5G OPERA

5G-OPERA Deliverable 3.3

Definition of Requirements for Open RAN Solutions

Document Properties	
Nom du projet :	5G-OPERA
Titre du document :	Definition of Requirements for Open RAN Solutions
Donneur d'ordre :	Ministère de l'économie, des finances, et de la relance, Bundesministerium für Wirtschaft und Energie
Référence officielle :	5G-OPERA D3.3
Relecteur :	Florian Kaltenberger, Thomas Höschele
Résumé :	
Date de publication :	10/02/2023
Version :	1.0
Accès :	Public
Mots clés :	Open RAN, 5G Private Networks, Requirements

Executive Summary

Within the 5G-OPERA project, German and French partners cooperate to develop a technological ecosystem for open Radio Access Networks (RAN) for private networks. This report explains the requirements of open RAN. The report starts with an introduction in Section 1.

Section 2 explains what are the vulnerabilities of open RAN network functions as well as how disaggregation of the open RAN has advantage on the security. Then, the risks are categorized in high, medium and low according to the how likely they occur. Then security testing examples are introduced. Then, the required threat mitigation examples have been presented. Afterwards, security assessment requirements and security test assessment methodologies for 5G-OPERA project has been explained. Finally, it is concluded with the idea of bringing together the security specifications from 3GPP and O-RAN standardization bodies.

Section 3 explains the requirement of time, frequency and phase synchronization of the fronthaul network: the network between Distributed Units (O-DU) and Radio Units (O-RU). More specifically, the configuration for LLS-C3 will be supported in the project. Finally, the required standards for synchronization are listed.

Section 4 and 5 present the hardware and software requirements specified by O-RAN Alliance. These requirements can be reference for the 5G-OPERA project. Particularly, for software point of view, the developed components from WP4 and WP5 can be delivered as a container image. Moreover, a possible solution for network management has been proposed, i.e., Open Network Automation Platform (ONAP).

Section 6 lists the requirements for hardware Acceleration Abstraction Layer (AAL) These requirements derived from O-RAN Alliance specifications.

Section 7 gives information about limit of performance related requirements, e.g., latency, bandwidth, and reliability derived from presentations done by demonstration project partners. These performance requirements vary according to the different use cases.

Section 8 explains the localization requirements for RAN side. The method intended to be used is Uplink- Time Difference of Arrival (UL-TDoA) based on Sounding Reference Signals (SRS). For localization, at least 4 synchronized gNB units are needed. Furthermore, the protocol and procedure for synchronization has been illustrated.

Section 9 introduce the TSN requirements in the RAN side, while section 10 summarizes and concludes the report.

Table of Contents

Abbreviations

OSM	OPERA Security Model
OSSM	OPERA Soundness Security Model
3GPP	Third Generation Partnership Project
SECAM	Security Assurance Methodology
RAN	Radio Access Networks
SFG	Security Forcing Group
WGs	Working Groups
NIST	National Institute Standards and Technology
AI	Artificial Intelligence
IoT	Internet of Things
STG	Security Task Group
LLS	Lower Layer Split
RIC	Radio Intelligent Controller
ML	Machine Learning
CIS	Center for Security
TIFG	Test and Integration Focus Group
O-CU-CP	Centralized Unit Control Plane
O-CU-UP	Centralized Unit User Plane
O-DU	Distributed Unit
MoU	Memorandum of Understanding
DPAA	Datapath Acceleration
GTP	GPRS Tunnelling Protocol
OS	Operating System
CPU	Central Processing Unit
OAI	OpenAirInterface
C	Confidentiality

I	Integrity
A	Availability
NACM	Network Configuration Access Control Model
LAN	Local Area Network
DDoS	Distributed Denial of Service
SBOM	Software Bill of Material
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
IT	Information Technology
OCI	Open Container Initiative
K8S	Kubernetes
ONAP	Open Network Automation Platform
AAL	Acceleration Abstraction Layer
OR	Operating Room
E2E	End-to-End
LMF	Location Management Function
SRS	Sounding Reference Signals
gNB	Next Generation NodeB
O-RU	Open- Radio Unit
SSB	Synchronization Signal Block
RRC	Radio Resource Control
NRPPa	NR Positioning Protocol A
UP	Uplink
TDoA	Time Difference of Arrival

Table of Figures

Table of Tables

1 Introduction

The 5G-OPERA project aims to build a Franco-German ecosystem for private 5G networks under the joint leadership of TU Dresden and EURECOM (Sophia Antipolis). The focus of the project is the idea of open hardware and software with open interfaces in the area of mobile communication networks to allow multi-vendor options for technical equipment. The goal of the project is to ensure that the hardware and software of all project partners can work together. In addition to setting up reference test environments and demonstrators in Industry 4.0 environments of both countries, **5G-OPERA** is supporting the trials in the three demonstration projects and will advise all additional projects joining the program.

This deliverable is the third of the 5G-OPERA project and defines the requirements of open Radio Access Networks (RAN) solutions. The requirements of open RAN can be a long list. However, this document includes some of them, which are most relevant with the project. The requirements that are covered in this report are security, synchronization, hardware, software, Abstraction Acceleration Layer (AAL), performance and localization.

The Radio Access Network (RAN) subsystem consists of one or multiple gNBs, which could potentially be split into Centralized Unit (CU), Distributed Unit (DU) and Radio Unit (RU). This document at first explains the security requirement coming into scene when the split is applied. For instance, the new interfaces, e.g., F1 and E1 are introduced. The secure communication over these interfaces is a requirement. Moreover, software and minimum hardware requirement of these units are also need to be specified. Furthermore, requirements related to the performance, e.g., latency, bandwidth, and reliability can vary based on the use cases and need to be specified. Last but not least, the TSN requirements and the localization requirements of RAN side are also important for the project.

Many section of this deliverable take the requirements of O-RAN Alliance in to account since 5G-OPERA project is committed to follow the specification of 3GPP and O-RAN Alliance. However, it is important to note that 5G-OPERA project is in development phase, therefore at the end the requirements specified in O-RAN Alliance may not completely overlap with the requirements of the project.

2 Security Requirements

At OPERA, we put best efforts to incorporate security and privacy considerations into all relevant aspects and phases of our product.

Our efforts in this area follow internal control framework known as **OPERA Security Model (OSM)**

The OSM is approach to achieve product security and privacy by design and type of deployment ambitions. High-performance 5G networks are bringing limitless connectivity for connected devices and mobile applications. At 5G-OPERA, we do the networks study that are resilient, secure and able to protect individuals' privacy. Our approach to telecom security is built on four key pillars:

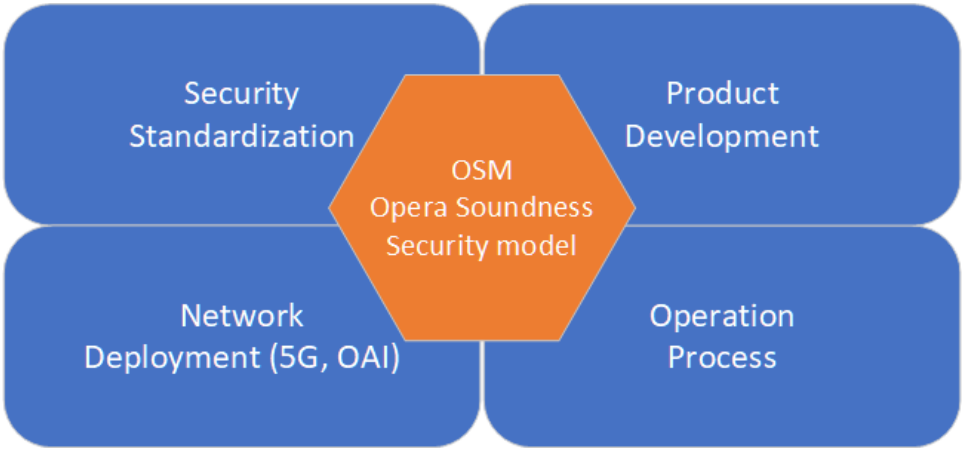

Figure 1: Opera Security Model

At 5G-OPERA, we drive and contribute to security standardization proactively on 3GPP, O-RAN standards.
We follow strongly to the O-RAN Alliance and 3GPP Security Assurance Methodology (SECAM).
5G-OPERA summarizes of this key milestone in the development of the open Radio Access Networks (RAN) system.

a. Security & Testbed Standardization refers to the actual testbed deployment and what security standards are built-in.
b. Validation and Verification refers to assurance of products and solutions in the testbed.
c. Compliance and Forms Process is about providing guidance for security and privacy in use.
d. Implementation and Performance refers to ensure that security and privacy are maintained, monitored and reported.

2.1 Introduction

Open RAN Alliance is an enabler of both telecommunications and industrial use cases. The security requirements of telecommunications networks are well defined and have been widely published. Open RAN networks will play a central role in achieving the digital transformation. Indeed, open RAN networks have the potential to enable and support a wide range of applications and functions, extending far beyond the provision of mobile communication services between end users.

Fundamentally, system design requires an in-depth security analysis and appropriate security measures in place to prevent or mitigate potential attacks. With the introduction of each new entity to a system, a comprehensive threat analysis and corresponding security design is required to account for new potential attacks attempting to exploit the new interfaces and functionality.

However, an increased attack surface does not mean the system is less secure. Rather, open interfaces are more transparent than black-box implementations, facilitating the alignment with security standards and best practice.

2.2 Security Force Group ORAN and GSMA

The O-RAN Security Force Group (SFG) is responsible for security guidelines that span across the entire O-RAN architecture. The security analysis and specifications are being developed in close coordination with all O-RAN Working Groups (WGs), as well as GSMA, regulators, and standards development organizations.

The O-RAN Alliance SFG is using a risk-based approach to characterize risks in open RAN systems according to the ISO 27005 risk analysis methodology using a Zero Trust Architecture, as defined by the National Institute of Standards and Technology (NIST).

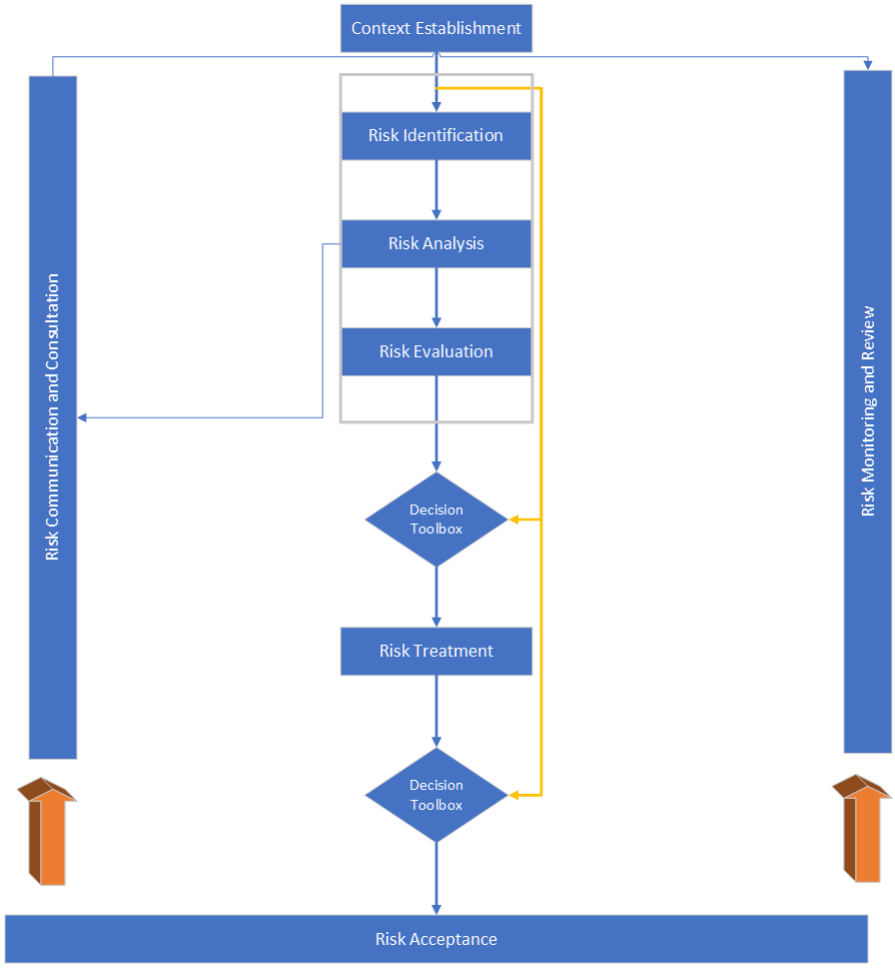

Figure 2: ORAN and SFG (Security Force Working Group) Model

The Open RAN faces the same security challenges as today's RAN and other virtualized architectures. The disaggregation of functions increases the RAN threat surface. The strict latency requirements on the RAN need to be considered when implementing security controls, such as encryption, on the Open Fronthaul Interface. The increased reliance on open source software in modern telecom platforms increases the open RAN dependence on secure development practices within open source communities. The use of Artificial Intelligence (AI) in the RAN may lead to unanticipated consequences as it has in other domains (e.g. racially biased facial recognition). Finally, the dramatic growth in the number of Internet of Things (IoT) devices requires all RAN deployments to protect themselves against the increasing likelihood of attacks by compromised devices.

Recognizing the possible security challenges and the criticality of a secure RAN, the O-RAN Alliance is following the 3GPP security design practices of rigorous threat modeling and risk analysis to identify security requirements and solutions that enable O-RAN to provide the level of security expected by the industry and 5G users.

The O-RAN Alliance Security Task Group (STG) engages with O-RAN Alliance WGs to tackle security challenges on all O-RAN interfaces and components, specifying and recommending modern, practical security solutions

2.2.1 ORAN and GSMA – Secure Interface

a. O1 interface and the Open Fronthaul M-plane, must be protected using industry security best practices such as TLS and/or SSH with strong ciphers, mutual authentication using X.509 certificates.
b. Similar analysis is being performed on the other O-RAN defined interfaces: A1, E2, O2 and Open Fronthaul CUS-plane.
c. The separation of the O-DU and O-RU introduces a potential new attack surface in the RAN: the open fronthaul interface operating the lower layer split (LLS) interface.
d. Securing the x/rApp microservices in the Near and Non Real-Time RAN Intelligent Controllers (RICs), joint work with WG2, WG3 and STG, requires a robust security architecture. They leverage real-time data about the RAN to assess its health and performance using analytics, ML and AI techniques.
e. The underlying O-RAN software platform will be secured by following industry benchmarks such as Center for Internet Security (CIS) benchmarks for OS, Docker, and Kubernetes.
f. The integration of a functional security testing framework – addressed by O-RAN's Test and Integration Focus Group (TIFG) – with standard end-to-end testing will guarantee secure interoperability and overall system security.

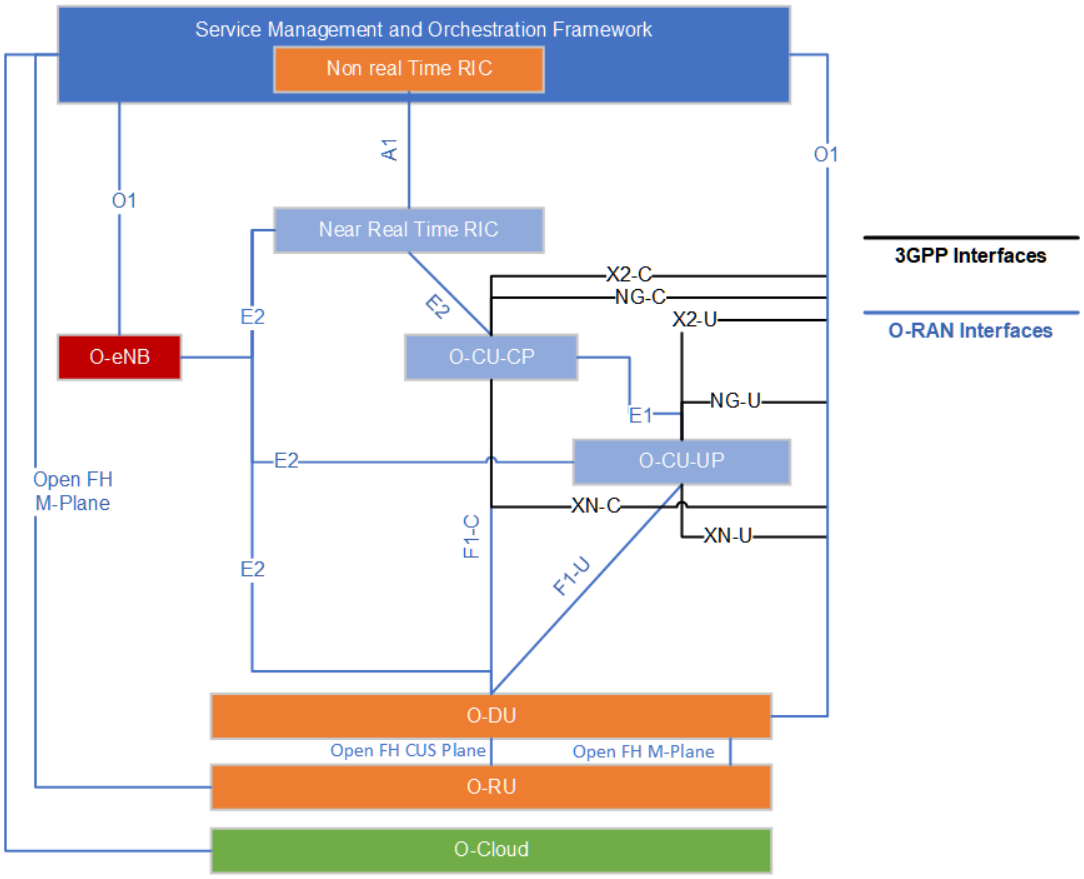

Figure 3: ORAN Alliance Architecture

2.3 OPERA Security Specifications

The openness and disaggregation of open RAN has many positive effects on security. Open interfaces are more transparent than black-box implementations, facilitating the alignment with security standards and best practices. Disaggregation improves security agility, adaptability, and resiliency.

Network functions such as the Near Real-Time RIC, Open-Centralized Unit- Control Plane (O-CU-CP), Open-Centralized Unit-User Plane (O-CU-UP), and Open-Distributed Unit (O-DU), implemented as containerized microservices can leverage cloud native security advances such as hardware resource isolation, automatic reconfiguration, and automated security testing, which can improve both open-source vulnerability management and security configuration management. Opera recognizes cybersecurity as an essential topic on its agenda and is earnestly searching for the optimal means to improve cyber resilience of the Opera system.

5G-Opera Memorandum of Understanding (MoU) with French and German project partners who deploy and manage Opera infrastructure are committed to handle cybersecurity. To have a thorough understanding of cyber risks in open and interoperable networks like Opera systems and need to know how to leverage from security measures and mitigation techniques specified within Opera specifications and must identify hardening measures for operational environments so to cope with cyber risks and regulations.

2.4 Opera THREAT & ATTACK Assessment methodology

Risk-based threat modeling and remediation analysis used for managing risks and for building an effective Opera security architecture.

A zero-trust architecture means even in a closed proprietary implementation, interfaces between internal proprietary software modules shouldn't be trusted. Many of today's security threats come from faults in one module opening access to compromise of other critical modules. From this standpoint, even closed proprietary implementations should examine their own internal proprietary threat surfaces.

The process of risk assessment evaluates the risk for each asset-threat-vulnerability combination and then assigns it a risk score. Each identified threat is assigned to an impact level and based on the likelihood of it occurring. Taking the two values coming from the likelihood of a threat to occur and the impact it will cause a risk level for each threat is derived.

Risks are categorized in priority as **High, Medium, or Low** in relation to how likely they are to occur.

"A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the nation. Threat events are caused by threat sources. A threat source is characterized as: (I) The intent and method targeted at the exploitation of a vulnerability or (II) A situation and method that may accidentally exploit a vulnerability."

Part of the risk assessment steps includes assessing current security controls to determine if the implemented or planned controls will minimize or eliminate risks to Opera

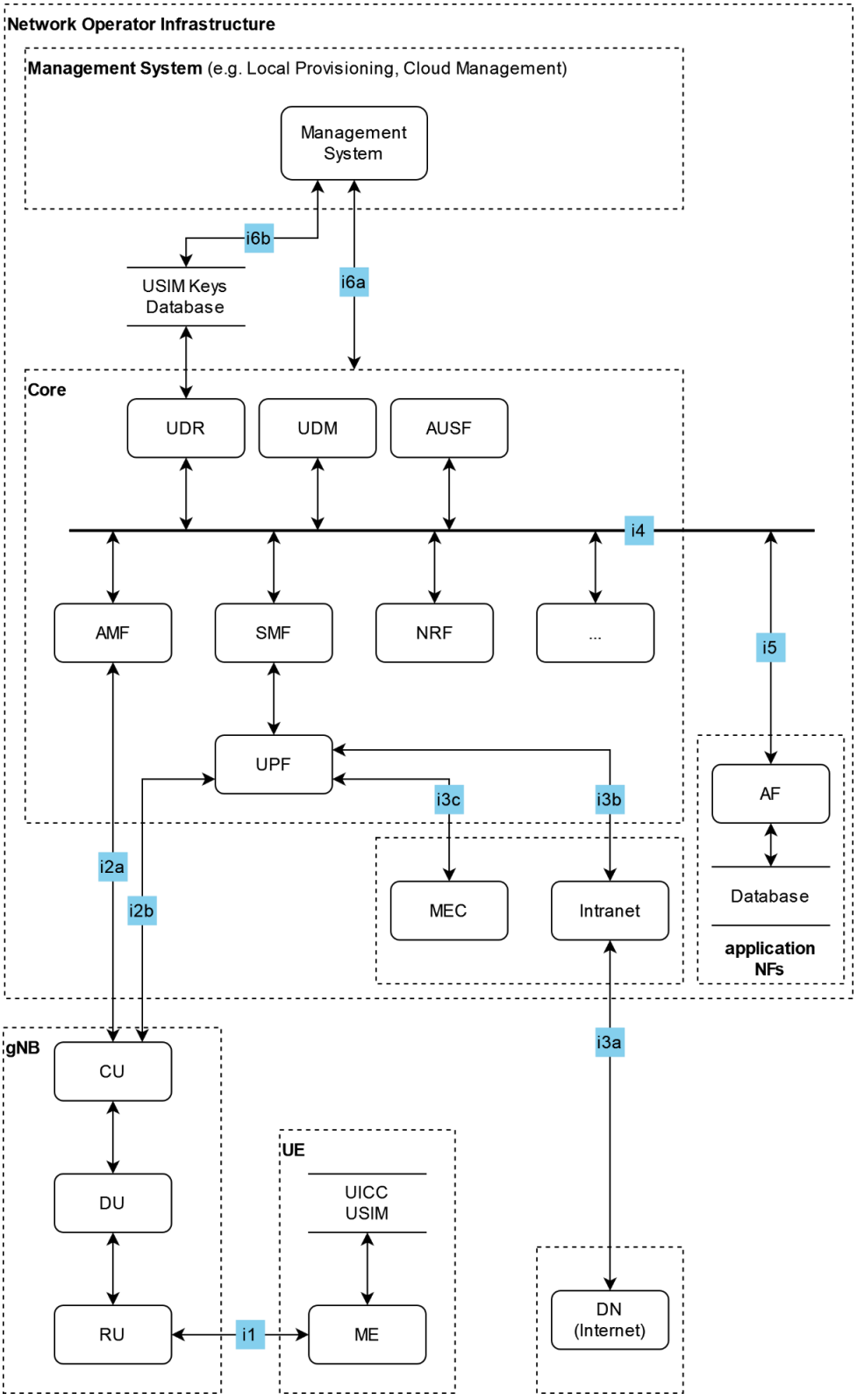

Figure 4: Stride Model (TUD)

Threat modelling and remediation analysis identified specific vulnerabilities. The identified threats are grouped in below.

2.4.1 5G Opera Examples for Offensive Security Testing.

Threat-1: Misconfiguration or poorly configured Opera components e.g., Lack of isolation between network functions in the form of micro-segmentation or not implementing a policy of least privilege access.

Threat-2: Lack of appropriate access controls in management of Opera components

Threat-3: Lack of authentication on Opera interfaces, such as unauthenticated access to open fronthaul networks.

Threat-4: Not following best practices for container images including vulnerabilities in images and libraries.

Attackers exploit these vulnerabilities to inflict damage on the infrastructure. Some of the common attacks include:

Attack-1: An attacker exploits insufficient/improper mechanisms for authentication and authorization in management systems to compromise Opera components.

Attack-2: An attacker exploits un-authenticated/un-authorized access to open fronthaul Ethernet L1 physical layer interfaces to masquerade and impact timing on the Open Front Haul interface.

Attack-3: An attacker uses vulnerabilities in the deployed workload to escape from the container and mount lateral attacks.

Attack-4: An attacker exploits misconfiguration in Dockers/Kubernetes and container security to escalate its privileges and cause damage to the host.

2.5 Opera Security for Mitigating Threats

The impact of threats can be minimized when a network is built based on a well-established set of security principles. Security principles provide a high level and abstract statement of the intended solution to countering potential threats and serves as the foundation for a secure Opera Network.

2.5.1 Example of Open RAN Protection

SEC cipher engines are part of Datapath Acceleration (DPAA) hardware solutions available on NXP platforms like LX2xxx processors. The engine provides a number of hardware accelerators for ciphering/authentication, control blocks and protocol accelerator primitives that can be flexibly programmed. Table 1 Shows some of the security algorithms, as well as protocols supported by SEC accelerators.

Table 1. Selected Algorithm and Protocol Accelerators in SEC

Hardware-accelerated security algorithms.	AES, DES, MD-5, SHA, CRC, ZUC E, ZUC A, RNG, SNOW F8, SNOW F9

Built-in protocol accelerator primitives	IPsec, TLS, PDCP, MACsec, SRTP, WIFI

A sample use case is the protection of the link between the Near-Real-Time RAN RIC and the O-DU in an architecture where both components/entities run on separated hosts. NXP SEC cipher hardware engine can be used to mitigate threats to Confidentiality, Integrity and Availability in the open RAN network by enabling IPsec tunneling to protect that communication link for the E2 interface. Similar approach might be applied to an O-CU hosted by suitable NXP processors.

Provided that GPRS Tunnelling Protocol (GTP) protocol is used to communicate the open RAN components/entities, it can be assumed that GTP processing modules are instantiated in the RIC server and in the O-DU host. It is also assumed the O-DU host runs on a Linux Operating System (OS). Figure 5 shows the example deployment use case for an O-DU based on an NXP LX2xxx processor.

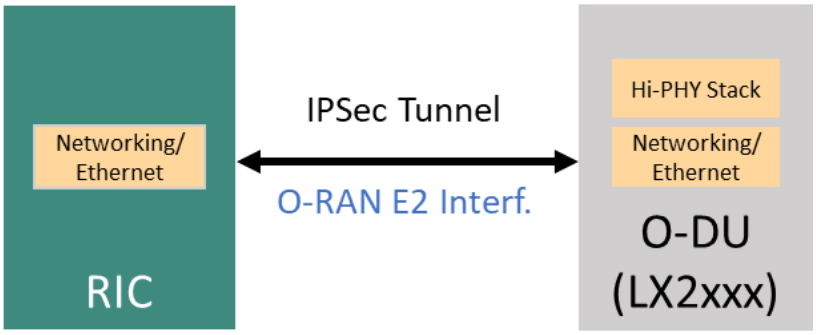

Figure 5. Sample deployment of IPsec to secure O-RAN E2 Interface. O-DU and (Near-RT) RIC run on separated hosts.

SEC engine can provide support to Central Processing Unit (CPU) cores accelerating a variety of IPsec features. Some of them are summarized in Table 2. Also, the host processor is enabled to offload bulk packet processing from the Linux kernel as depicted in **Error! Reference source not found.**.

Table 2. Some IPsec features supported by SEC engine. Source: NXP Semiconductors

IPsec	Supported feature
Protocols	ESP/AH
Algorithms	DES, 3DES, AES (CBS, CTR), HMAC-SHA1, HMAC-SHA2, HMAC-MD5
Hardware acceleration	Integrated with NXP Security engine for protocol and crypto acceleration
Other	Extended sequence number
	Random IV generation for each packet
	IPv4, IPv6 support
	Anti-Replay Mechanism
	IKEv1 and IKEv2

In addition, for performance optimization reasons, 5G stacks and GTP processing are typically implemented in Linux User-Space. Hardware acceleration engines leverage that to deliver packets directly to the GTP modules in the user-space, bypassing the Linux kernel.

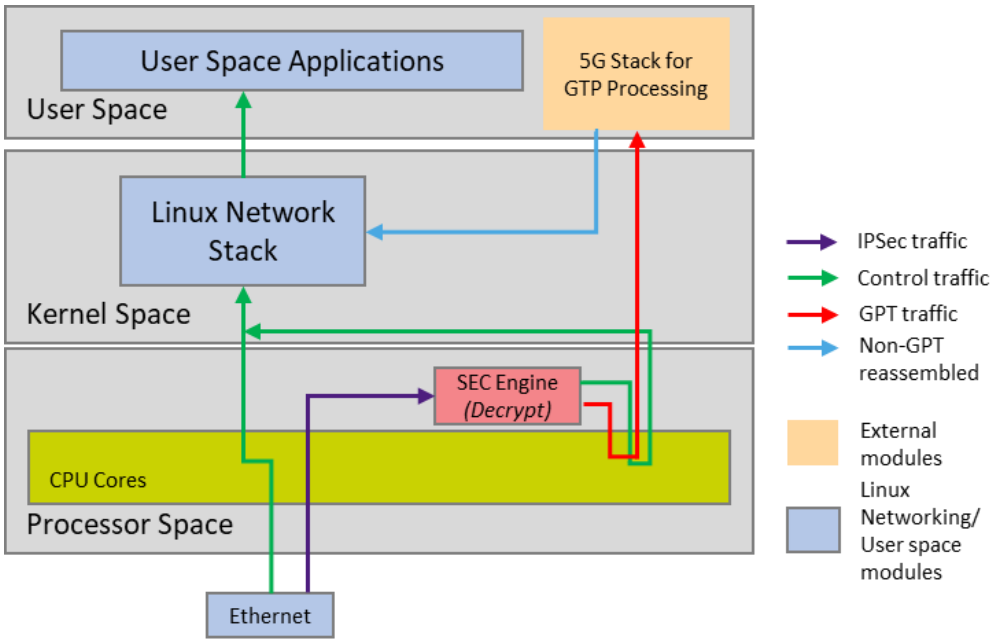

Figure 6: NXP's SEC engine and CPU cores offload bulk packet processing from Linux Kernel, accelerating IPsec packet flow on O-DU's E2 interface. Downlink flow, from RIC. Source : NXP Semiconductors.

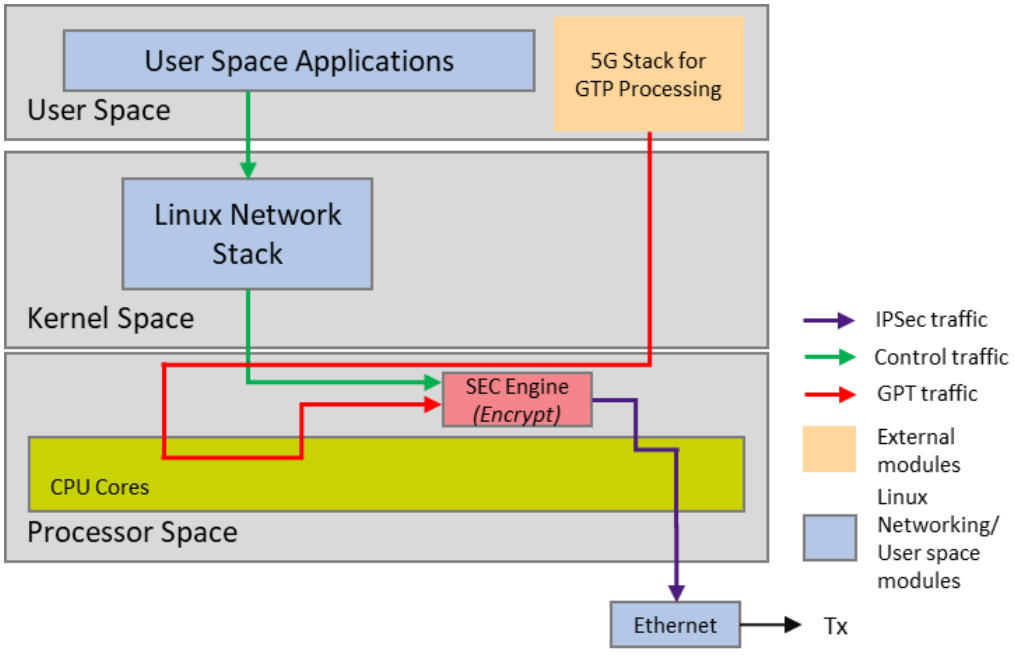

Figure 7: NXP's SEC engine and CPU cores offload bulk packet processing from Linux Kernel, accelerating IPsec packet flow on O-DU's E2 interface. Uplink flow, towards RIC. Source: NXP Semiconductors.

Figure 6 illustrates the packet flow for downlink path traffic received on E2 interface. ESP-encapsulated GTP packets are received from the E2 interface Ethernet port. Then, configured CPU cores pre-process packets to be submitted to SEC engine for IPsec processing. After IPsec processing, packets are classified and GTP traffic is sent for further processing in User Space. Packet flow for uplink traffic is shown in Figure 7. There, GPT application enqueuers packets to configured cores which filter packets that can be directly sent to the SEC engine for encryption and encapsulation with ESP header. Afterwards, the processed packets are sent for classification and transmission on the Ethernet port.

2.5.2 Example Threat Mitigations

Mitigating Threat-1: Mutual authentication SHOULD be established between communicating entities in an Opera system, with each entity identified by a unique identifier and credentials.

Mitigating Threat-2: Access control SHOULD be implemented that only allows authenticated and authorized personnel and services to access Opera resources.

Mitigating Threat-3: Principle of least privilege SHOULD be followed to ensure that accounts have the least amount of privilege required to perform their business processes.

Mitigating Threat-4: Measures SHOULD be taken to provide a secure and trusted runtime environment for cloud applications by implementing security controls that reduce the risk of firmware exploitation and impact of many published early-boot vulnerabilities when bootstrapping a cloud native platform.

Mitigating Threat-5: Domain separation or security zones SHOULD be implemented to group systems and resources that have similar needs for information protection, access controls

Mitigating Threat-6: Security controls SHOULD ensure that lateral movement is detected and prevented when attackers have successfully exploited a vulnerability to gain initial access into a 5G cloud system

Mitigating Threat-7: The system SHOULD ensure protection of data-at-rest, data-in-transit, and data-in-use according to industry best practices (e.g. ISO27001).

Mitigating Threat-8: The system SHOULD be bootstrapped to be secured by default and it should be up to the Admin to reduce the security perimeter of the end user system or devices by automated rules if necessary.

Mitigating Threat-9: Industry best security such as DevSecOps practices SHOULD be followed when using open-source components, to minimize risks.

Mitigating Threat-10: System should be pre-tested by offensive security testing team like Mittre Att&ck framework as developed in 5G-OPERA Project.

2.6 Opera Risk Assessment methodology

The criticality of the identified threats is assess based on their potential impacts. Indications of severity level for each threat are given whether they are considered as high, medium, or low. This severity is seen as a global perception of the risk based on its impacts.

Table 3 : It is the Security principles are identified among them, authentication and access control mechanisms, trusted communication, secure cryptographic operations, secure storage, secure boot, trusted and secure update, secure management of open-source components, robust isolation, continuous security development, testing, logging, monitoring and vulnerability handling, and security assurance.

The security principles rationale is provided to trace all security principles back to threats and demonstrate that the defined security principles contribute to counter those threats.

Table 3: Security Testing Table - Opera Interfaces

Severity	Affected Node	Model	Clock Model and Sync Topology	C = Confidentiality	I = Integrity	A = Availability
High / Medium	Core	Mittre Att&ck	Metaspolitable Attack on Core network using backdoor	X	X	X
High / Medium	Core and RAN	Mittre Att&ck	Hydra Attack	X	X	X
Low / Medium	O-DU is effected	Mittre Att&ck	DoS Attack	X		X
High / Medium	Ngap / RAN	Mittre Att&ck		X	X	X
Low / medium	Ue Air Interface Attack		Side Channel Attack		X	X
Low	Ue App attack		3rd party Attack		X	

2.7 Opera Security Assessment Methodology

The initial security requirements per OpenAirInterface (OAI) and per OPERA component. Requirements address Confidentiality (C), Integrity (I), and Availability (A)- (CIA) protection by considering key controls such as authentication, authorization, replay protection, least privilege access control, and zero-trust among others in Figure 8.

Requirement 1: Confidentiality, Integrity, Replay protection and Data origin authentication mandatory requirements for A1, O1, O2, E2 interfaces.

Requirement 2: Least Privilege Access Control on O1 interface enforcement with IETF RFC- 8341 Network Configuration Access Control Model (NACM).

Requirement 3: Authentication and Authorization based on IEEE 802.1x Port based Network Access Control requirements to control network access in point-to-point Local Area Network (LAN) segments across the open fronthaul interface.

Requirement 4: Mandatory support for TLS 1.2+ and Public Key Infrastructure X. 509 (PKIX) for mutual authentication on the Fronthaul M-Plane.

Requirement 5: Transversal requirements and tests cases for Networks Protocols and Services, Distributed Denial of Service (DDoS) attacks protection, password protection policies and vulnerability scanning.

Requirement 6: Software supply chain security support in the form of Software Bill of Material (SBOM) requirements for every O-RAN software delivery following NTIA guidance

Reference Requirement 4: Minimum requirement to secure layer 4 ideally secure layer 3 with IP-Sec wherever system interface supports it.

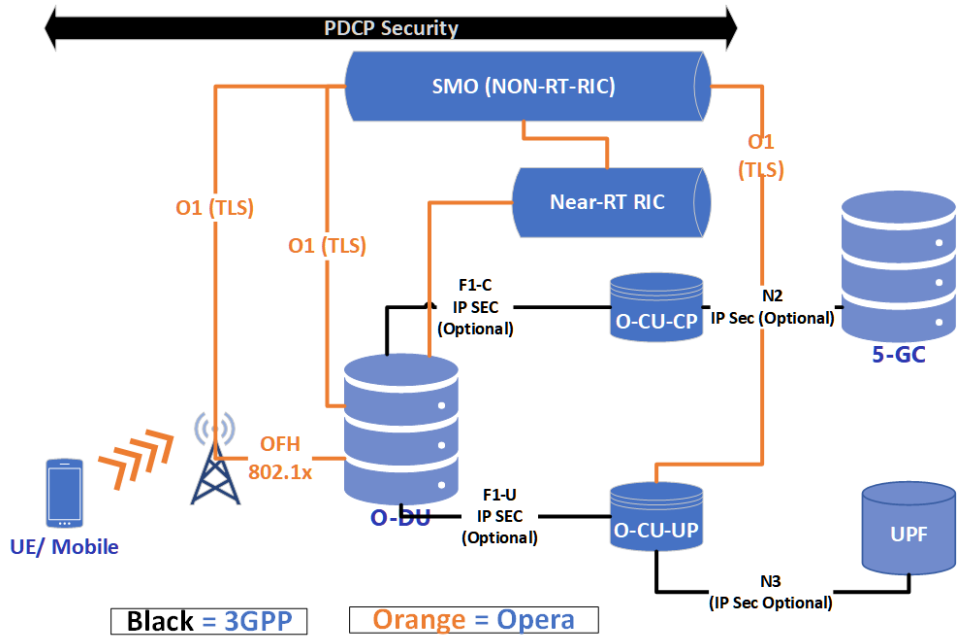

Figure 8: Security Testing Table - Opera Architecture

Table 4: Security Mechanism on Opera Interface

#	Opera Components	Between nodes	Security Mechanism	Standardization
1	O1 Interface	SMO and Opera elements	mTLS	O-RAN
2	A1 Interface	Near-RT RIC and Non-RT RIC	mTLS	O-RAN
3	E1 Interface	O-CU-CP and O-CU-UP	NDS/IP (IPSec) or DTLS	3GPP
4	F1 Interface (Midhaul)	O-CU-CP and O-DU (F1-C) O-CU-UP and O-DU (F1-U)	NDS/IP (IPSec) or DTLS 3GPP	3GPP
5	Open Front Haul M-Plane	O-RU and O-DU/SMO	mTLS, SSHv2	O-RAN
6	Open Front Haul CUS Interface	O-DU and O-RU	IEEE 802.1x with EAP-TLS O-RAN	O-RAN
7	Backhaul Interface	O-CU-CP and 5GC (N2) O-CU-UP and 5GC (N3)	NDS/IP (IPSec) or DTLS	3GPP
8	E2 Interface	Near-RT RIC (xAPPs) and O-CU-CP	NDS/IP (IPSec) or DTLS	O-RAN

9	O2 Interface	SMO and O-Cloud	Under Study	O-RAN
10	X/R Apps Interface	Non/Near-RT RIC	Under Study	O-RAN
11	Xn Interface	Source gNB and Target gNB	NDS/IP (IPSec) or DTLS	3GPP
12	Secure Physical Assets		Apply Best Practices	3GPP

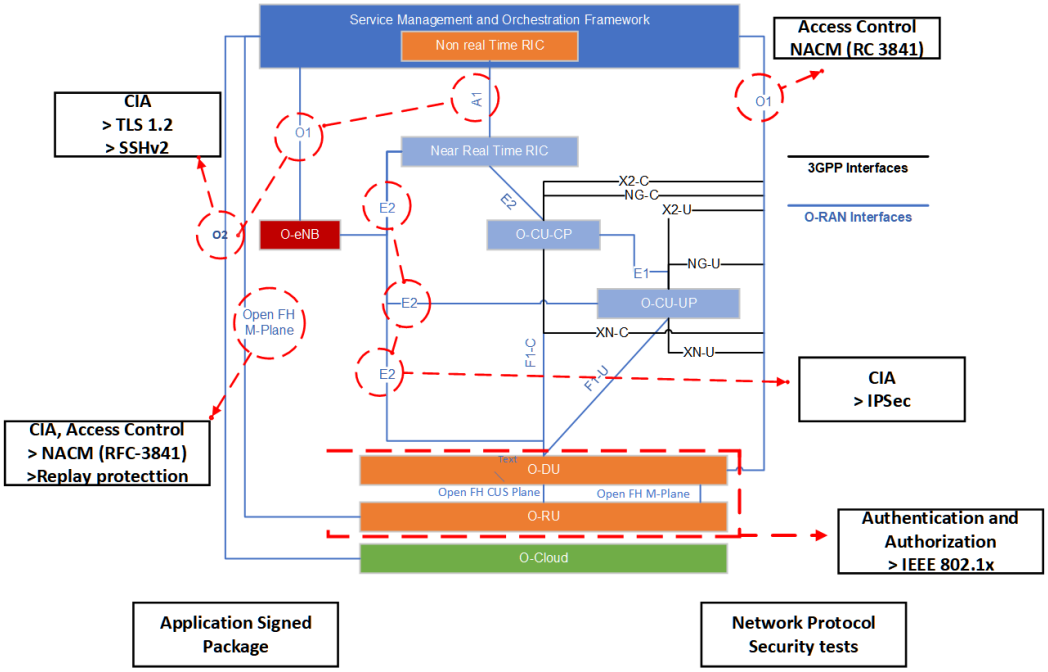

Figure 9: Security Protocol reference ORAN Architecture

2.8 Opera Security Test Assessment Methodology.

The security tests needed to validate security-related functions, configurations, and protocols requirements and is the first step towards verifying the security requirements of O-RAN systems.

The focus of the security test specifications is on.

Security Testing-1: Validating the proper implementation of security protocols requirements specified by 3GPP and Open-RAN in Security Protocols Specifications (SSH, TLS, DTLS, and IP-Sec).

Security Testing-2: Emulating security attacks doing vulnerability testing on Core and RAN against the OPERA components, interfaces, and the system to measure the robustness.

Security Testing-3: Validating the effectiveness of the security mitigation methods to protect the OPERA system and the services it offers.

Security Testing-4: Validating transversal requirements for Networks Protocols and Services, DDoS attacks protection, password protection policies, and vulnerability scanning defined in Opera security requirements.

2.9 Security assurance framework

In 5G-OPERA project, we will bring together security specifications from 3GPP, ORAN and other standardization bodies, security best practices from CIS and NIST, along with security features that add a whole new dimension of security to telecom.

The Security Assurance Platform has baseline security requirements that bring in the essence of Network Equipment Security Assurance Scheme (NESAS), National Institute of Standards and Technology (NIST), 3GPP.

2.10 Conclusion

5G and open RAN introduce new infrastructure, functions, and interfaces and within 5G-OPERA project we use these technologies that have the potential to make 5G as secure network generation to date, but only when carefully configured and securely operated.

This security baseline must be completed by vendor- and operator-implemented security controls to reach a high level of hacking resistance for the IT and cloud systems underpinning modern networks.

When implementing these additional controls, telco vendors and operators can borrow knowledge and experience from related industries: Cloud & IT.

We hope that the best practices underline in this guide contribute to the overall global security of 5G-OPERA system.

Our societies rely on secure and reliable communication and information systems, and we are honored to contribute to the open knowledge pool on how to best secure the networks of the future.

For the study case of 5G-OPERA the goal of reliable and secure communication systems at a low cost for open 5G campus networks is targeted.

3 Synchronization Requirements

The development of boundary clock supporting L2 platform based on IEEE1588v2 PTP/SyncE is required for the 5G-OPERA project. More specifically, special emphasis will be given to the fronthaul network: the network between O-DU and O-RU. As illustrated in Figure 10, scenario LLS-C3 will be supported. A Telecom Boundary Clock functionality needs to be provided to validate the clock on the source interface(s) and distribute the timing information to the different slave interfaces [1].

The following synchronization methods will be supported:

- Frequency synchronization (ITU-T G.8265.1)
- Phase synchronization (ITU-T G.8275.1)
- Time synchronization (ITU-T G.8275.1)

The accuracy objective is Class C as defined in ITU-T 8273.2.

The following SyncE standards will be implemented:

- G.8261 Timing and Synchronization Aspects in Packet Networks
- G.8262 Timing characteristics of a synchronous equipment slave clock

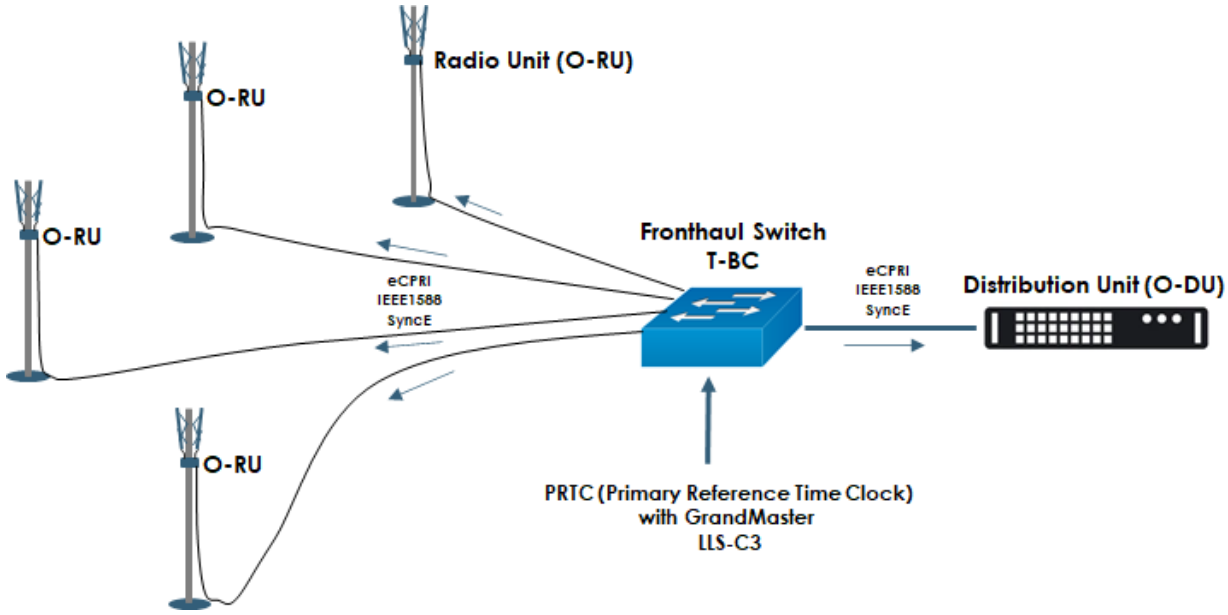

Figure 10: Fronthaul switch in clocking scenario LLS-C3

4 Cloud Platform Hardware Requirements

Table 5 presents hardware requirement for regional and edge cloud platform specified by O-RAN Alliance. These requirements will be taken into account by 5G-OPERA project partners; however, it may be possible that 5G-OPERA project partners can have additional or different hardware requirements from requirements listed in Table 5. The exact list of hardware requirements is not clear now since the development and deployment of units are still ongoing.

Table 5: Requirements for cloud platform [2].

Components	Description
Server	• Regional cloud: standard COTS server • Edge cloud: depth ≤ 450mm, height ≤ 2RU, width ≤ 19in • Minimum 16-core CPU at 2.2 GHz base frequency and 128 GB DDR4 • At least 2x 25GbE ports for front-haul interface (or higher, depending on site), 2x 10GbE ports for backhaul interface, and 1x 1GbE out-of-band management port • SR-IOV-capable NICs with network link aggregation enabled • For single-socket, at least 3 PCI-E slots for 3x HHHL or 1x FHFL + 2x HHHL cards; for dual-socket, at least 4 slots for 4x HHHL or 1x FHFL DW + 3x LP cards • All hard disk drives require hot-pluggable • Management interfaces support IPMI, SNMP, and Redfish (preferred) • UEFI secure boot enabled

Hardware Accelerator	• Required for O-DU in the edge cloud in forms such as FPGA, ASIC, and GPU • At least 2 ports at 10 or 25 Gbps eCPRI/RoE open front-haul interface • Acceleration for functions such as LDPC encoding and decoding, and end-to-end high PHY
Switch	• Standard COTS TOR switch
Storage	• Software-defined storage (e.g., Ceph) based on COTS servers

5 Software Requirements

This section describes the software requirements of O-Cloud. Depending on the implementation choice of O-CU, O-DU, and near-RT RIC, O-Cloud needs to support virtual machines or containers. In the project it is discussed that these functions are preferred to be deployed based on containers. Therefore, the developed software components from WP4 and WP5 will be delivered as a container image and will be aligned with container standard, i.e., Open Container Initiative (OCI). In order to manage, scale, and deploy containerized applications automatically, Kubernetes (K8S) system is proposed for the project. O-RAN Alliance has specified the container management and orchestration requirements in the Table 6. These requirements can be taken into account by project partners. However, due to ongoing work, the requirements listed in Table 6 may not fulfill the requirements of the project.

Table 6: Container management and orchestration requirements [2].

Components	Description
Container Management	Container management and scheduling with Kubernetes kube-apiserver, kubescheduler, etcd, kube-controller-manager
Container Orchestration	Container orchestration with HELM charts
Container Storage	Container persistent volume claims (PVCs)
Container Networking	Container networking with kube-proxy and CNI

Table 7: Requirements for the cloud platform operating system [2].

Operating system	Description
Linux	• Linux kernel with real-time preemption patches for O-DU workloads (i.e., SMP PREEMPT RT). Real-time kernel patch for O-CU is optional. • Deterministic interrupt handling with a maximum latency of 20 µs as measured by cyclictest for system interrupts (e.g., external I/O) and interrupt-based O-CU and O-DU implementations (e.g., those that rely on OS timers) • CRI-O and/or CRI plugin containerd support

Table 8: Requirements for the cloud platform runtime

Components	Descriptions
Accelerator Driver	Edge cloud: driver for loading, configuring, managing and interfacing with accelerator hardware providing offload functions for O-DU container or VM

Crypto Driver	Crypto offload driver for networking and O-CU wireless cipher (optional)
Network Driver	Network driver(s) for front-haul, back-haul, mid-haul, inter container or VM communication, management and storage networks
Board Management	Board management for interfacing with server hardware and sensors
PTP	Precision time protocol for distributing phase, time and synchronization over a packetbased network
Software-defined Storage (SDS)	Software implementation of block storage running on COTS servers, optional for edge cloud and required for regional cloud If used in edge cloud, required to be hyperconverged; in regional cloud, either hyperconverged or deployed on dedicated storage nodes
Container Runtime	Executes and manages container images on a node

Moreover, the requirements of cloud platform operating system as listed in Table 7 and runtime as listed in Table 8 are specified by O-RAN Alliance. These requirements also will be taken into account. Addition to these, the generic requirements for O-Cloud platform management are also listed in [2], e.g., configuration managements, host managements, service management and fault management. Since specification of the O-RAN Alliance is in scope of the project, the requirements that provided by the O-RAN Alliance can be considered as baseline.

For the orchestration and automation of developed virtual and physical network functions, Open Network Automation Platform (ONAP) is proposed. Because ONAP provides benefits such as enabling common management of services and connectivity, while applications run separately, orchestration for both virtual and physical network functions, and enabling operators to use same deployment and management mechanism, besides using same platform [3].

6 Hardware Acceleration Abstraction Layer Requirements

O-RAN specifies the Acceleration Abstraction Layer (AAL) as a common and consistent interface for hardware device accelerators to the applications which facilitates decoupling of an application, e.g. O-RAN Cloudified Network Function, from a specific hardware accelerator device implementation. Its general interface principles, which are appropriated as design requirements for the scope of this project, are listed in Table 9. More details can be found in [4].

Table 9: General interface principles of the hardware acceleration abstraction layer

General Interface Principles	Descriptions
Extensibility	While being based on 3GPP specifications and O-RAN deployment scenarios the API shall be extensible to accommodate future revisions of the specification.
HW Independence	An AAL profile API should be independent of the underlying HW.

Interrupt and Poll Mode	The AAL shall support both interrupt mode, poll mode and any combination of both.
Discovery and Configuration	The AAL shall support application software to discover and configure the AAL Device.
Multiple Device Support	The AAL shall support an application using one or more AAL Devices at the same time.
AAL offload capabilities	The AAL shall support different offload architectures including look-aside, inline, and any combination of both.
Look-aside Acceleration Model	The AAL shall support look-aside acceleration model where the host CPU invokes an accelerator for data processing and receives the result after processing is complete.
Inline Acceleration Model	The AAL shall support inline acceleration model where acceleration by function and I/O-based acceleration are performed on the physical interface.
API Concurrency and Parallelism	The AAL shall support multi-threading environment.

7 Performance Requirements

The performance related requirements can change from use case to use case. Therefore, in this document, some performance requirement from demonstration project partners is presented. It is not guaranteed that all these requirements will be achieved by 5G-OPERA. However, the more doable ones can be provided.

Table 10 shows the availability, reliability, End-to-End (E2E) latency, and bit rate requirements for use cases listed in the table.

Table 10: Requirements for use case presented by project 5G-OR

Use cases		**Requirements**			
		Availability	Reliability	E2E latency	Bit rate
AI-assisted continuous monitoring		>99%	48h	Al low as possible	100 Mit/s
5G remote enabled needle-based procedures	Teleman slice	>99.99%	48h	<1 ms	100 Mbit/s
	Stream slice	>99%	48h	<35 ms	4 Gbit/s
Mobile robotic Operating Room assistant (AG)		>99.999% (class 5 availability)	24h	<10 ms	<300 Mbit/s Upload
Surgical data provision and AI-Analysis		>99%	24h	<60 ms	2.8-11.2 Gbit/s

Table 11: Requirements for use cases from 5G-Forum

	Requirements

Use Cases	UE type	Latency	Bandwidth	# of connected devices	Prioritization	Others
Standart control traffic	Smartphones or 5G modules	< 500 ms	Several kB/s	4-10	No	TCP & UDP
Video Traffic	Smartphones	-	>2Mbps	2-3	No	WebRTC
Low-Latency control	5G modules	<100 ms <10 ms is better	Several kB/s	4-5	Strict prioritization of real-time traffic	UDP Employing network slicing and/or TSN over 5G

8 Localization Requirements for RAN Side

In the 5G-OPERA project we will use Uplink- Time Difference of Arrival (UL-TDoA) localization method based on Sounding Reference Signals (SRS).

We deploy multiple gNBs and each gNB is connected to one O-RU. In this setup we will use gNB to describe the ensemble of CU and DU. For localization this will simplify the implementation, as we will not have to implement the localization specific messages over the F1 interface.

All gNBs use a different cell ID and each gNB transmits a single Synchronization Signal Block (SSB) but with a different SSB index to reduce interference. The O-RUs need to be synchronized in time and frequency as described in Section 3.

In the 5G-OPERA project we will need at least 4 synchronized gNBs, see Figure 11, and corresponding O-RUs.

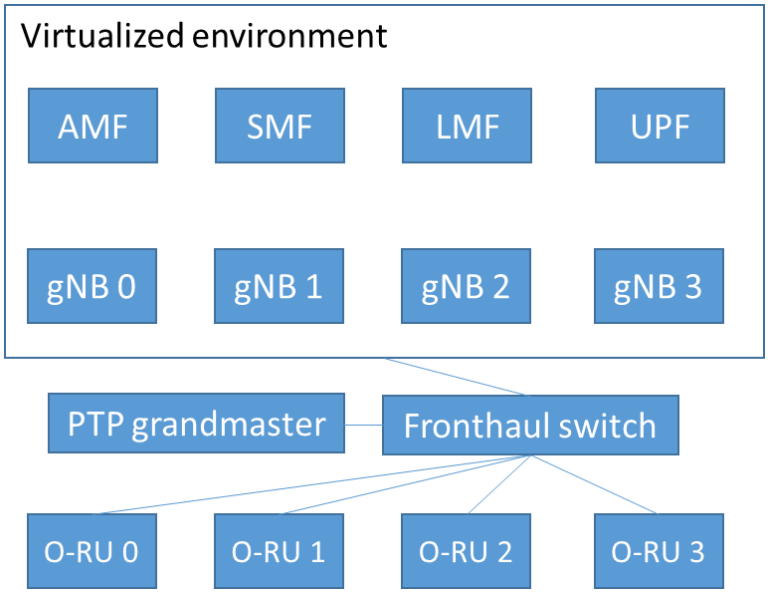

Figure 11: Deployment scenario for localization.

The gNB needs to be able to configure SRS over Radio Resource Control (RRC), perform channel estimation as well as estimation of the multipath components of the channel estimate.

The estimates are then sent over NR Positioning Protocol A (NRPPa) to the Location Management function (LMF). The gNB therefore needs to support the required NRPPa messages for the UL-TDoA procedure as indicated in Figure 11. Moreover, Figure 12 shows the procedure of localization for UL.

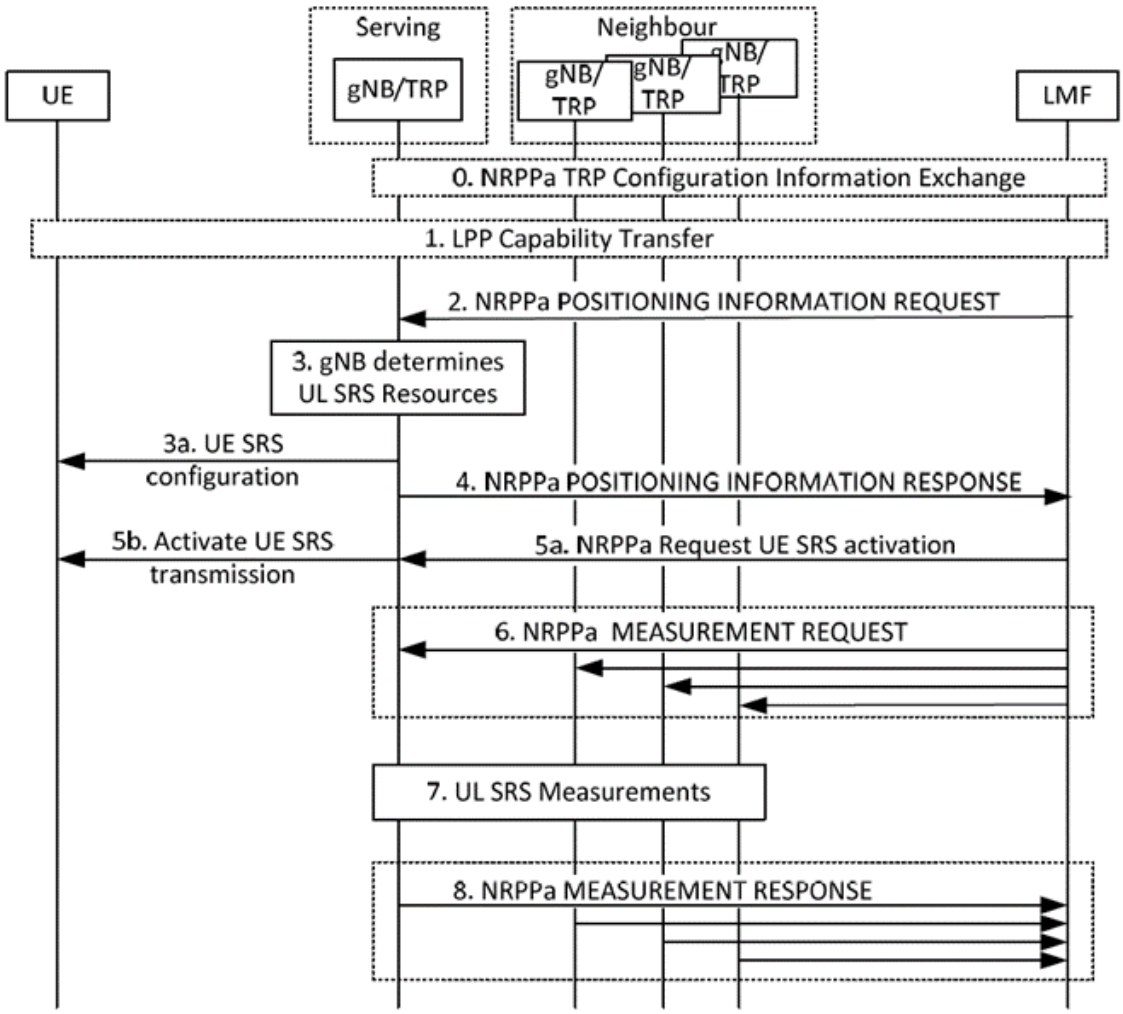

Figure 12: UL-TDoA localization procedures. Taken from 3GPP TS 38.305.

9 Requirements from RAN Side for TSN Integration

The main goal of TSN is to provide deterministic, reliable, high bandwidth and low latency services over wired networks, i.e., to provide guaranteed delivery in a guaranteed time window. This means that the packets should be transported over the network with guaranteed low latency, low packet loss and low jitter. In order to have a good end-to-end quality of service, there should be good internetworking between TSN and 5G system.

In 5G-Opera project, to support TSN services over the 5G system certain enablers/requirements should be satisfied in order to effectively integrate TSN with 5G system. These enablers in the RAN system provide reliability and transport latencies. The TSN features such as **Traffic shaping, Resource management, Synchronization and Reliability**, which help in deterministic delivery of packets are enabled in 5G system using URLLC (Ultra Reliable and Low Latency Communication) features.

In 3GPP specifications, latency reductions can be achieved using

- mini-slots,

- Flexible numerology
- Preemptive indicators in downlink transmissions
- Uplink configured grant transmissions
- Downlink semi-persistent scheduling
- Reduced UE and gNB processing times

Reliability is achieved using

- Multi-antenna transmission, i.e, space diversity to avoid probability of experiencing deep fades
- Higher layer packet duplication, preferably at PDCP layer
- Sending the transport Blocks in consecutive slots – multi slot repetition
- MCS enhancements with low spectral efficiency entries in MCS tables – low code rates

However, the above features are limited in particular to Radio Access network(RAN) and do not consider the complete end-to-end(E2E) connectivity or Quality of service(QOS).

Some of the key requirements for successful integration of TSN with 5G systems at network level includes mapping of respective protocols of each other, i.e

- For every active port at each DD-TT/NW-TT, a PDU session must be established to transfer traffic of specific QOS. In TSN based packet prioritization, eight priority levels are used which are mapped to queues of each port. Similarly, in 5G system, a PDU session is established with different QOS flows using different QOS priorities. When TSN traffic arrives at the 5G system, the traffic in a specific queue must be mapped on to a QOS flow, the QOS configuration of the TSN traffic is received via TSN AF.
- In order to efficiently forward the TSN streams and avoid the queuing delays, the arrival time must be considered in the 5G system. Using the arrival time, the time sensitive communication assistance information (TSCAI) must be evaluated by the 5G core and must be forwarded to the 5G RAN and the packet scheduler in the MAC uses it to efficiently transmit over the air interface by maintaining the deterministic packet delay.

10 Conclusions

In this report, the most relevant requirements of open RAN solutions have been described and related standards have been searched and cited. The following point are the summary of requirements:

- The system design of open RAN requires an in-depth security analysis and appropriate security measures in place to prevent or mitigate potential attacks.
- Disaggregation of units requires synchronization in time, frequency and phase. The scenario of LLS-C3 will be supported in the project for synchronization scenarios in fronthaul network.
- Hardware requirements of commercial of-the-shelf (COTS) servers as well as definition of the software requirements such as container management, OS, and runtime of O-Cloud platform has been listed.
- Hardware Acceleration Abstraction Layer requirements have been described.
- Limits of performance requirements such as delay, bandwidth, availability, and reliability has been introduced.
- Localization is an important feature for private 5G networks as well as integration of TSN. Therefore, requirements for TSN and localization in the RAN side has been described.

In conclusion, this deliverable covers the requirements important for 5G-OPERA project and it is the third in a series that will define the work that we will carry out in the 5G-OPERA project. Deliverable3.4 is the following deliverable that will define the requirements of open core solutions.

11 References

[1] O-RAN Alliance, "O-RAN Architecture Description 7.0 (O-RAN.WG1.O-RAN-Architecture-Description-v07.00)," October 2022. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications. [Accessed January 2023].

[2] O-RAN Alliance, "O-RAN Cloud Platform Reference Designs 2.0," February 2021. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications. [Accessed January 2023].

[3] "Open Network Automation Platform Overview," ONAP, January 2023. [Online]. Available: https://docs.onap.org/en/latest/platform/overview/index.html. [Accessed January 2023].

[4] O-RAN Alliance, "O-RAN Acceleration Abstraction Layer General Aspects and Principles 4.0," October 2022. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications. [Accessed Janury 2023].