TELECOM INFRA PROJECT

OpenRAN ROMA CD/CT OpenRAN Automation White-Paper

Version: V1.0

January 18, 2023

Authors

- Robin George – Director Mobile Network Services, Amdocs
- Shoujit Mitra- Solution Architect, Mobile Network Services, Amdocs
- Atul Khanna - Sales Director, Mobile Network Services, Amdocs

Contributors

- Takai Eddine Kennouche, VIAVI Solutions
- Alexey Rusakov, Red Hat
- Raul Barranquero Simon - Telefonica
- Rajesh Rasalkar - ROMA Technical co-leads, Meta
- Siddharth Mankikar - ROMA TPM, Meta
- Xinli Hou - ROMA Technical co-leads, Meta
- Ramon Guevara - Vodafone
- Beatriz Gonzalez Rodriguez - Telefonica
- Jorge Ilopis – Vodafone
- Jorge Fernandez Cortes – Telefonica
- Guillermo Carreto Lopez - Telefonica
- Zheng Cai – T-Mobile
- Veronica De Alba - Vodafone

TIP Document License

By using and/or copying this document, or the TIP document from which this statement is linked, you (the licensee) agree that you have read, understood, and will comply with the following terms and conditions:

Permission to copy, display and distribute the contents of this document, or the TIP document from which this statement is linked, in any medium for any purpose and without fee or royalty is hereby granted under the copyrights of TIP and its Contributors, provided that you include the following on ALL copies of the document, or portions thereof, that you use:

1. A link or URL to the original TIP document.

2. The pre-existing copyright notice of the original author, or if it doesn't exist, a notice (hypertext is preferred, but a textual representation is permitted) of the form: "Copyright © 2021, TIP and its Contributors. All rights Reserved"

3. When space permits, inclusion of the full text of this License should be provided. We request that authorship attribution be provided in any software, documents, or other items or products that you create pursuant to the implementation of the contents of this document, or any portion thereof.

No right to create modifications or derivatives of TIP documents is granted pursuant to this License. except as follows: To facilitate implementation of software or specifications that may be the subject of this document, anyone may prepare and distribute derivative works and portions of this document in such implementations, in supporting materials accompanying the implementations, PROVIDED that all such materials include the copyright notice above and this License. HOWEVER, the publication of derivative works of this document for any other purpose is expressly prohibited.

For the avoidance of doubt, Software and Specifications, as those terms are defined in TIP's Organizational Documents (which may be accessed at https://telecominfraproject.com/organizational-documents/), and components thereof incorporated into the Document are licensed in accordance with the applicable Organizational Document(s).

Disclaimers

THIS DOCUMENT IS PROVIDED "AS IS," AND TIP MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR TITLE; THAT THE CONTENTS OF THE DOCUMENT ARE SUITABLE FOR ANY PURPOSE; NOR THAT THE IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

TIP WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE DOCUMENT OR THE PERFORMANCE OR IMPLEMENTATION OF THE CONTENTS THEREOF.

The name or trademarks of TIP may NOT be used in advertising or publicity pertaining to this document or its contents without specific, written prior permission. Title to copyright in this document will at all times remain with TIP and its Contributors.
This TIP Document License is based, with permission from the W3C, on the W3C Document License which may be found at https://www.w3.org/Consortium/Legal/2015/doc-license.html.

Exhibit A

TIP CONFIDENTIAL

This document contains TIP Confidential Information as defined in Section 1.3 of the TIP Bylaws. Subject to Sections 16.1 and 16.2 of the TIP Bylaws, use and disclosure of the document and its contents are strictly prohibited. Copyright © 20__ Telecom Infra Project, Inc. All rights reserved. The Telecom Infra Project logo is a trademark of Telecom Infra Project, Inc. (the "Project") in the United States or other countries and is registered in one or more countries. Removal of any of the notices or disclaimers contained in this document is strictly prohibited. The publication of this document is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS," AND WITHOUT ANY WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. UNDER NO CIRCUMSTANCES WILL THE PROJECT BE LIABLE TO ANY PARTY UNDER ANY CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER LEGAL OR EQUITABLE THEORY, FOR ANY INCIDENTAL INDIRECT, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR FOR ANY COMMERCIAL OR ECONOMIC LOSSES, WITHOUT LIMITATION, INCLUDING AS A RESULT OF PRODUCT LIABILITY CLAIMS, LOST PROFITS, SAVINGS OR REVENUES OF ANY KIND IN CONNECTION WITH THE SUBJECT MATTER OR USE OF THIS DOCUMENT.

Change Tracking

Date	Revision	Author(s)	Comment
11/15/2022	Template	Rajesh Rasalkar Xinli Hou	Develop Template
12/15/2022	1st Draft	Robin George Shoujit Mitra Atul Khanna	1st Draft
12/23/2022	2nd Draft	Robin George Shoujit Mitra Takai Eddine Kennouche Alexey Rusakov Rajesh Rasalkar	Updates based on internal review
01/04/2023	3rd Draft	Xinli Hou	Minor editorial updates of contributors and affiliations + formatting changes
01/26/2023	V1.0	Rajesh Rasalkar	Updates based on ROMA community review comments Formatting based on TIP branding

Glossary

3GPP	3rd Generation Partnership Project
CI/CD	Continuous integration, continuous deployment
CD/CT	Continuous deployment, continuous testing
CD/D	Continuous delivery, continuous deployment
CNF	Containerized network function, or cloud-native network function
E2E	End-to-end
EMS	Element management system
ETSI	European Telecommunications Standards Institute
FCAPS	Fault, configuration, accounting, performance, security
NMS	Network management system
NGMN	Next Generation Mobile Networks
RAN	Radio access network
SMO	Service Management and Orchestration
SOL005+	Extension of ETSI-NFV-SOL005 API definition
vCU	virtualized central unit
vDU	virtualized distributed unit
VM	virtual machine
VNF	virtualized network function

Table of Contents

1. Introduction

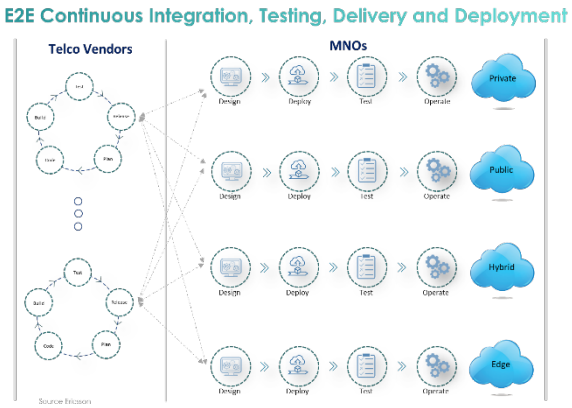
This white paper aims at outlining the challenges, industry best practices and standards in integrating the CD/CT platform for Open Radio Access Networks (Open RAN). The paper follows on from our previous paper titled "TIP OpenRAN White Paper Toward OpenRAN CICD Automation October 2020" Therefore, readers of this white paper are encouraged to read the previous one as an introduction, thus also familiarizing themselves with the concepts of virtual RAN, Open RAN and Continuous Deployment. Open RAN architecture continue to enable principles of intelligence, virtualization, and disaggregation.

One of the biggest challenges often raised in the industry is of complexity of Open RAN automation. This challenge comes as no surprise as Open RAN represents one out of many examples where systems get disaggregated into smaller pieces. Such dis-aggregation inevitably calls for the corresponding aggregation – i.e., the integration. Open RAN is (in many of the cases) a multi-vendor exercise where vendors of various parts of the RAN as well as infrastructure vendors need to come together and make sure their products are interoperable in the configurations requested by the market.

2. Executive Summary

Continuous testing and deployment (CD/CT) has been a proven model in IT services domain but yet to be embraced entirely in Telecom domain.

A continuous integration, testing, delivery and deployment framework unlocks many benefits for communication service providers. The key being the delivery of the latest and greatest software in a "continuous" fashion. This enables the service and business agility – reducing time to market for new features, allowing security vulnerabilities addressed in time, and reducing OPEX with the automated delivery of software.



With cloud-native, Open RAN, and 5G adoption, value creation will require increasing software change accompanied by the complexity to achieve shorter time to market. As a result, there is an obvious tipping point where traditional ways of software adoption (activate, upgrade, update, rollout) and testing will fail to scale. As Open RAN and 5G core services are rolled out, service providers will face an order of magnitude increase in the demand for software configuration testing and validation. While this volume of testing will take some time to reach its new sustained level of intensity, there is no doubt that automation is essential.

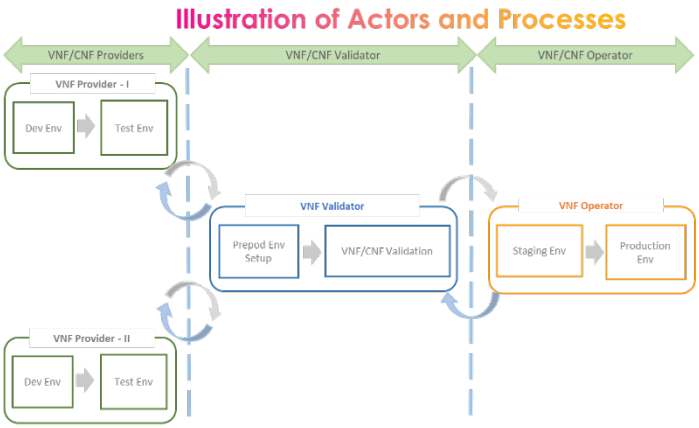
Inherently, there has been a gap between DevOps CI/CD and operator CD/CT. This gap between CI automation in one network zone and deployment automation in other network zones hinders seamless CD automation. Current focus of the whitepaper is CD/CT.

Service Management and Orchestration (SMO) developed by O-RAN plays a vital role in provisioning and lifecycle management of Open RAN service. RAN service (vDU, vCU, xApp, rAPP, other applications) instantiation to upgrade, to reconfiguration, is accomplished through SMO. Therefore, a standardized interface between CD/CT and SMO is essential to achieve end-to-end CD/CT workflow automation.

3. Standards and Specifications Landscape

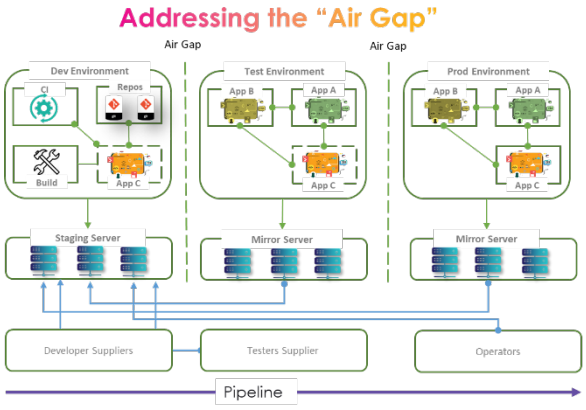
Specifications and Standards development organizations (SDO) such as ETSI, 3GPP, TMF, O-RAN and open forums such as NGMN have published guidelines, reports, and whitepapers for CI/CD, CD/CT, and CD/D. These publications are not limited to Open RAN but also extend to all domains such as Core, Transport and MEC. All the documents mentioned further put the primary emphasis on applying continuous integration, testing, delivery and deployment from a provider domain to the operator domain.

ETSI GR NFV-TST 006 V1.1.1 [I] document provides guidance and recommendations on how to leverage DevOps and CI/CD techniques across the boundary from a SW provider to the service provider, or any combination of developer, installation, and operational entities. It explores the implications of the processes about the impact of the SW package hand-off between a SW provider and the service provider, the required functionality in the NFV system, the different deployment, and operational options. Current guidelines are for VNF but can be extended for CNF.



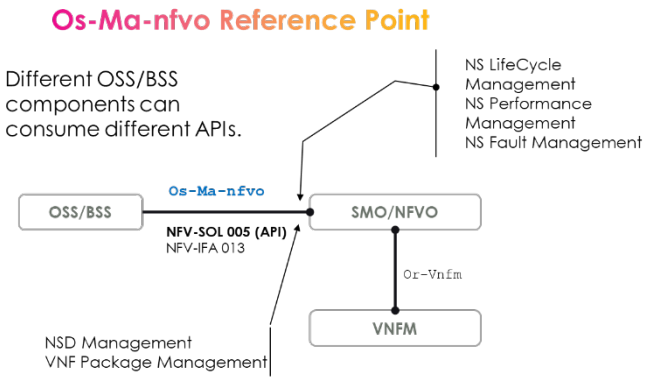
Similarly, 3GPP TR 28.819 V18.0.0 [II] document studies key issues in automating CI/CD based testing of 3GPP NFs after delivery to the operator's operational environment. This document describes the support of the 3GPP system for CI/CD and other testing such as: 1) support for operational and simulation testing 2) information relating to NFs required for testing 3) feedback on the new NF's performance.

Besides ETSI and 3GPP guidelines, the NGMN Alliance Whitepaper on Continuous Delivery in Telecommunication Network Environments [III] also highlights the need to bridge the "air gap" between automated builds executed in vendor CI environments and automated deployments executed in test and production environments. The paper highlights five main aspects that are to be considered for standardization:



1) **Release model** is the complete set of items required for instantiating a software-based function. In terms of 3GPP NF this would be the information and the supporting artifacts required to instantiate the 3GPP NF

2) **Environment model** describes the environment to which releases could be deployed. This refers to the available software and hardware artifacts in that environment. Release models may be specific to environment models.
3) Use of **version control** in the operator environment
4) **Automated deployment steps** that include testing the software artifacts delivered from across vendors in a staging environment, and
5) **Clear separation** of development, testing and operations environment for security reasons.



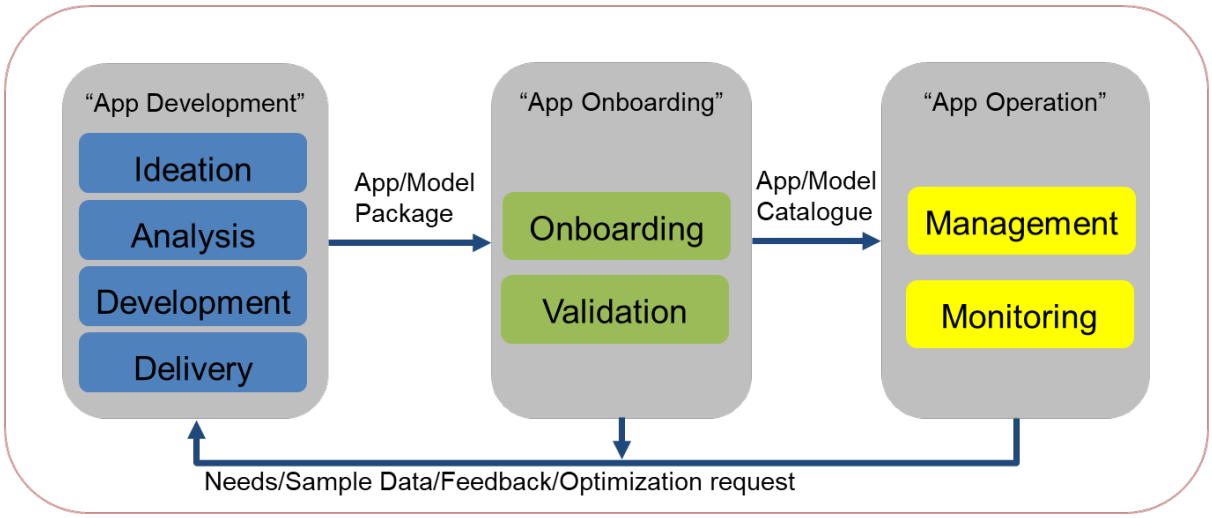
ETSI GS NFV-SOL005 [IV] document specifies a set of RESTful protocol specifications and data models fulfilling the requirements for the interfaces between OSS/BSS and SMO/NFVO (Os-Ma-nfvo reference point). The SOL005 API definition has been designed for NFV and needs to be extended for cloud-native telecommunications infrastructure.
SOL005 API coverage is extensive and covers all aspects of

1) NSD management Interface
2) NS Lifecycle management Interface
3) NS PM Interface
4) NS FM Interface
5) VNF Pkg management Interface
6) NFVI Capacity Information Interface,
7) VNF Snapshot Pkg management Interface, and
8) NS LCM Coordination Interface.

However, from CD/CT perspective, the APIs primarily required are for Network Service (NS) Lifecycle Management purpose, and NSD management and package management.

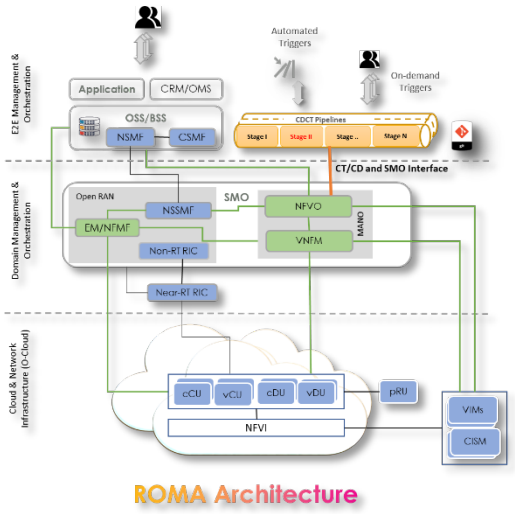
SOL005 API definition has a critical role for CD/CT workflow integration with SMO. Nevertheless, extension of SOL005 API may be required to support coexistence of OSS/BSS and CD/CT interface with SMO/NFVO and alignment with CD/CT architecture & design principle expectations.

The O-RAN OAM Group defines the architecture and principles of the Lifecycle Management of applications that are developed by a Solution Provider and delivered to a Service Provider or Network Operator for deployment in O-RAN. It standardizes the unified approach for developing, onboarding and operation of RAN NF's, rApps and xApps. This O-RAN standard pay a significant role in RAN CD/CT automation. The working flow could be summarized as three phases: Development, Onboarding and Operations (see below picture). The LCM of the NF's or App's package may use the ETSI NFV-SOL005 API described above.



4. CD/CT deployment options under considerations

TIP ROMA focus area is OpenRAN orchestration and life-cycle management automation features and functions as well as multi-vendor interworking. ROMA architecture takes the ETSI NFV model as a starting point and takes it further to support both VNF and CNF orchestration. The picture highlights one possible context of the CD/CT platform with respect to SMO where it can be considered as a part of or adjacent to OSS. Alternatively, the CD/CT can be considered as a service provided at the infrastructure level, with the CD/CT platform taking place as a part of, or adjacent to, VIM/CISM.
In addition to the CD/CT platform requirements, architecture, and core capabilities, the ROMA CD/CT working group's focus area is on exploring options for the interface between SMO and CD/CT pipeline that does not see much standardization work so far.



ROMA Architecture

The table summarizes the ROMA CD/CT scope with respect to design principles, architecture, and few other important attributes.

Scope	Requirement	Description
Technology	OpenRAN service	Deployment, upgrade, configuration, and lifecycle management of OpenRAN components.
	SMO agnostic	The CD/CT platform should be able to integrate with multiple vendor SMOs
	Cloud platforms support	Support for both open source and vendor specific infrastructure layers such as containerization offerings (such as Kubernetes) and virtualization offerings (OpenStack, VMWare vCenter).
Design Principles	GitOps design principles	The CD/CT platform based on GitOps principles and concepts. Git is used as the single source of truth for all changes on the network; artifacts, configuration, deployment charts, NS definitions, etc. are updated in Git, from where changes are propagated to the network.
	Well-defined API	Well-defined APIs between the CD/CT platform and SMO.
Architecture	CDCT platform decoupled from SMO	The CD/CT platform is unbound from the SMO platform; the two integrate through REST API

	Centralized repository	Common internally consistent repository for artifacts, configuration, resources, etc.
	Cloud-agnostic	Private, public, hybrid, edge, centralized, and access cloud
	Open Source use	Maximize use of Open Source tools in development of the CD/CT platform
	Upstream feedback and notification	Continuous feedback to northbound systems, status updates, notifications, KPIs, etc.
Monitoring	CD/CT Dashboard	Monitoring of CD/CT workflow progress, status, and faults
Data Collection	Centralized logs, reports, and data	Observability and traceability
Resilience	Graceful rollback	In case of an upgrade failure, graceful rollback of the changes without affecting the service
	Reconfiguration	Ability to revert to the previous configuration
Automated Validation	Pre-production testing	Functional, system, interoperability, soak, etc.
	Production testing	E2E, interoperability, etc.
	External Test Tools	Integration with external test tools, simulators
Platform Security	CD/CT platform access control	Ability to allow certain changes to only be carried out on behalf of specific users
	API security	Security principles for APIs between CD/CT and SMO, IT Services and CD/CT Platform
	Repository access	Token-based secure access to Git, Nexus and any other repository
Policy	Policy-driven deployment, configuration, rollback, reconfiguration	Deployment, upgrade, configuration and activation of an OpenRAN service based on policy
	Policy-based testing	Configurable and selective testing depending on the CD/CT phase, deployment scenario, and any specific requirement

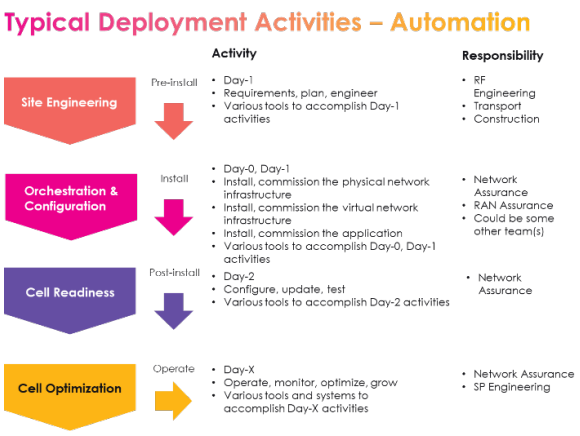
5. Current state of CD/CT

In today's 5G deployments, network functions are predominantly CNF as opposed to VNF. Originally NFVOs were designed to support VNFs and have been enhanced to support CNF orchestration. Cloud platforms and technologies such as Kubernetes, Nephio, etc. have a deeper impact on SMO capabilities, architecture, and control. They not only complement SMO capabilities but also take over some of the functionality. For reference, a brief comparison between the orchestration models proposed by ETSI and by Nephio is presented in appendices.

The ROMA architecture is based on the ETSI model, therefore the CD/CT discussion in this whitepaper assumes SMOs that follow the ETSI model. This approach is aligned with orchestration architecture developed by O-RAN specifically with the option that leverages the ETSI NFV model by defining the ETSI NFV profile for NF's deployments orchestration.

Conventionally, the workflow to instantiate, configure, update, upgrade and reconfigure a network service is through OSS/BSS and network service upgrades are done less frequently. However, in the ever-changing 5G world continuous upgrade/update of network services is expected. Moreover, the network infrastructure itself is increasingly software-defined and multi-vendor. This dictates the need for a secure, reliable, resilient, and flexible CD/CT platform that can support pipelines involving multiple vendors and all layers at different stages, from physical to software infrastructure and further to network functions.

Implementation of CD/CT platform for auto instantiation, and lifecycle management of network services in production network is a complicated process. Conventionally, instantiation of network service (ex. vDU, vCU instantiation) is a multi-step activity and spread across multiple teams, involving a combination of manual and automated steps. Similarly, lifecycle management of deployed service is complex and poses several challenges. Therefore, the requirement and expectations from a secure, reliable, flexible, and resilient CD/CT platform is enormous.



Keeping in view of the challenges mentioned above, limited form of CD/CT automation is currently deployed in production environments of MNOs. However, there is a clarity on requirements and expectations of a carrier grade CD/CT platform.

The CD/CT platform for OpenRAN deployment and beyond needs to be vendor-neutral, service-agnostic, customizable, and policy-driven. The CD/CT Platform requirements could primarily be divided into seven pillars – Security, Workflow Engine, Infrastructure Management, Test Framework, Policy, and Data Collection. The platform expectations are not limited to the following but depend on use cases.

Security

- Highly secured platform, from user access to API access
- Administrative and user level access control

Workflow Engine

- Pre-integrated & tested workflows for wide range of use cases
- Configurable, programmable, and extendable as per use case
- Catalogue of workflow triggers. Flexibility to extended available triggers and notifications as per use case
- Secured APIs for easy integration with external application

Artifacts Pre-check

- Validation of vendor artifact definition and compliance testing.
- Security and authenticity validation of vendor artifacts
- Integrity check of vendor artifacts, and dependencies

Infrastructure Management

- Capability to build complex test environment on-demand
- Orchestration, instantiation, and configuration of vendor VNF/CNF/PNF directly or through SMO, on private or public cloud
- Inclusion of external test tools, applications, and services in the test environment
- Ability to save test environment for analysis & debugging
- Job Scheduler for continuous testing
- Secured APIs for integration with external applications

Integrated Test Framework

- Model-driven, and adaptive OpenRAN, 5G, etc. testing platform
- Secured APIs for 3rd party integration.
- Simplified integration with vendor, customer, and test equipment vendor test cases/suites.
- Plugins for multiple test equipment vendors.
- Data collection and analytics for fault isolation and root cause analysis
- Robust protocol plugin support – Python, ROBOT, REST, NETCONF, CLI, Ansible, and custom plugins for a wide range of network resources

Staging, Data Collection and Analytics

- Staging of verified and certified artifacts & configuration for delivery & deployment
- Consolidation of correlated logs and data collection at each stage of the workflow
- Analysis of aggregated data, configuration, and topology
- Simplified and intuitive visualization of logs for analysis and debugging

Policy-driven Platform

- Policy-based software upgrades, updates, and rollouts
- Easy and intuitive steps to manage and configure policy
- Programmable and extendable
- Policy-based decision at micro and macro level at each stage of the workflow

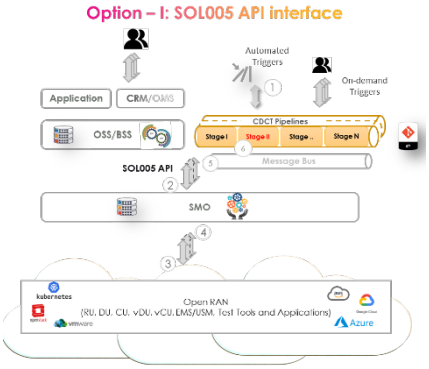
For illustration a sample CD/CT workflow is presented in Typical CD/CT Workflow.

6. Integration architecture options

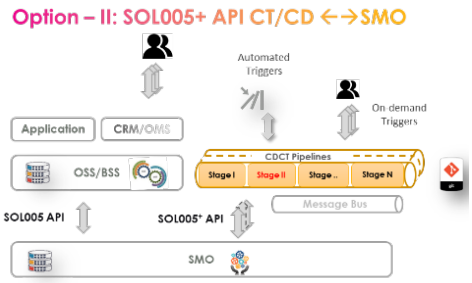
Coordination of CD/CT platform with other applications such as OSS/BSS, Service Assurance, Monitoring, etc. in the production environment poses its own challenge. As mentioned above, CD/CT platform can be introduced in either of two ways into the operator's architecture: either to the north from SMO, adjacent to OSS/BSS; or as a part of an "infrastructure platform" – adjacent to, or included into VIM/CISM. Without trying to pick a superior option we present both below, along with possible approaches to integration and the questions concerned. A more detailed analysis of strong and weak points for each way is out of scope of this whitepaper.

Let's first look at the case where CD/CT is connected to SMO's northbound interface. There are more than one deployment options for CD/CT platform and its integration with SMO, OSS/BSS, and other connected applications & services; we see SOL005 being the most popular API standard used in the industry for the discussed purpose. Use of TM Forum's OpenAPIs is also an option for CD/CT and SMO integration in this case. Either way, differences in the architecture and LCM between cloud-native and virtualized workloads are leveled out in SMO. It's worth pointing out that GitOps design principles are not necessarily satisfied by this architecture, as it pre-dates GitOps usage in the industry and does not assume a version-controlled repository as a source of truth. The existing practice shows however that this is a viable option at least for the transitional period when different network functions follow different paradigms (VNF vs. CNF).

Let's assume SOL005 as the API for now. One challenge this model possesses is the data synchronization between OSS and SMO, when a network service instance is created by OSS but later updated by CD/CT workflow. By GitOps design principles CD/CT workflow doesn't use any persistent storage (inventory) of its own for configuration data management. CD/CT platform relies on Git repository updates produced by OSS/BSS - however, SMO must apply changes to the network that arise both from OSS/BSS requests, as well as artifacts from CD/CT flows, and these must be synchronized somehow.



It is possible to mitigate this data inconsistency issue by extending the SOL005 API while maintaining the same deployment option. SOL005+ implies customized API to accommodate CD/CT requirements. SOL005+ suggests inclusion of Git repository reference in the API request. Sample SOL005+ API definition is presented in appendices.

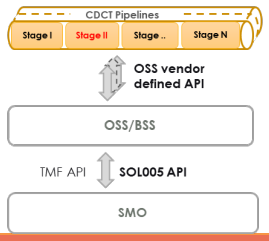


Differentiators	SOL005 API	SOL005+ API
Industry acceptability	ETSI standard supported by commercial SMO/NFVO SOL005 APIs is already being updated to accommodate CNF	May not be embraced by all SMO vendors. One of the objectives of ROMA CDCT working group is to define the appropriate API interface.

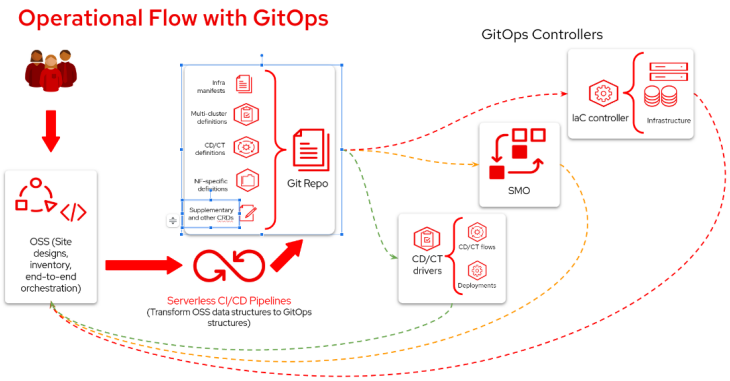
Industry acceptability	ETSI standard supported by commercial SMO/NFVO SOL005 APIs is already being updated to accommodate CNF	May not be embraced by all SMO vendors. One of the objectives of ROMA CDCT working group is to define the appropriate API interface.
Scope	Primarily defined for OSS/BSS and NFVO	Extension of SOL005 API and simplified interface required for CDCT and SMO
Deployment	Centralized OSS to SMO/NFVO	Multiple CDCT pipelines to SMO
Design Principle	API request includes all data	Pull data from Git repository. Based on GitOps design principles
Data Synchronization	OSS database/inventory is in sync with SMO active inventory	Change in architecture and interface(s) required to address the data consistency issue across OSS/BSS, SMO, and CDCT (Git repository)

The third deployment option is the CD/CT interface to SMO through OSS/BSS stack. This deployment option resolves the data inconsistency issue mentioned above. However, there are pros and cons of the deployment model of its own. In this case the CD/CT interface with OSS/BSS cannot be 'standardized' for obvious reasons.

Option – III: CT/CD ←→ OSS/BSS←→SMO



Criteria	Pros	Cons
Standard Compliance	OSS/BSS stack provides APIs for external app integration	OSS northbound interface is not based on standard Every OSS vendor has their custom northbound interface
Data Consistency	OSS/BSS and SMO data synchronized by flow of events.	No issues
Performance & Scalability	OSS/BSS application is a core platform in an MNO environment and is capable of processing large number of requests OSS processes request	The model will enforce excessive burden on OSS/BSS workflow. Large number of continuous updates expected through CDCT platform. OSS could be the bottleneck



Now let's consider the architecture with a common CI/CD/CT platform being a part of the infrastructure. This architecture would allow to cover all parts with a unified CI/CD/CT framework, including the infrastructure itself, the SMO, and network functions. The picture above describes how the network configuration travels trough the stack. In this case the CI/CD/CT platform is used both to translate changes to a model that could be stored in Git and then to enact the changes with SMO as an integral part of the process ; but OSS/BSS can make changes in Git directly, and trigger CD/CT accordingly. This is very well aligned with the architecture proposed by Nephio. It also aligns with the ETSI model but assumes a somewhat different role for the API between OSS/BSS and SMO/CD/CT: assuming that the proposed changes to SOL005 are accepted, instead of passing the network configuration in-band, the SOL005+ API would use Git references to refer to the configuration to be enacted - similar to one of the cases described above. The downside of this option is that this architecture is not something currently assumed in the industry, and it is not backwards compatible with existing stacks, again in the same vein as the case above.

7. Summary

Traditionally, RAN & Core network & service upgrades were done quarterly, but in the ever-changing Open RAN & 5G world it is going to be at a much higher cadence. However, there is an apprehension in Telecom Operators to move forward with fully automated CD/CT platform. The need for a CD/CT platform that bridges the gap between vendor agile processes to reduce time to market for new updates, products and features, and operator's integration process for each environment or platform, with design, deploy, test, and operate phases is imperative.

Based on the above discussion, the immediate recommendation is to move forward with ETSI-model based SMO. Nephio with community support will evolve over a period of time and the recommended approach will need to be re-evaluated based on maturity.

With respect to CD/CT integration with SMO, there are broadly three different deployment options. Pros and cons of each of the options are briefly discussed above. Initial study suggests, use of standard ETSI-NFV-SOL005 is an option. Further detailed analysis will be needed.

Extension to SOL005 API will also have a potential, as it attempts to address some of the issues and aligns with CD/CT GitOps principles. Additional details of the SOL005+ API definition, data/event flow between components (CD/CT, OSS, SMO, Service Assurance, Monitoring, etc.) are subject of ongoing study.

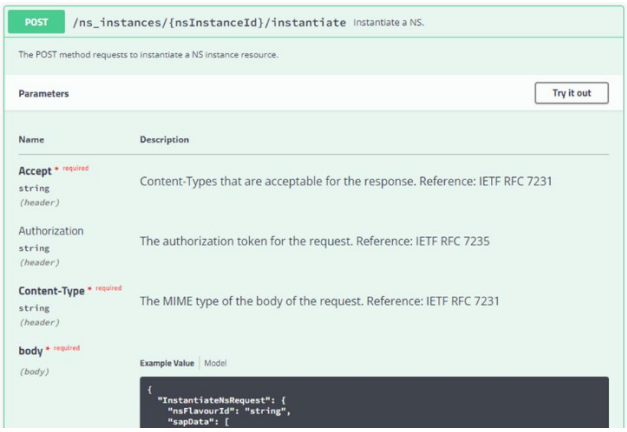
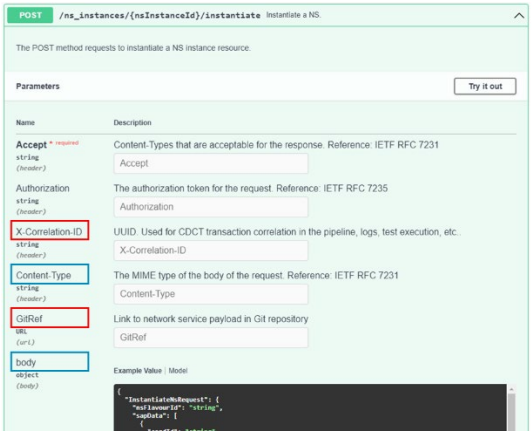
8. References

I. ETSI GR NFV-TST 006 V1.1.1 (2020-01) Network Functions Virtualization (NFV); Testing; Report on CICD and DevOps
II. 3GPP TR 28.819 V18.0.0 (2022-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Management and orchestration; Study on continuous integration continuous delivery support for 3GPP NFs (Release 18)
III. Continuous Delivery in Telecommunication Network Environments by NGMN Alliance
IV. ETSI GS NFV-SOL 005 V4.3.1 (2022-08): Network Functions Virtualization (NFV) Release 4; Protocols and Data Models; RESTful protocols specification for the Os-Ma-nfvo Reference Point.
V. O-RAN.WG1.O-RAN-Architecture-Description-v08.00 (2022-11): O-RAN Architecture Description
VI. O-RAN.WG10.OAM-Architecture-v07.00 (2022-10): O-RAN Operations and Maintenance Architecture

9. Appendices

Comparison between SOL005 and SOL005+ API

Sample comparison of the API request is presented in this section. The SOL005+ API change is only for illustration.

SOL005 InstantiateNsRequest API	SOL005+ InstantiateNsRequest API
	

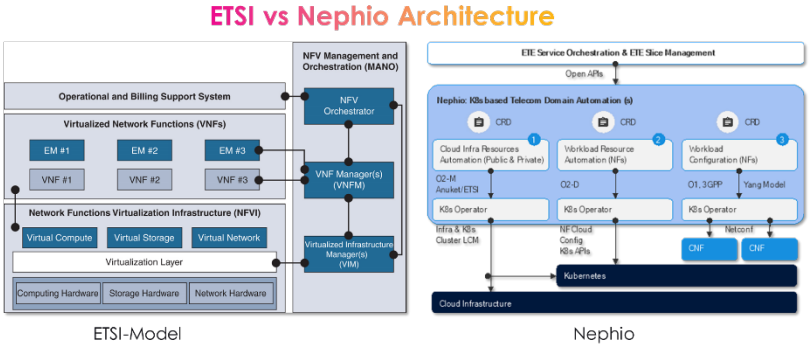
Suggested SOL005+ sample API, two optional parameters correlation-id and Git repository reference) included. Updated content-type and body of the message to be optional. The SOL005+ API definition needs to be backward compatible.

Use case: If the InstantiateNsRequest API is invoked from a CD/CT workflow, it is expected that the payload (API data/body) is passed as Git repository reference. Correlation-id is a global parameter in CD/CT workflow used for correlating all activities within a pipeline.

High-level comparison between ETSI and Nephio

ETSI-NFVO model was primarily developed for VNF, therefore evolution of VNF to CNF, have led to enhancements to ETSI based SMOs. Furthermore, Cloud native network functions, Kubernetes, intent-based networking have led to the new initiative, Nephio.

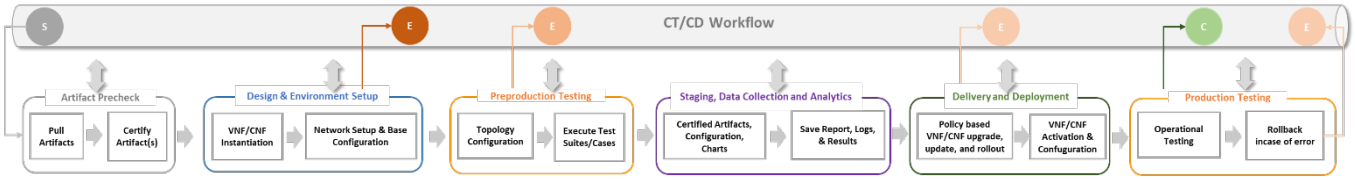
Nephio offers carrier-grade, simple, open, Kubernetes-based cloud native intent automation and common automation templates that



materially simplify the deployment and management of multi-vendor cloud infrastructure and network functions across large scale edge deployments. As can be seen from the Nephio architecture picture it will be aligned with O-RAN O2 interface.

Requirement	ETSI-Model	Nephio
Maturity	Has been in existence for over 10yrs. Almost all NFV-O are aligned with ETSI.	Google Cloud founded the Nephio project in April 2022, with major vendors and CSPs joining the initiative
Scope	Management and orchestration across infrastructure, NFs to Network Services	Cloud-native NF infrastructure and domain orchestration; end-to-end orchestration is out of scope
CNF/VNF LCM	NFV-O/SMO	Nephio controller manages LCM of CNF. SMO integrates with Nephio controller to manage end-to-end service lifecycle
Type of Network Function	VNF, CNF, PNF	CNF
API	Explicit APIs for service design, network function LCM, and service LCM	Minimum API requirements as CRs are automatically pulled from Repository
CNF (workload configuration)	NFV-O/SMO->VNFM->EMS->CNF	CNF configuration through CRD(s)
Provisioning of Complex Services	SMO	SMO
Complex Services (Network Slice, etc.) LCM	SMO	SMO
Service Assurance	Guaranteed by SMO	Managed by Nephio Controller
Rollback	NFV-O/SMO->VNFM->EMS->CNF	Managed by Nephio controller
Alignment with ROMA architecture	Aligned	Drifting away from ETSI Model. Limited control of SMO over CNF LCM
Platform security	API based	API based
Vendor dependency	Managed by VNFM and EM	K8s Operator maturity per vendor

Typical CD/CT Workflow



At a high level the CD/CT workflow is partitioned into six stages, and it is tied to a set of predefined triggers. It is undeniable fact that there is no one-size-fits-all CD/CT solution, therefore customization is inevitable. However, the fundamental components needed for CD/CT are likely to be the same, and there is an opportunity to reuse and further advance the work that is done in the open source community in order to reduce the amount of custom code. That being said, significant integration effort is expected to successfully deploy a CD/CT or CD/D platform at any site.

Stage-I is the preliminary stage of the pipeline. Artifact definitions are pulled from repository(s), that have vendor access too. New artifacts are pushed to repository by vendor(s), triggering the workflow engine. Artifact integrity, security, and deployability prechecks are done. Policy based decisions are taken to catalogue artifacts for further processing. In Policy, user can define policies, rules and criteria encompassing the artifact promotion to next stage.

Stage-II defines the steps to design and dynamically build the preproduction test environment. VNF/CNF, and cloud-native applications, instantiation in target cloud, and reservation of PNF and Test Tools, are part this stage. Depending on the target environment, VNF/CNF/Application instantiation can be done through SMO. Infrastructure management involves not only update and upgrade of network resources but also rollout of new network resources in the network.

Lab & Preproduction Testing of the new updates to the network, services, and applications is a critical activity. Requirement specific test environment created in Stage-II is the foundation for comprehensive testing in **Stage-III**. From system testing to network resource functional testing to interoperability testing to E2E network & services testing to performance testing to every silo of testing is covered by integrated test platform.

The test framework needs to be pre-integrated with test equipment for protocol, security, performance, compliance, and interoperability conformance testing.
The test platform needs to be complemented by analytics engine for debugging, and fault isolation. Hybrid networks consisting of PNF, VNF, CNF, and applications is highly complex. The ability to test individual segments in a controlled, coherent manner is required for the rapid, automated isolation of functional to performance degradation across the end-to-end digital network.

Tested, promoted, and certified artifacts, configuration files, helm charts, templates, and other network resources are stored in deployment catalog in **Stage-IV**. Logs from all the stages, correlated test execution logs, and consolidate data are pushed to persistence storage and analytics platform for easy access, indexing, visualization, and data manipulation.

Delivery and deployment of VNF/CNF/Apps/Controller/etc. upgrades, updates and rollouts are controlled by policies, and rules defined by Policy. Control is at a micro and macro level. **At stage-V**, network upgrade is done through SMO platform.

Finally, at **stage-VI** selective production testing is critical to verify the changes and operationalize the updated network & services. The Test Platform is expected to execute test cases/suites specifically designed for production network validation. Test failure automatically triggers, rollback sequence.