLIANCE or its Members, Contributors or Academic Contributors. Except as expressly set forth in this Agreement, no party is authorized to make any commitment on behalf of Adopter, or O-RAN ALLIANCE or its Members, Contributors or Academic Contributors.

In the event that any provision of this Agreement conflicts with governing law or if any provision is held to be null, void or otherwise ineffective or invalid by a court of competent jurisdiction, (i) such provisions will be deemed stricken from the contract, and (ii) the remaining terms, provisions, covenants and restrictions of this Agreement will remain in full force and effect.

Any failure by a party or third party beneficiary to insist upon or enforce performance by another party of any of the provisions of this Agreement or to exercise any rights or remedies under this Agreement or otherwise by law shall not be construed as a waiver or relinquishment to any extent of the other parties' or third party beneficiary's right to assert or rely upon any such provision, right or remedy in that or any other instance; rather the same shall be and remain in full force and effect.