5G OPERA

5G-OPERA Deliverable 5.5

E2E Network Management and Automation

Document Properties	
Name of project	5G-OPERA
Document title:	E2E Network Management and Automation
Client:	Ministère de l'économie, des finances, et de la relance, Bundesministerium für Wirtschaft und Energie
Official reference:	5G-OPERA D5.5
Reviewer:	Florian Kaltenberger, Thomas Höschele
Abstract:	
Date of publication:	26/01/2024
Version:	1.2
Access:	Public
Keywords:	Open RAN, 5G Private Networks, E2E Network Management

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 E2E network management and Automation of open RAN.

The report starts with an introduction in Section 1, and then follows with Section 2 where the topic of end-to-end network management is described, selected tools are presented and an implementation of the O1 interface in OpenAirInterface for 5G-OPERA is introduced.

Table of Contents

Abbreviations

OSM	Open Source MANO
E2E	End-to-End
RAN	Radio Access Networks
O-CU-CP	Centralized Unit Control Plane
O-CU-UP	Centralized Unit User Plane
O-DU	Distributed Unit
O-RU	Radio Unit
RIC	Radio Intelligent Controller
PNF	Physical Network Functions
NMA	Network Management and Automation
ONAP	Open Network Automation Platform
NFV	Network Function Virtualization
3GPP	Third Generation Partnership Project
OAI	OpenAirInterface
SMO	Service Management and Orchestration
SW	Software
gNB	Next Generation NodeB

Table of Figures

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, **5G-OPERA** is supporting the trials in the three demonstration projects and will advise all additional projects joining the program.

This deliverable of the 5G-OPERA project defines the improvement of the E2E network management and automation of open Radio Access Networks (RAN) equipment, gathering network information and presentation. This work package will include software solutions for automated RAN configuration and integration with software independent of Open RAN vendors. Addition to these, implementation of the network management in 5G-OPERA project, particularly O1 interface is explained. O1 is a logical interface which is used to manage near-RT RIC, the O-CU, and the O-DU. Managing O-RU towards O1 interface is for future investigation. Some of the management services supported via the O1 interface are file management services, trace management service, fault supervision management services, provisioning management services, and startup and registration, and software management services for Physical Network Functions (PNF). Standard protocols such as SSH, TLS, and NETCONF are used for management functionalities and YANG is used for data models.

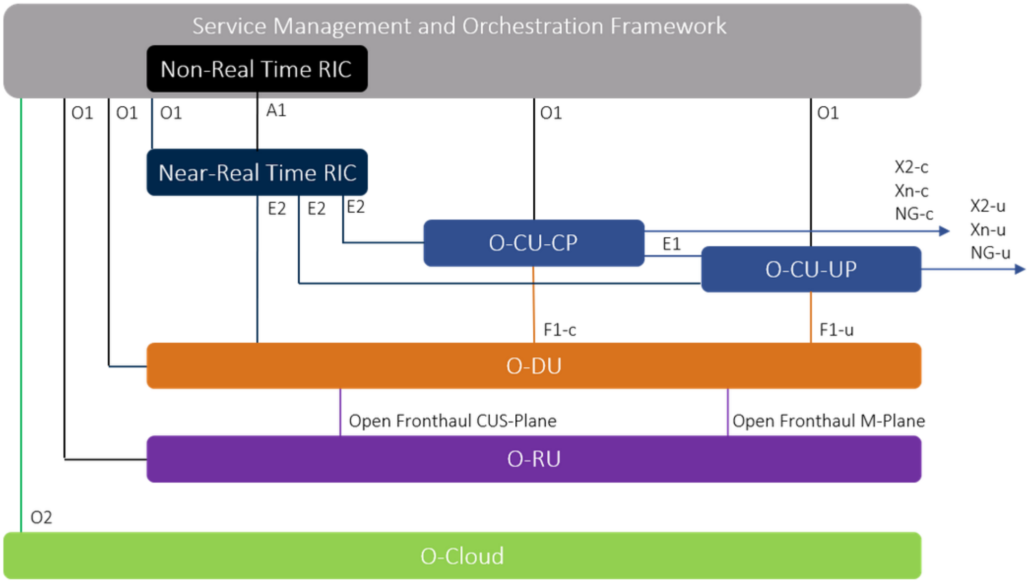

Figure 1: O1 interface and network functions [1]

2 E2E network management and automation

2.1 Network management

Network Management and Automation (NMA) aims to improve network operability for 5G. The heterogeneity of network elements demands an enhanced level of automation. NMA for 5G network should support:

- Providing an interface for managing and controlling the network

There are three stages of interfaces; Day 0, Day 1, and Day 2. Day 0 is the stage when the network is designed, requirements are specified, and the architecture is decided. Day 1 is the stage when the network is deployed, and initial configurations are done. Day 2 is the stage when the product is available for customers, maintenance, re-configuration, and optimizations are done.

- Reduction of manual work
- Software updates

When a new version of a network component is ready, or when a new feature/interface is added to the component, these software updates should be in an automated way.

- Efficiently managing the disaggregated RAN components

When integration and validation developed components need to be done, then these new components should be plugged in the network in an automated way so that manual work will be as little as possible. For instance, a new RU should be integrated/added to the network, then it should be connected in an automated way.

- Efficient configuration

It is necessary to have a high level and user-friendly configuration. Configuration parameters such as vendor, frequency, interfaces and bandwidth should be set once before connection, then should remain vendor agnostic during the interoperability tests.

- Monitoring and optimization of the performance metrics such as signal quality, throughput, latency, and reliability.
- Fault management by focusing on detecting, diagnosing, and resolving issues that may occur within the disaggregated RAN components.
- Security management to protect the network infrastructure, user data, and services from potential security threads

2.2 ORAN Management

O-RAN Alliance accepts the definition of Management Service given in 3GPP TS 28.533. The examples of Management Services supported by O-RAN are listed in O-RAN Operations and Maintenance Architecture. Some of them are Provisioning, Fault Supervision, Performance Assurance, Trace Management, File Management, Software Management, etc. Figure 1 shows the relation between the O1 interface and O-RAN network functions. One of the architectural building block is the service management and orchestration framework. It is responsible for management and orchestration of the O-RAN network functions.

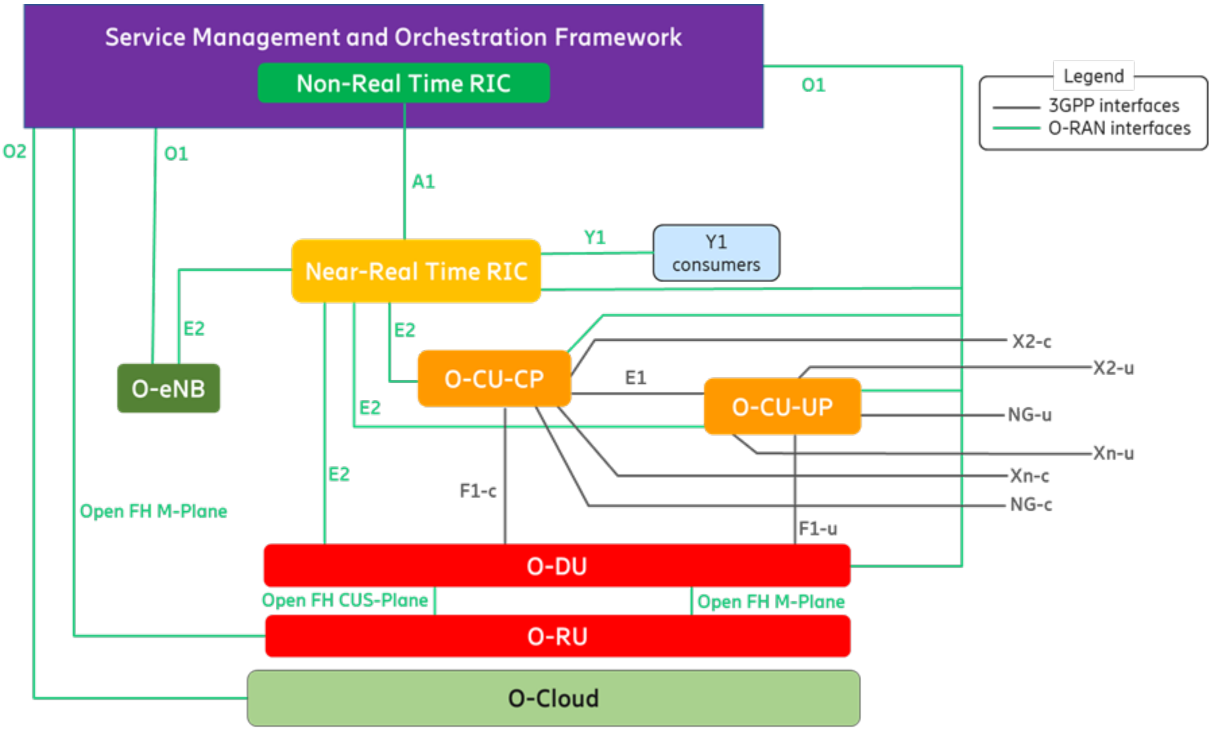

Figure 2: Logical Architecture of O-RAN with O1 Interface [2]

2.3 5G OPERA testbeds: implementation of network management

In this section we explain integration of O1 interface to the OAI and our view about security aspects of O1 interface.

2.3.1 O1 integration in OpenAirInterface

To investigate the concept of SMO and O1 interface in 5G-Opera testbeds, there is an integration of the O1 interface to the OAI software framework available, developed by Fraunhofer HHI together with Highstreet Technologies and the OAI Software Alliance. The implementation is based on a novel O1 adapter for OAI. The adapter, Figure 3, has been used to successfully connect an ONAP-based Service Management and Orchestration (SMO) system to OAI. The general architecture is shown in Figure 3. The O1-adapter for OAI currently supports (1) PM data reporting, (2) VES-based alarms and notifications, as well as (3) RAN reconfiguration based on the ONAP SDNC.

The O1 adapter has been successfully deployed in the Fraunhofer HHI testbed (cf. Figure 4). It has been already used to showcase all three above-mentioned features of the O1-adapter in a live-reconfiguration demo. In this demo, the monitoring functionality is used to report the number of connected UE, the total load in a base station, and total throughput of users in UL and DL. Moreover, the system is initially configured to 20 MHz and a load threshold is defined for the base station. Initially a single UE is connected that produces load lower than the threshold. When a second UE is connected, the load exceeds the threshold. A warning is consequently triggered in the ONAP system, and using the SDNC, the bandwidth of the system can be increased (in the demo to 40 MHz). It can then be observed that the load drops below the threshold again.

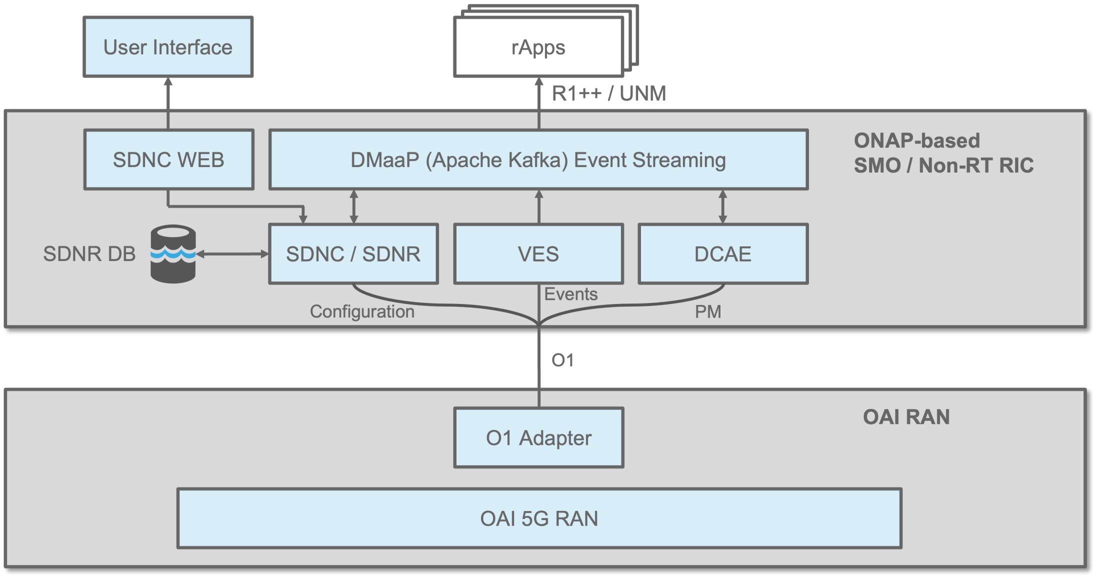

Figure 3: General architecture of ONAP and OAI integration using the O1-adapter.

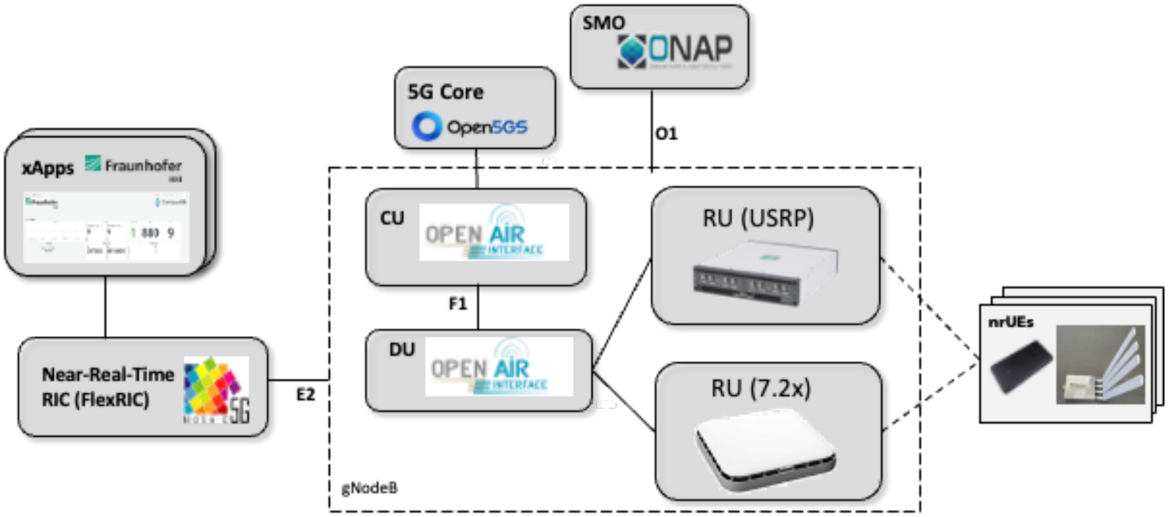

Figure 4: Current (Dec 2023) deployment architecture including ONAP and OAI-O1 interface (Fraunhofer HHI / 5G Berlin Testbed)

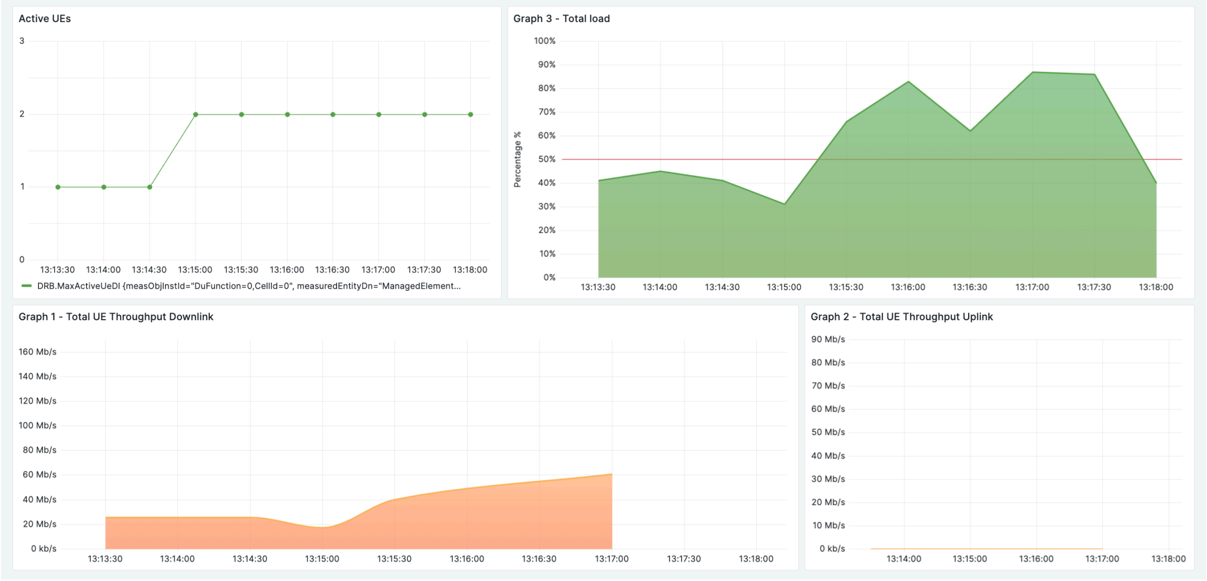

Figure 5: Grafana-based visualization of exemplary KPIs transmitted over O1 interface to ONAP system

2.3.2 O-RAN O1 and SW recommendations for Security

The O1 interface enables management of several components of the O-RAN architecture like nRT RIC, CU, DU and eventually RU. Then, security compromise of O1 can be critically harmful. As a first recommendation, since this interface uses NETCONF over SSH, it is important to configure the SSH service such that only NETCONF can be started through it. Without additional security measures, SSH could be exploited to allow the execution of any program.

Special attention is brought to O1 interface between O-DU and SMO. In addition to management, O1 is also involved in DU software installation, configuration etc., Therefore, TLS should be mandatory for the authentication of the O-DU and also for the NETCONF data exchange. A general recommendation in this vein is to replace SSH with TLS where data transfer is concerned.

Other general recommendations

Design and implementation of O1 interface should follow a “zero trust” approach, i.e. doing minimal trust assumptions about all stakeholders and components. Several mechanisms established by 3GPP and O-RAN security are optional (e.g., at the transport layer), opening vulnerability issues like information disclosure. Security and privacy should be implemented by default and not optionally. It is also recommended to enforce user authentication for the O-Cloud

Regarding software management, all apps should be written in secure programming languages like Rust. Specially to avoid attacks like memory overflow. Files should be encrypted not only during transmission, but also “at rest” or when they are stored permanently. Secure connections to external data sources also need to be defined. xApps/rApps should be specified in such a way that that they are clearly separable, while secure communication between rApps should be enabled. Even if it requires a higher effort for the developments, it is recommended to deploy formal verification of the O-RAN/3GPP specifications (and even better in the related implementations) during the software generation. That is an essential enabler of secure systems.

2.3.3 Further developments

Other Open RAN interfaces between core network and RAN (N2), between core network and UE (N1), and N3 and N6 interfaces for UPF core network function are also available from TU Dresden side. Apart from the integration of Open RAN with 5G core network, the integration of RAN from proprietary hardware suppliers like Nokia with 5G core network was also done in TU Dresden testbed. Integrated core networks are form OAI, Open5GS, and commercial GenuisCore. Moreover, different core network architectures also can be provided. These different architectures are local UPF based core network, monolithic and separated core network functions.

3 References

[1] Metaswitch, "What is an Open Radio Access Network (O-RAN)?," Metaswitch, 2020. [Online]. Available: https://www.metaswitch.com/knowledge-center/reference/what-is-an-open-radio-access-network-o-ran. [Accessed 2024].

[2] O-RAN, "O-RAN Architecture Description - O-RAN.WG1.OAD-R003-v10.00," 2023. [Online]. Available: https://orandownloadsweb.azurewebsites.net/specifications. [Accessed 2024].

[3] BubbleRAN Technology, "BubbleRAN," Eurecom, [Online]. Available: https://bubbleran.com/. [Accessed 2024].

[4] Open Network Automation Platform, Linux Foundation Projects, [Online]. Available: https://www.onap.org/. [Accessed 2024].

[5] ETSI, "Open Source MANO," ETSI, [Online]. Available: https://osm.etsi.org/. [Accessed 2024].

[6] QCT, "Quanta Cloud Technology," [Online]. Available: https://www.qct.io/. [Accessed 2024].

[7] Highstreet Technologies, "Highstreet Technologies Network Solutions," highstreet technologies GmbH, [Online]. Available: https://www.highstreet-technologies.com/. [Accessed 2024].