D2.9 ORANOS Final Report

Authors: Cellnex, Parallel Wireless, Satellite Applications Catapult, WeaverLabs.io, Attocore & University of Bristol

15/6/2023

Contents

Executive Summary 3
Introduction 4
ORANOS System Architecture 4
Deployment 5
University of Bristol 5
Weaverlabs 7
Record use in the ORANOs Project..8
Attocore 15
Parallel Wireless...19
Appendix 1 – Benefits Realisation 20
Appendix 2 – Lessons Learnt 29

Executive Summary

ORANOS's main motivation was to address key architectural and technological challenges for deploying end-to-end OpenRAN multi-domain (private-public) interoperable network solutions.

This will allow the creation of new business models that can be used for both Enterprise and public sector customers as well developing new use cases.

The project aimed in adding value to the OpenRAN Alliance specifications by particularly focusing on the emerging public and private 5G network multi-vendor Open RAN environment and their interworking challenges. To achieve this, O-RANOS leveraged the rApps and xApps development framework supported by the Open RAN architecture. The project aimed to develop x and r application templates that enabled APIs to interact with the A1 and E2 interfaces as well as Machine Learning production models (CNFs predictors). For example, a key focus for xApps development will be RIC based handover between public and private networks.

To extend further the opportunity of private-public interoperation, the project looked at implementing novel backhauling and neutral hosting services with a particular focus on satellite backhaul (mainly GEO and LEO constellations) for connecting to different core vendors.

In order to aid the development of further features, validate outcomes and accelerate deployment, ORANOS built an AppStore that will deployed and managed applications. One example was implementing a Zero Trust approach for security. ML training phase and production models will be leveraged as part of the AppStore offering.

Introduction

ORANOS looked at the development of x/r Apps, security model, and deployment of Apps to the RiC (Radio Interface controller) that would allow the sharing of network resources between a public and private networks.

The Use case described was a 'ESN' (emergency Services Network) SIM being used on it's home network being able to make calls on a Private Network when it's home network was no longer available, such as at a large port or a chemical plant.

The project also looked at the use of Satellite communications to provide backhaul to enable the use of 5G private networks on multiple sites using a single core or to enable the ability to switch messages between different back haul routes.

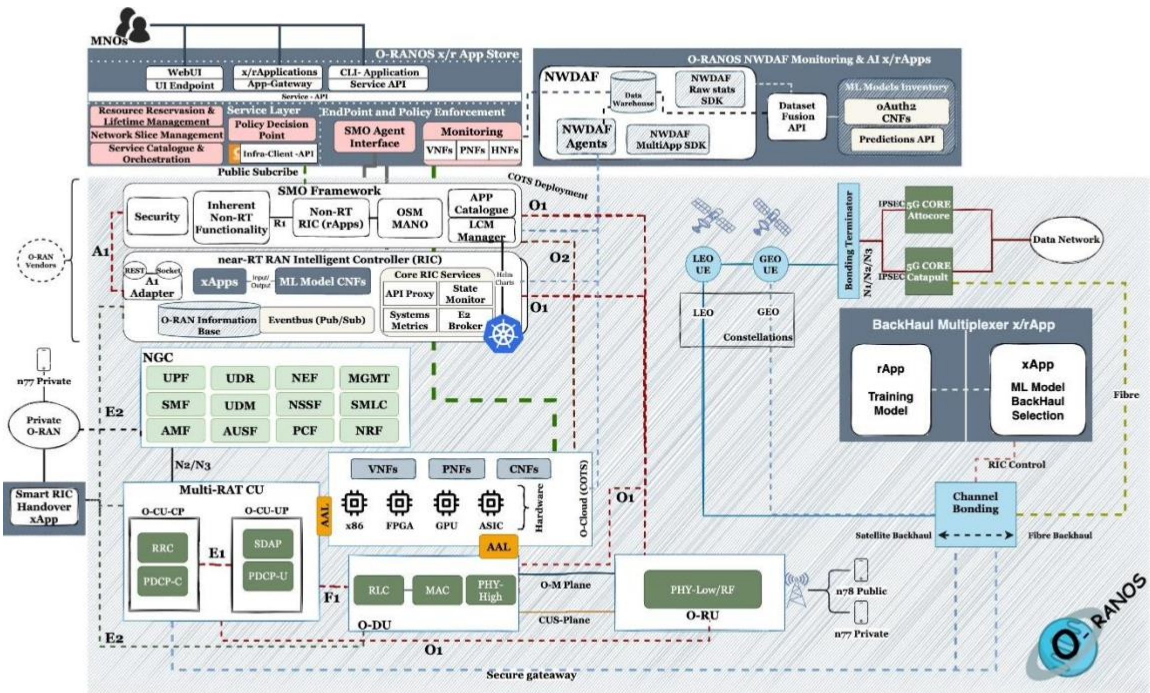
The partners in the project where Attocore, WeaverLabs, University of Bristol, Satellite Applications Catapult, Parallel Wireless and Cellnextelecom.

The O-RANOS system (Figure 2was broken down into 4 different areas of work: (i) the transport network units (RU, DU, CU, O-Cloud and NGC); (ii) the RIC software elements SMO and near-RT RIC; (iii) the external frameworks such as the x ,rAppstore; and (iv) xApps and rApps as individual subsets of the O-RANOS architecture (grey boxes Figure 1).

ORANOS System Architecture

O-RANOS proposes to generate demonstrated value overall in four areas of work.

Below we discuss the components where the main innovation will be carried out and describe them in further technical detail.



Deployment

The RAN (Radio Access network) was deployed in two locations, one in the centre of Bristol and the other at the Satellite Applications Catapult in Westcott.

The RAN used the same core and was connected to the Smart Internet Lab at Bristol University by both fibre and a LEO and a GEO Satellite connection.

University of Bristol

Introduction

The university of Bristol smart internet lab contributed in all work packages of the ORANOS project. In particular, the contributions were focused on design of the project HLDs and LLDs architectures, systems integration, use case development and testing.

ORANOS System Architecture

The project system architecture is comprised of several building blocks including physical assets, software components, integration components, connectivity endpoints and data collection and analysis. Physical Assets: These are the tangible resources involved in the project, such as hardware devices, equipment, or infrastructure. Examples include servers, sensors, actuators, or any other physical components required to support the system.

Software Components: These components encompass the various software elements that make up the system. They can include applications, modules, libraries, or frameworks that are responsible for executing specific tasks or functionalities within the project.

Integration Components: Integration components facilitate the seamless communication and interaction between different software components or systems. They provide the necessary interfaces, protocols, and middleware to enable data exchange, interoperability, and collaboration among the various elements of the project.

Connectivity Endpoints: These endpoints serve as the interfaces through which the project system interacts with external entities or systems. They can be physical interfaces (e.g., ports, connectors) or virtual interfaces (e.g., APIs, web services) that enable data transfer, control, or interaction between the system and external parties.

Data Collection and Analysis: This building block focuses on the mechanisms and processes involved in gathering and analysing data. It includes techniques for collecting data from various sources, such as sensors or databases, and utilizing analytical tools and algorithms to extract valuable insights, make informed decisions, or drive system optimizations.

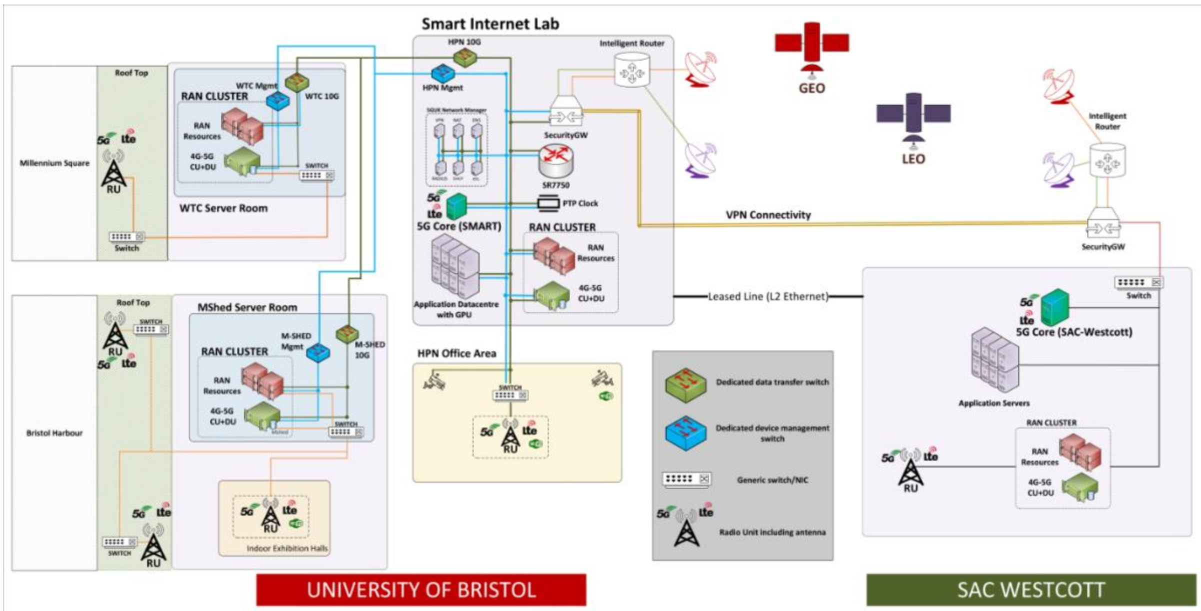


*Figure **X** ORANOS Overall Deployed Architecture*

In Figure X the building blocks are depicted which constitute the unique technical proposition of the ORANOS project and are described below:

1. Bristol Harbour RAN and Computing: Radios in different locations have been deployed to provide coverage around the area of the Bristol Harbour both for 5G and 4G devices.
2. Bristol City centre RAN and Computing: Similarly, coverage was provisioned in the Bristol city centre by deploying additional access networks.
3. Westcott Innovation Center RAN and Computing: A smaller 2 radio deployment was conducted for the Westcott facilities.
4. Facilities integration fibre leased line: The OpenRAN facilities in Westcott and Bristol have direct fibre communication.
5. Facilities integration with LEO Starlink terminal: The OpenRAN facilities in Westcott and Bristol have direct LEO satellite communication.
6. Network Orchestration: An SMO software deployed on the Bristol infrastructure orchestrates VNFs and CNFs on both facilities.
7. RIC Westcot installation: A near-real time RIC was deployed in the westcott cloud to orchestrate xApps
8. RIC Bristol installation: A non-real-time and near-real-time RIC was deployed in smart internet cloud to orchestrate x and r Apps.
9. NoSQL RIC database: A NoSQL database was configured to store real time RIC data

Conclusions

Weaverlabs

Weaver Labs work in this project has been focused on the following areas:

1. Deliver a cybersecurity strategy, expand the research and development of supply chain mapping, and further develop the cross-supply chain cyber security risk assessment tool, Record.
2. Expand the design of a Zero Trust architecture for cross-domain telecommunications infrastructure integration
3. Design a standard method, following secure processes, for x,rApp onboarding into the infrastructure
4. Develop bare metal infrastructure management to control the OpenRAN infrastructure from the orchestration

In the following we expand on the work delivered and the lessons learned.

A. RECORD development and testing

At the beginning of the ORANOS project, Weaver Labs' risk assessment tool was implemented and first developed as a prototype WebApp where we had the possibility to create a single organisation risk assessment. As part of our role as cybersecurity leads we decided to develop further this tool in order to assess supply chain mapping, and how complex supply chains such as OpenRAN would deal with it.

Record use in the ORANOs Project

The ORANOs project comprises a consortium of organisations that form a supply chain with one another, additionally each organisation works with other external parties to the consortium which extend the supply chain. This coalition of organisations will all have differing cybersecurity strategies yet the amount of collaboration in the project means that individual cybersecurity strategies may be threatened by other members of the supply chain. Therefore, the key objective of the use of Record within the ORANOs project is the developing and testing a comprehensive cyber framework for collaborative supply-chain.

Cybersecurity risks throughout the supply chain are the results of threats that exploit vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures within the supply chain itself.

Record aims to provide a holistic cybersecurity strategy throughout the ORANOs consortium by reviewing the current strategy or profile to identify threats, and then mitigating these threats by providing controls to bring each organisation to the target profile necessary for the project.

The core components and definitions of a supply chain are as follows:

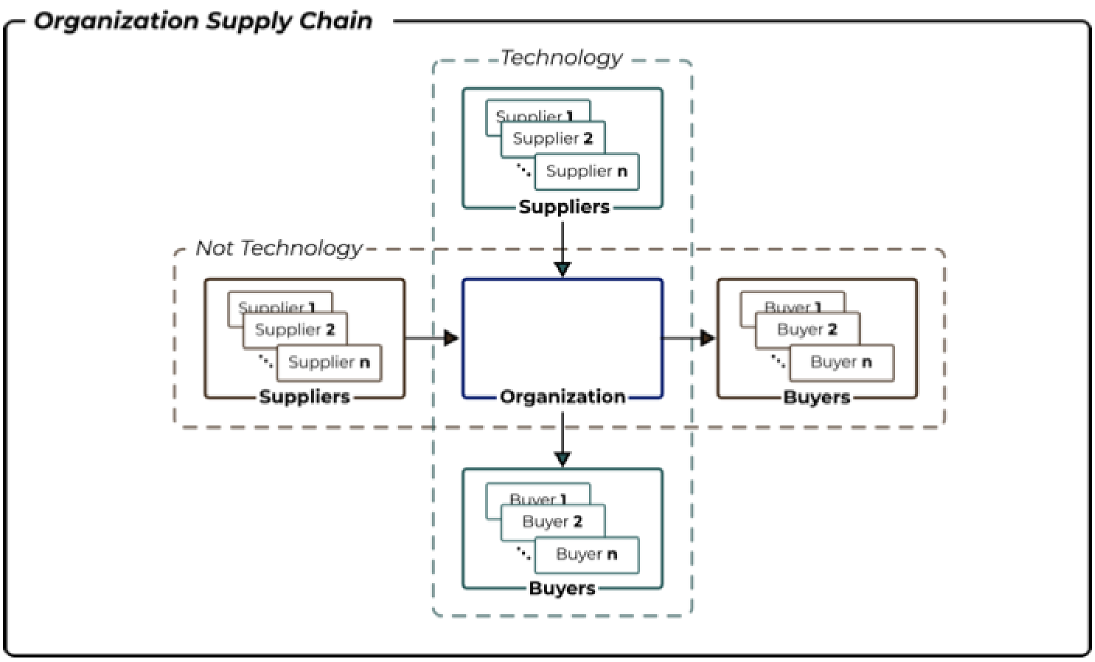
Supply Chain
the set of resources and processes shared between and among multiple levels of an enterprise forming a relationship or chain in the form of supplier and buyer. An enterprise creates a dependency chain on the supplier during the sourcing of products and services which extend to the buyer and the product/service lifetime.

Actors
The set of agents an organisation interacts with during the pursuit of its business mission or product/service development.

Roles
A grouping of functions an actor can perform within the supply chain. Roles can have a set of agreed-upon interactions. supply chain. In the simplest case, this is the set of actions between a buyer and supplier.

Understanding relationships amongst stakeholders within the supply chain can inform a cybersecurity posture and assist in the minimization of counterparty risk.

The following was used to define the supply chain:



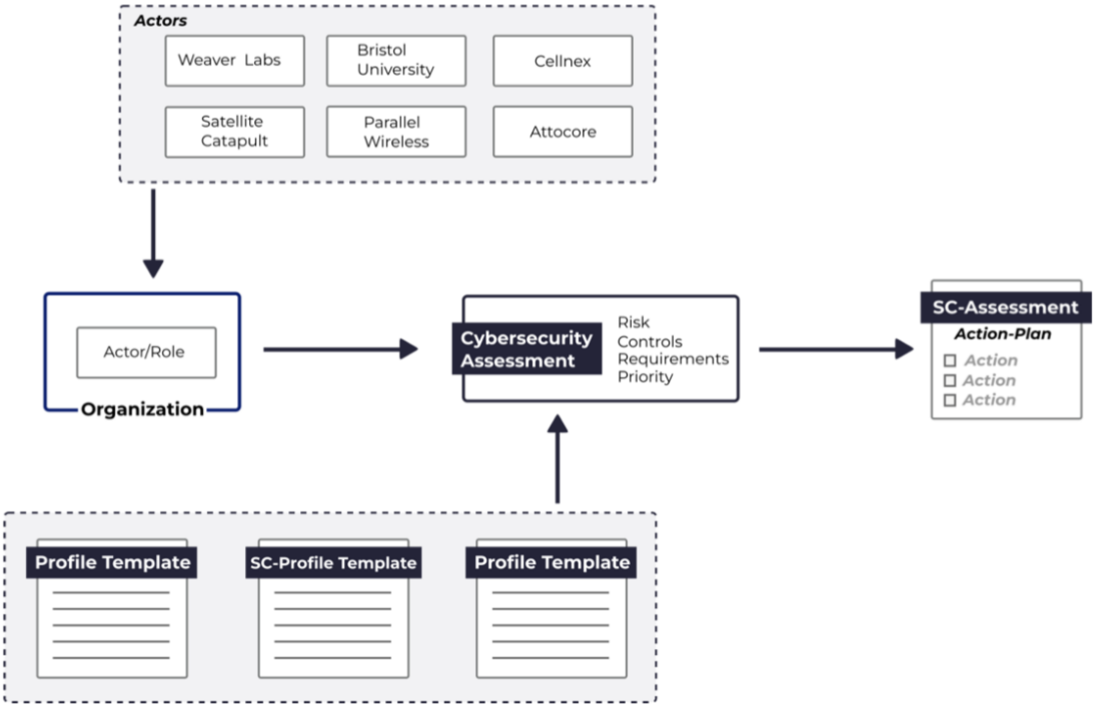
The organizations stakeholder dependency/relation chain

In reality, these relationships are often tightly bound and their interactions can be challenging to identify, initially.

Once the actors and their roles within the supply chain are identified, we can build profiles within Record that distinguish certain functions and categories from the cybersecurity frameworks that are relevant to that specific role within the supply chain, ensuring that the assessments are correctly targeted to each organisation with the following workflow:

1. Identify the Actors and roles
2. Using Record, extract the relevant policies to serve as a template.
3. Each organisation completes an assessment based on a templated supply chain org profile

The overall use for ORANOs is shown in the below image:



The organizations use of a templated profile and Record

An example profile for an organisation within a supply chain that we can apply to the consortium members in the ORANOs project is "Supply-Chain-Assessment" which uses the following NIST controls to make up the profile:

Term	Definition
Identify: Business Environment	
ID.BE-1	The organisation's role in the supply chain is identified and communicated.
ID.BE-2	The organisation's place in critical infrastructure and its industry sector is identified and communicated
ID.BE-4	Dependencies and critical functions for delivery of critical services are established.
Identify: Governance	
ID.GV-1	Organisational cybersecurity policy is established and communicated.
ID.GV-2	Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and

	external partners.
ID.GV-4	Governance and risk management processes address cybersecurity risks
Identify: Supply-Chain	
ID.SC-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders
ID.SC-2	Suppliers and third party partners of information systems, components, and services are identified, prioritised, and assessed using a cyber supply chain risk assessment process
ID.SC-3	Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organisation's cybersecurity program and Cyber Supply Chain Risk Management Plan.
ID.SC-4	Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
ID.SC-5	Response and recovery planning and testing are conducted with suppliers and third-party providers
Protect: Data Security	
PR.SD-4	Adequate capacity to ensure availability is maintained
PR.SD-6	Integrity checking mechanisms are used to verify software, firmware, and information integrity
PR.SD-7	The development and testing environment(s) are separate from the production environment
PR.SD-8	Integrity checking mechanisms are used to verify hardware integrity
Protect: Information Security Processes	
PR.IP-1	A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)

Detect: Anomalies and Events	
DE.AE-5	A baseline of network operations and expected data flows for users and systems is established and managed
Respond: Communications	
RS.CO-1	Personnel know their roles and order of operations when a response is needed

Cybersecurity results and lessons learned:

1. The development process suffered some setbacks because of hiring problems. We had to use contractors to develop the tool which ended up being a costly and very difficult way to manage the product development. In the end we managed to find a full time front end developer who has been vital for this development.
2. We circulated the tool amongst all partners and each partner successfully received an assessment view and an action plan to improve their Supply Chain risks. However some key issues encountered during the process where:
    a. Having a buy-in from security teams within the organisations was a challenge. Since the ORANOs project does not involve members working on development of organisational security strategy, the risk assessment process was very difficult to achieve.
    b. Some organisations gave good feedback about the complexities of understanding how to proceed with the risk assessment and answering the policies, which helped us shape the user guide and give better examples in order to alleviate these concerns.
    c. Security is far from being considered an integral approach. Our main conclusion is that applying Zero Trust to Telecoms architecture if we cannot conduct adequate supply chain risk management will be a patchy solution that doesn't solve key cybersecurity issues in the OpenRAN architecture, and therefore will impact mass adoption.
    d. Security scoring and regulator interventions can be a good way to solve the lack of engagement with the industry.

B. Zero Trust architecture

The principle of Open RAN itself and software platforms in general is based on open interoperable interfaces, also known as Open APIs. In Open RAN the entire radio network does not depend on one single vendor, rather multiple components from different suppliers that can communicate with each other through the defined Open APIs. This, coupled with the number of end-point APIs that are exposed to integrate the different components of Open RAN, result in classic perimeter security models being not fit for purpose. This allows mobile network operators to reduce costs in deployments, and mitigate the security risk of national dependency on a small number of suppliers, given that it inherently allows many more suppliers to exist. Moreover, perimeter models have been useful for entire infrastructures that do not require integration with other infrastructures outside of their own domain. However, with the rise of neutral hosts and 5G private networks, infrastructure integration and shared infrastructure models are the new norm.

Unlike the perimeter security model, in a zero-trust network an individual inside of a network is not assumed to be trusted and must continue to authenticate *everywhere* and for *every* request. Together, identification achieved through authentication and access control based authorisation can help an organisation move towards the zero-trust model of security.

The relevant components in Cell-Stack that take care of the Zero Trust principles are contained in the Identity Manager Service (IdM) and in the Monitoring and Data Aggregation (Mon) service.

Zero Trust Principles rely heavily upon the proper monitoring of networks, users and devices. Cell-Stack is being developed with monitoring as a separate functional component of the MANO architecture. Unlike in the ETSI NFV architecture, CellStack creates a standalone set of monitoring microservices in order to properly address the Zero Trust monitoring related principles as outlined below.

- Know your architecture including users, devices, and services
- Know the health of your devices and services
- Focus your monitoring on devices and services

In the ORANOs project we focused on the design of Monitoring for the Virtual Infrastructure Management (VIM) and the Metal Infrastructure Management (MIM) and the design of the monitoring reference points.

Monitoring - Metal Infrastructure Manager (Mon-Mi)

This reference point is responsible for

1. Forwarding of virtualized resources state information.
2. Forwarding Hardware resource configuration and state information exchange.
3. Forwarding virtualized and physical host metrics
4. Endpoint event requests (resource allocation requests) and debugging.

Monitoring - Metal Infrastructure Manager (Mon-Mi)

This reference point is responsible for

1. Forwarding of virtualized resources state information.
2. Forwarding Hardware resource configuration and state information exchange.
3. Forwarding virtualized and physical host metrics
4. Endpoint event requests (resource allocation requests) and debugging.

A first high-level integration of the Mon-Mi was implemented and integrated to the orchestration in order to retrieve real-time information from the metal infrastructure.

C. Secure x,rApp onboarding

Our third security objective was to define a standard “entry door” for all the software in the network. Defining standard onboarding processes, with clearly defined descriptors and file structures allow to mitigate security risks of compromised software being deployed and run in the network. This becomes extremely important with the rise of integration of Apps in the network, that can incorporate sophisticated elements like AI or ML and compromise key network functions.

Finding a common framework for deploying network function helps the industry, and in particular OpenRAN deployments in the following:

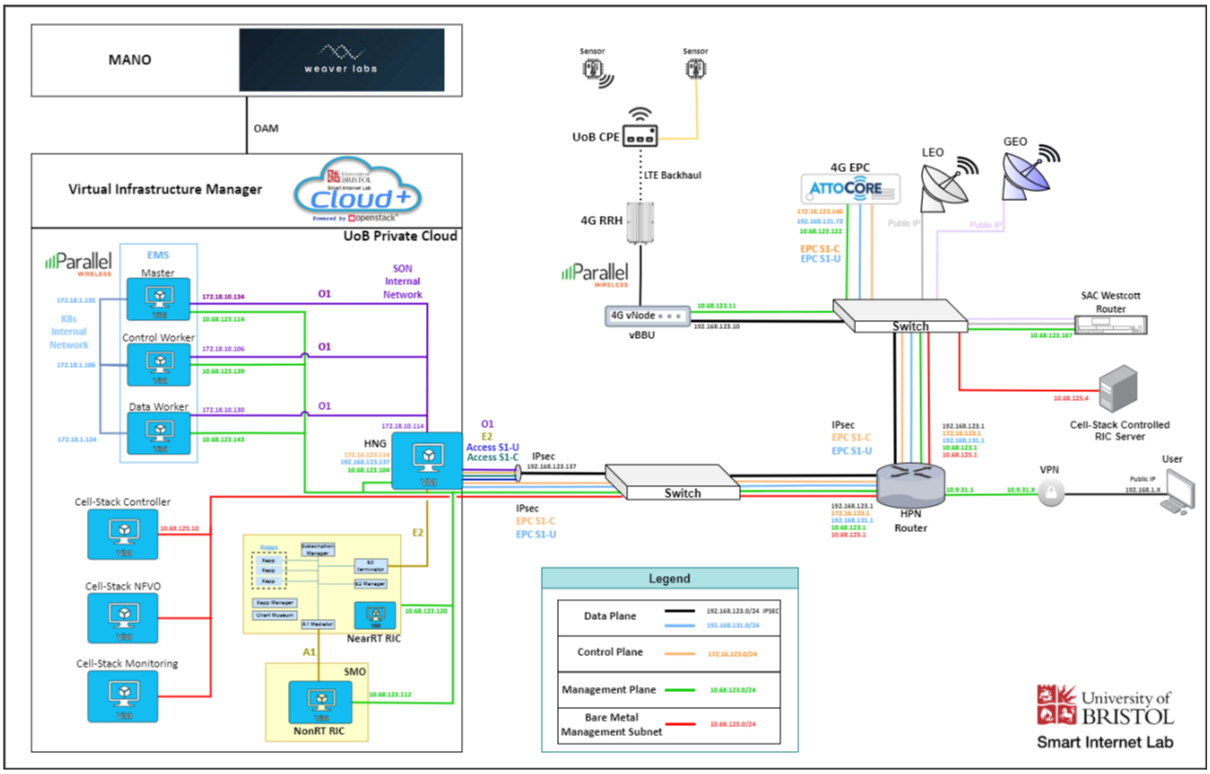
1. Creates a common language based on standards (ETSI-NFV) that everyone in the industry can follow
2. It simplifies onboarding and deployment of software components, building on the case for open and interchangeable networks - a core objective for OpenRAN
3. It provides the necessary tooling for security checks as it reduces the risk of code injection or instructions that can impact the network security

Results and lessons learned:

- We worked collaboratively with UoB to identify the RIC requirements to onboard the network functions related to x,rApps. We identified that there was a tight integration with the RIC required since these Apps reside within the RIC and follow design principles set out by the components of the RIC. We documented all the work in Deliverable 5.3.3.
- Key findings for x,rApps are that the management and deployment of the x,r Apps will be outlined by the RIC, and the orchestration framework will treat the RIC as a VNF (with a similar procedure as outlined above). Further collaboration between RIC software and higher layers orchestration software is required to create interfaces that can allow for ad-hoc creation and deployment of x,r Apps. At the moment we see a limitation in the architecture to completely decouple the RIC from the x,rApp onboard and deployment.
- Given the lack of activities in the standardisation bodies to bring closer ETSI-MANO orchestration and management principles to the O-RAN alliance development, as well as the lack of openness of the RIC we have in the project, the work we developed in this context had to conclude in the design.

D. Orchestration software for Bare Metal management

Lastly, as part of this project Weaver Labs provided the orchestration software for the network, integrating into the architecture as follows:



Cell-Stack infrastructure layer integrates a novel mechanism to manage and orchestrate bare metal resources, by leveraging Metal as a Service. Since the entire PW software is running in bare metal, the team had to integrate the Metal Infrastructure Management (MIM) endpoints to the UoB private cloud. After several issues with operating system compatibility, we successfully managed to integrate cell-stack MIM endpoints to the bare metal infrastructure, as seen in the following screenshots:

```
ubuntu@cell-stack-controller:~$ nmap -sn 10.68.125.*
Starting Nmap 7.80 ( https://nmap.org ) at 2023-06-01 15:40 UTC
Nmap scan report for _gateway (10.68.125.1)
Host is up (0.0020s latency).
Nmap scan report for 10.68.125.5
Host is up (0.00049s latency).
Nmap scan report for host-10-68-125-10.openstacklocal (10.68.125.10)
Host is up (0.00014s latency).
Nmap scan report for 10.68.125.180
Host is up (0.00056s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.75 seconds
ubuntu@cell-stack-controller:~$
```

FQDN ∨ | MAC IP	POWER	STATUS	OWNER TAGS	POOL NOTE	ZONE SPACES	FABRIC VLAN	CORES ARCH	RAM	DISKS	STORAGE
Deployed 2 machines										—
VBBU-MSquare.maas 10.68.125.5 (PXE)	On Ipmi	CentOS 7	admin -	default	default	fabric-0 Default VL...	48 amd64	95 GiB	1	256.1 GB
VBBU-1.maas 10.68.125.4 (PXE)	Off Ipmi	Ubuntu 20.04 LTS	admin -	default	default	fabric-0 Default VL...	56 amd64	128 GiB	1	4 TB

Attocore

In support of the project objectives a mobile wireless network was to be deployed to provide the required mobile wireless connectivity. This connectivity was required to underpin mechanisms for handover between public and private networks and also to test the possibility of switching backhaul technology from terrestrial to satellite.

At the start of the project a 4G/LTE network was deployed in both lab and field environments. Multiple instances of AttoCore's 4G Core (AttoEPC) was also deployed to enable end-to-end 4G connectivity and technical support was provided. AttoEPC is a well-established commercial product and so there was no further development required.

Later in the project, a 5G RAN network was deployed in both lab and field environments.

Multiple instances of AttoCore's 5G Core (Atto5GC) was also deployed to enable end-to-end 5G connectivity and technical support was provided.

Additional 5G core developments were required and in the course of the project the following features were added to the Atto5GC capability:

Handover design & development,

Intra-CU Mobility

- Move between cells controlled by the same RAN CU

Relocation

- Move between gNodeBs while not actively transmitting traffic
- gNodeBs may be connected to the same or different AMFs

Xn Handover

- Move between gNodeBs while actively transmitting traffic
- gNodeBs must be connected to the same AMF

N2 Handover

- Move between gNodeBs while actively transmitting traffic
- gNodeBs may be connected to the same or different AMFs

Kubernetes enhancements:

Atto5GC can run containerised in the cloud or distributed. Kubernetes enhancements enable or improve:

- Performance running the Atto5GC in the cloud.
- Distributed as Docker image and Helm Chart
- Simplified installation (I.e: helm install atto-5gc atto-5gc-helm.tgz [options]
- Extensively tested on Kubernetes 1.23
- Tested on clusters from AWS, Linode, WindRiver, Kind

Prometheus enhancements:

Addition of a number of new counters and enhancements for export of KPI data for performance monitoring:

- Create Dashboards to monitor KPIs in the Atto5GC
- General workflow:

- Count metrics in the Atto5GC
- Export metrics using Fluentd
- Accumulate metrics in Prometheus
- Create dashboards in Grafana

IPv6 design & development:

To enable devices to connect to the network and utilise any advantages of IPv6

Satellite Applications Catapult

Satellite Applications Catapult (SAC) primarily aimed to incorporate satellite technology into the O-RAN ecosystem, with a focus on backhaul multiplexing and neutral hosting, as part of WP 6. This involved creating a hybrid satellite-terrestrial backhaul network, connecting the O-RAN to the Core Network, enhancing resilience and availability through the use of diverse backhauling technologies. The usage of these technologies was intended to be managed by the RAN Intelligent Controller (RIC), with assistance from one or more xApps. Another key aspect was exploring and demonstrating the deployment of Neutral Host within O-RAN.

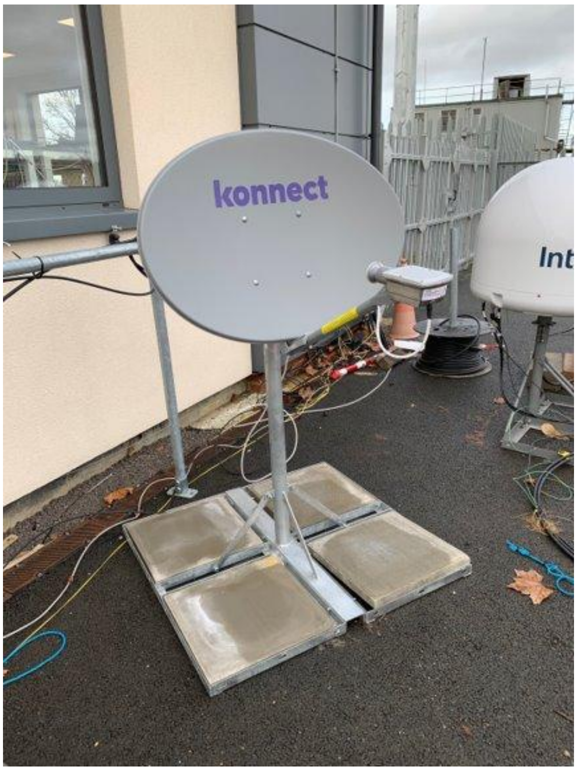


Figure 1 GEO terminal at Westcott

Figure 2 LEO terminal at Westcott

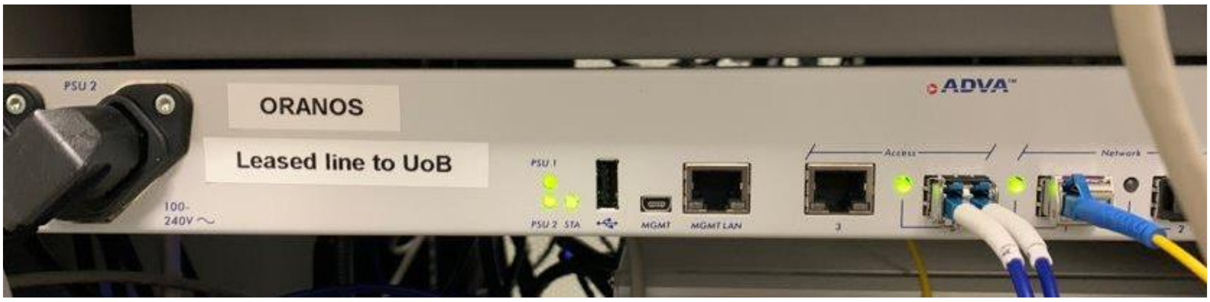


Figure 3 Leased Line termination at Westcott

Challenges arose with the staging lab integration with satellite backhaul, where the LEO satellite and the leased line between Bristol and Westcott had some delays on their corresponding service provisioning. However, a successful live demonstration of the GEO satellite link, LEO satellite link and Leased Line integration with the testbed was eventually conducted at the University of Bristol.

Despite technical challenges with the xApp/rApp framework and Juniper's RIC, an alternative RIC was developed. The implementation test and validation confirmed the live status of the satellite backhaul, its ability to pass traffic between environments, and successful integration of multiple backhaul links.

Figure Multi-backhaul usage dashboard

Finally, the project demonstrated a live hybrid backhaul controlled by network applications. This highlighted the use of satellite and fibre connectivity for backhauling and how RIC and xApps manage these technologies. Furthermore, the project examined the impact of the Neutral Host environment and hybrid backhaul service on various use cases, ending with the demonstration of an xApp used to redirect multiple users through the predefined backhaul link.

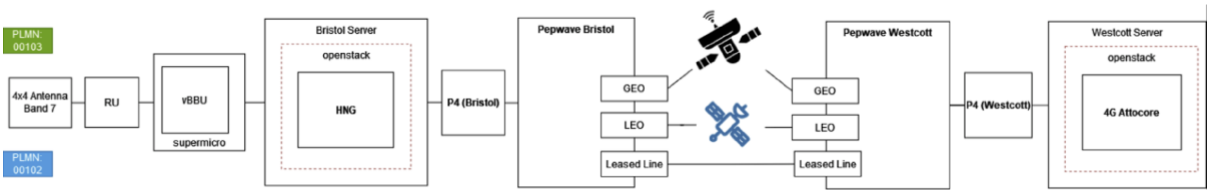


Figure SAC Testbed scenario

Parallel Wireless

Parallel Wireless project goal was to deploy a stable test network as an enabler for the project partners to achieve their deliverables. An initial 4G band 7 deployment was established covering 3 core outdoor sites (MShed East, MShed West, and We The Curious) a single cell was deployed into the smart internet lab at the University of Bristol and a further two cells were deployed at Satellite application catapult in Westcott, one being a fixed node and the other a nomadic node as pictured.

Juniper RIC instances were deployed and the cells were able to be moved between multiple cores to support the partners test objectives.

Late in the project stage a 5G cell was implemented into the University of Bristol smart internet lab unfortunately due to hardware availability a supply chain issue meant that this was too late for a full retest of the partners objectives.

Appendix 1 – Benefits Realisation

Project%20Status%20and%20Benefits%

Benefit ID	Benefit owner/ Beneficiary	Enabler	Benefit Name	Benefit description	Benefit type	KPI type	KPI to provide	Measurement start date	Measurement end date	Baseline	Target	Frequency of measurement	Updates
FRANCBen01	UoB Weaverlabs Parallel Wireless	Organisations looking to adopt 5G and O-RAN	Streamline system integration	By reducing the complexity in system integration, network upgrades and scalability we contribute to the wider benefit of accelerating adoption of 5G and O-RAN. This project invests £3.2M in solving these issues by working on standardised processes for	Qualitative	TRL	Compare previous case studies to user feedback. TRL 7	01/01/2022	30/06/2023	There are existing challenges around working with multiple suppliers in an already complex supply chain, which can deter large organizations from adopting a diverse supply chain strategy TRL 3	A standardised processes for onboarding Apps, automate functionality integration and deployment as well as integrate all O-RAN APIs into a single management framework. TRL 7	Quarterly	TRL 5: Component has been validated in relevant environment for Cell-Stack Metal Infrastructure Management, we expect the project to advance this to TRL 7. **To be updated once project closure report submitted with final results and TRL**

				onboarding Apps, automate functionality integration and deployment as well as integrate all O-RAN APIs into a single management framework.								
FRANCBen03	UoB Parallel Wireless Attocore Weaverlabs SATC	Project partners and suppliers	Early exposure to partner functionality and integration opportunities	By being involved in a research and development project, project partners will have early exposure to emerging functionality and integration opportunities within the 5G O-RAN sector. They will have the opportunity to help shape regulations for the	Qualitative	Improved interoperability	Accessibility to new functionality in comparison to competitors not involved in the project E.G x/r Apps	01/01/2022	30/06/2023	There are ongoing challenges for various suppliers to access the latest and most up to date functionalities	An environment where project partners can utilise new technology exclusively whilst it remains within a "test" environment	Start/End	ORANOS Project Partners have worked well together to share innovation and ideas. The use of 5G and O-RAN at UoB testbed has attracted interest from the Baltic Delegation. This is a soft benefit and will not be measured by final results or TRL's. **This benefit has been realised as the partners have worked successfully and collaboratively on this project**

				sector moving forward									**and will continue to do so going forward**

FRANCBen 04	SATC UoB Parallel Wireless	End Users	Hybrid network connectivity	By providing end to end network connectivity through means of hybrid satellite and fibre backhaul links we will be able to demonstrate and challenge network resilience.	Qualitative	TRL	TRL 6	01/10/2022	30/06/2023	Currently providers only provide one backhaul option. TRL 3	Provide several backhaul options and the ability to switch between options to support resilience and offloading. TRL 6	Quarterly	The hybrid backhaul network (LEO, GEO and leased line) is live and bidirectional traffic can be passed between the University of Bristol (UoB) and SA Catapult sites. The xApp can be used to select the appropriate bearer (satellite or fibre). This is detailed in Deliverable 6.8 section 2 where the concept of Hybrid backhaul and the management of the switch over is detailed. The Visualisation Dashboard provides real time display of the link usage along with bandwidth consumption by each UE and the different backhaul links. This is detailed in the same report (figure 4) and shared in the final presentation. **To be updated once project closure report**

													submitted with final results and TRL

FRANCBen05	SATC Attocore UoB Parallel Wireless	End Users/ NH providers	Neutral Hosting	Implementation of Neutral Hosting to both the Catapult and Attocore 5G Core Networks to further demonstrate a resilient connectivity for end users and providing both private and public networks.	Quantitative	Improved interoperability	Improved network speeds and resilience	01/10/2022	30/06/2023	No neutural host network	Neutral Host with ability to provide both private and public network connectivity TRL 6	Quarterly	the radio in University of Bristol is currently configured in a Multi Operator Core Network (MOCN) setup, broadcasting live two PLMNs each one connects to a different core networks, one locally in Bristol and the second over the multi backhaul link at westcott. Using the MOCN, core networks can share the same RAN resources. The successful deployment of the NH scenario can be verified from both the UE and Radio (HNG) nodes. As shown in D6.8 Figure 6, HNG is connected to both peer Attocore MMEs, UoB and Westcott, and monitors the health state of the path. Figure 7 in D6.8 provides more details on the connection to each core, such as number of

												subscribers connected, PLMN information and health state among others. **TRL 6 achieved**
FRAN CBen 06	Cellnex	Development of an integrated software platform that integrates a multi-vendor OpenRAN network	Economic case for new business cases using Open RAN	The reduction of operational cost of network administration and cost to scale the network improves the economic case for Small Cell deployment	Quantitative	Cost benefit	Small Cell cost	15/01/2023	30/06/2023	Small Cell cost for single MNO use (£4,878)	Small Cell cost split by 4 (all 4 MNO's sharing one cell - £1,219.50)	One time	The aim of the project was to develop a way of sharing network resources between both public and private networks. The project has shown that this will be possible with future development of ORANOS and future updates to the RiC. This is something that we (cellnex) will continue to pursue with additional projects and within our small

													cell rollout. **Cost benefit outlined, full benefit will not be realised within the FRANC lifecycle due to RiC limitations**
FRANCBen07	Weaver Labs, Parallel Wireless, UoB	Development of a standard onboarding process for all software elements: OpenRAN network functions and x,r Apps	Streamline system integration	The reduction of necessary operational tasks to onboard software elements into the infrastructure by adding a standardised onboarding process	Quantitative	TRL	TRL 6	15/01/2023	30/06/2023	Number of different operational tasks needed to onboard all the software components into the platform to make them run TRL 3	Unification of Operational tasks and network management processes to onboard software elements into the platform TRL 6	One time	TRL 3: design of secure onboarding has been finalised, proof of concept in UI, but not possible to develop more given lack of integration with RIC. **To be updated once project closure report submitted with final results and TRL**

FRANCBen08	Cellnex, Weaver Labs	Collaborative cybersecurity risk management approach for multi-vendor supply chain	Cybersecurity risk management	The ability to create a cybersecurity strategy that comprises multiple profiles from the supply chain, allowing for a uniformed approach to cybersecurity across all suppliers, increasing the overall security of the project	Qualitative	Improved management of cybersecurity risks	Compare previous risk management processes to new one	01/10/2022	30/06/2023	No collaborative cybersecurity strategy and uninformed risk level within the supply chain	Increased visibility of cybersecurity risks generating more transparency in the supply chain. A uniformed approach to preventing and tackling cybersecurity attacks. **Each partner to complete an assessment of current cybersecurity principles, with a target to improve the score**	Quarterly	Some partners have completed the risk assessment. Maria to assess results and confirm outcomes. **To be updated once project closure report submitted with final results and TRL**

Appendix 2 – Lessons Learnt

Lesson ID	Lessons description	Permission to share with wider public audience (Full)/just DCMS (Internal Only)	Lesson Type	Date	What does the lesson tell us?	Who is the audience for the lesson?	Stop/ Start/ Continue	What needs to change as a result of this lesson?	What can you do to ensure the lesson is acted upon or shared?	Who owns these actions?
1	Start review cycles for deliverables earlier	DCMS internal	Project management	25/5/22	That documentation needs to be reviewed collaboratively and ahead of any deadlines	Project Management Teams	Start	Better planned review cycles	Include review cycles in the project plan and share final version	Cellnex
2	Give ourselves more time to gather evidence for grant claims	DCMS internal	Project management	25/5/22	The grant claim process can be time consuming	Project Management Teams	Start	Collate grant claim evidence earlier	Ensure all project partners understand exactly what is required. DCMS to outline requirements clearly	Cellnex
3	Make sure any NDA or inter-supplier security measures required are known	Full	Project management	25/5/22	Getting several partners to agree to an NDA can be time consuming	Project Management Teams	Start	Outline any requirements like this at the start of the project	DCMS to share with other FRANC projects. Extra vigilance with US suppliers involved as they tend to be a higher risk	Cellnex
4	Product line compatibilities across different suppliers	Full	Supply Chain	25/5/22	Proof of concept should be completed to confirm that different pieces of hardware are compatible	3rd Party Suppliers	Start	Proof of concept should be completed to confirm that different pieces of hardware are compatible	DCMS to share with other FRANC projects.	Cellnex

5	LEO Satellite providers	Full	Supply Chain	8/3/2022	There is currently only one LEO Satellite supplier in the UK who do not provide the required service. Suppliers for all aspects of the project should be researched and confirmed in advance	Project Management Teams	Start	Suppliers for all aspects of the project should be researched and confirmed in advance	DCMS to share with other FRANC projects. Extra vigilance with specialist suppliers involved as they tend to be a higher risk	Cellnex
6	Variations in Grant Claim Process	DCMS internal	Project managemen t	8/3/2022	The DCMS Grant Claim process can be complicated as we are working with multiple partners who all have different agreements/fundin g budgets	Project Management Teams	Start	All partners assigned to a project should work with the same or a very similar agreement	DCMS to create more in-depth guidelines to be shared with all partners, not just the project lead, ahead of project initiation	DCMS

7	The standardisation development of Open RAN interfaces doesn't currently allow for the app store functionality to be developed in a way that will be aligned with future implementations of the RIC	Full	Technical	8/15/2022	The x,rApps are specific components that run in the RIC. For the orchestration layer to be able to control the onboarding and deployment of x,r Apps in a similar way as an Appstore would do, the Orchestration layer (sitting on top of the SMO) should have direct communication with the RIC interfaces as well as exposure of control functions from the SMO to a higher layer orchestration. As it currently stands in the O-RAN Alliance and the development of the RIC the control of x,rApps from an end-to-end resource and service layer orchestration cannot be developed. The first reason is that O-RAN Alliance is not working in tandem with ETSI standards, and there is no mapping from one to the other. The second reason is that RIC manufacturers do	Technical development, product development, strategy	Start	The service layer of Cell-Stack cannot integrate with the RIC and OpenRAN as our product roadmap was expecting. We cannot force the Vendors to provide open APIs. This is a major issue for the industry, if we're looking to open up the supply chain outside of the core RAN network functions and allow for x,rApps to be developed by 3rd parties. Also, the RIC is becoming a big bottleneck of innovation in OpenRAN - wihout APIs to integrate into end to end service layer management tools (such as cell-stack) it will be very difficult to obtain multi-domain network	Communicate the issue to the RAN vendors who can pressure RIC manufacturers not to contribute to vendor lock-in in the SMO framework. Communicate the issue with DCMS to raise this as a problem that can impact wider strategy within supply chain diversification. Communicate with RIC manufacturers that SMO and higher layers of orchestration must be designed to work together	Weaver Labs, Cellnex

					not contemplate integration with higher layers of control software, which will prevent development in disaggregation in the future. This is also a cybersecurity concern as standard checks for software packages cannot be done through an onboarding process			integration and adequate supply chain disaggregatio n		

8	The juniper RIC does not deliver what was expected in terms of UE data, which impacts the development of x,rApps in the project	Full	Technical	8/15/2022	As part of the development of the x,r Apps, we require a constant stream of information from the RIC to make informed decisions. At it's current state the RIC doesn't export the required UE data the project needs to conduct the ML and backhaul switching based on RIC data. As the project evolves, we see how the RIC is in very early stages of development, and also how dependent any intelligence brought to the OpenRAN via x,rApps depends on the RIC chosen	Technical development, product development, strategy	Start	The design of the data feeds to support the development of the x,r Apps has to change, and instead of feeding data directly from the RIC, the x,rApps will receive data directly from PW RAN components	Communicate the issue to the RAN vendors who can pressure RIC manufacturers not to contribute to vendor lock-in in the SMO framework. Communicate the issue with DCMS to raise this as a problem that can impact wider strategy within supply chain diversification. Communicate with RIC manufacturers that SMO and higher layers of orchestration must be designed to work together	UoB, Weaver Labs, SATC, PW, Cellnex

9	While migrating the cybersecurity tool from excel to a WebUI, we have encountered a number of resource issues working with subcontractors. This has led to 2 months delay in the readiness of the tool as well as changes in the product roadmap and timelines for testing	Full	Technical	9/30/2022	In order to use the cybersecurity framework designed by Weaver Labs, the tool needed to migrate to a WebUI. After a good design process and successful mobilisation of the project, the work with the subcontractors became a big issue to deliver the tool as per the original project plan. The main issue has been the subcontractor's skills where not sufficient to deliver. The choice to go for a subcontractor was forced because of the lack of talent in the UK that can deliver front-end at a reasonable price. The lack of technical talent in the job market makes salaries grow exponentially, making it impossible for start-ups to hire talent and compete with large tech companies (with deep pockets)	Technical development, project management, operations management	Continue	The development timelines had to be adjusted, the budget had to increase (x3) and the feature release had to be adjusted	Communicate to DCMS that the job market and lack of tech talent is a barrier to deliver solutions fast. If the UK wants to compete with US tech start-up ecosystem we must have a competitive job market	Weaver Labs

10	Cybersecurity approaches are not consistent within each of the project partners, making a unified approach across the project very challenging	Full	Partnerships	1/25/2023	Different parts of the supply chain have different focuses and approaches to cybersecurity	Project Management Teams, 3rd party suppliers	Start	A greater focus needs to be given to cybersecurity from the start. A pre-project could take place to ensure all suppliers can align before entering into the project together	Communicate with DCMS that more time is required to ensure that project partners align before entering into an agreement together	Cellnex
11	Task based planning vs Gantt chart planning	Full	Project management	1/25/2023	ORANOS was originally set up with a Gantt chart based plan. This has been incredibly hard to maintain, as each of the project partners have been able to work in an Agile way, meaning tasks have been completed outside of the original planned order. The various work packages completed by each of the project partners are not necessarily dependent on each other, meaning the plan is very fluid and constantly changing	Project Management Teams	Start	Use task based planning with a greater efficiency for dealing with changes	Any R&D projects to be set up with a task based plan rather than a Gantt chart based plan	Cellnex, DCMS

12	Collection of data and UE/radio statistics is limited and challenging in order to build proper ML models	Full	Partnerships	6/21/2023	Tests performed with a limited number of registered UEs and limited time for generating collecting data.	Technical development, product development, strategy	Start	Build on open framework with mobile operators for sharing if possible network data. Also current projects require more testing time for data generation and collection	Discuss/work closely with MNOs and extend testing periods if possible	UoB,SAC

ORANOS Final project review
July 2023