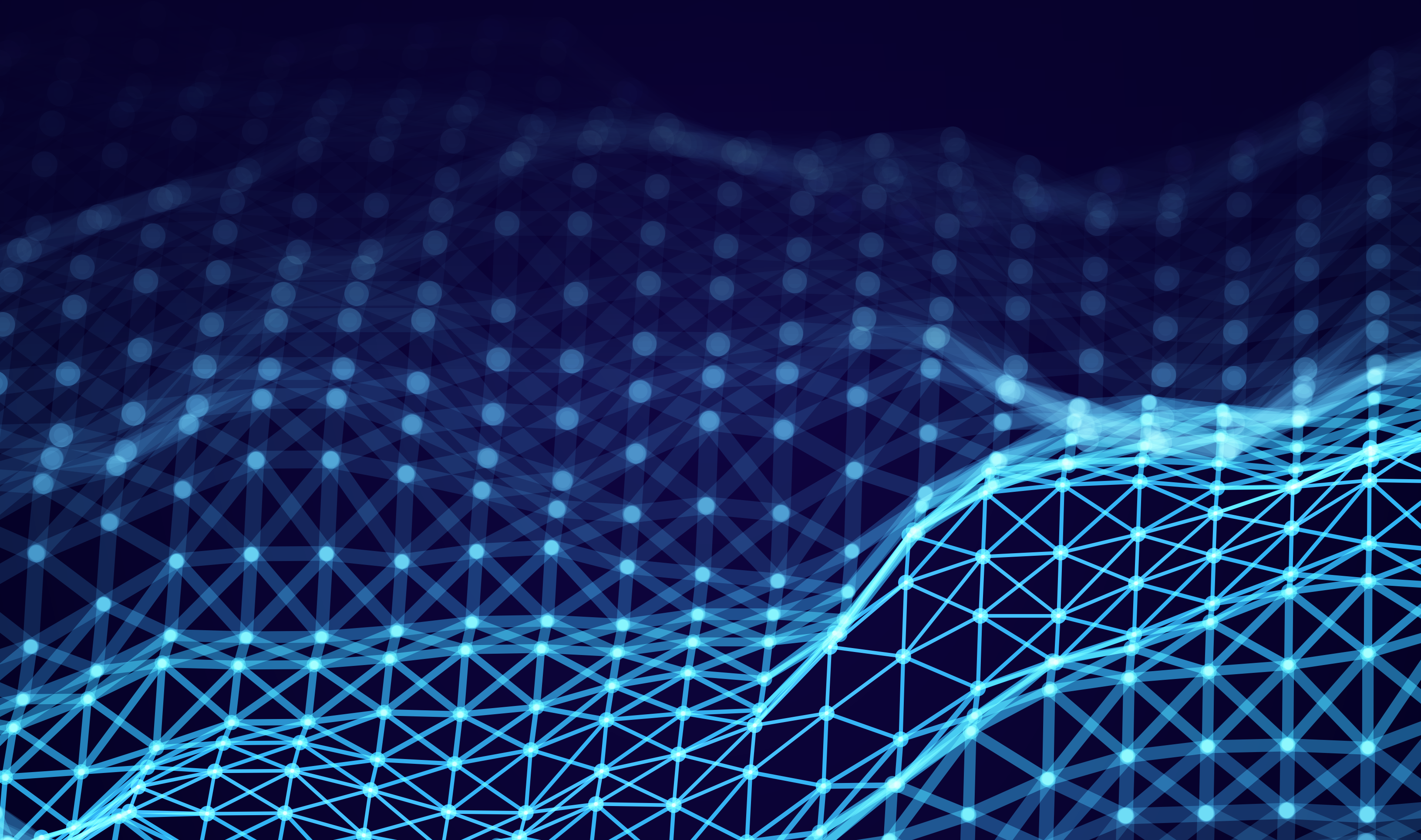
LF NETWORKING THE LINUX FOUNDATION ONAP NEXT GENERATION NETWORK AUTOMATION

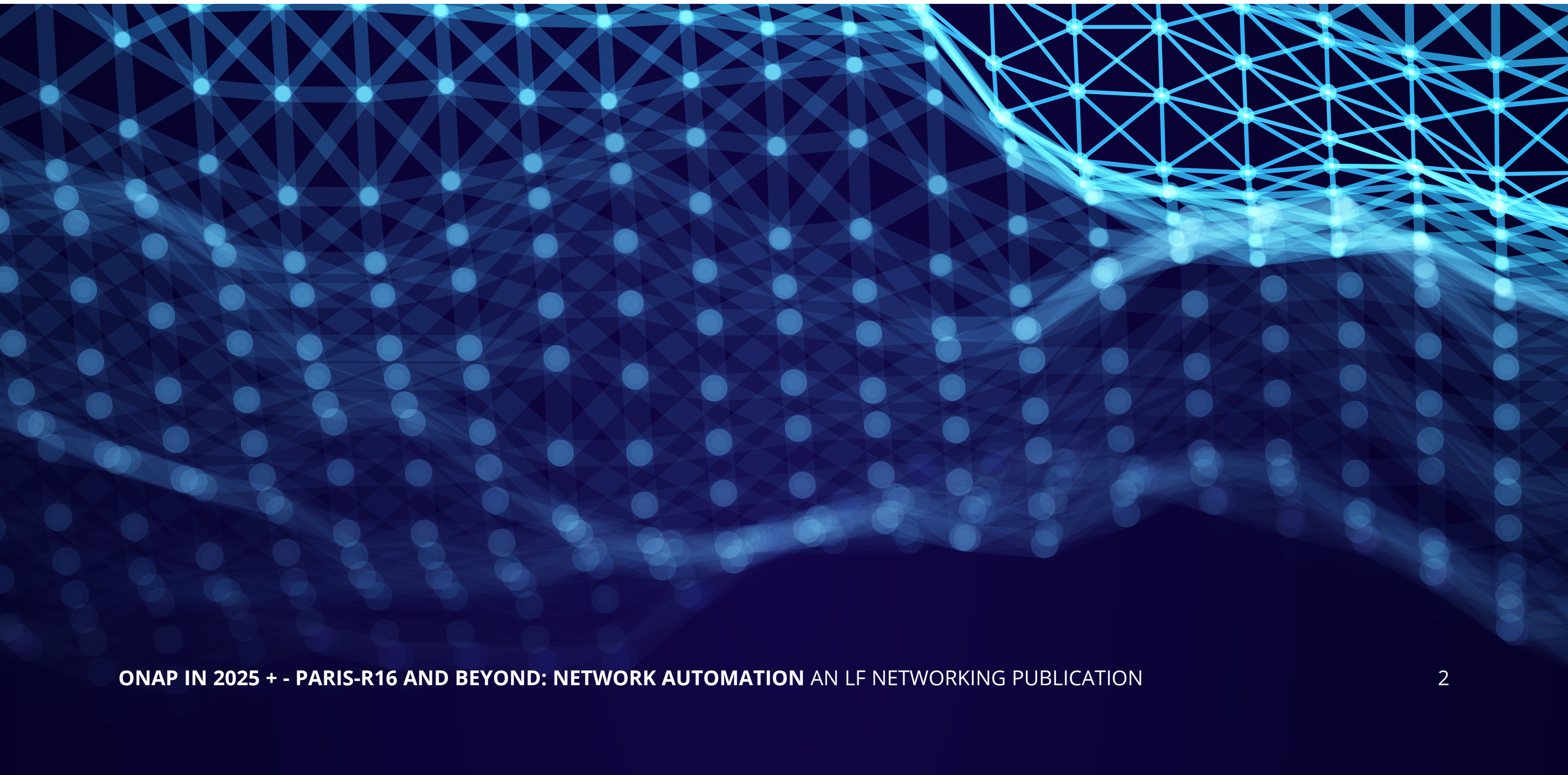
ONAP in 2025 + - Paris-R16 and Beyond: Network Automation

A Linux Foundation Networking publication



Executive Summary

ONAP has transformed from a monolithic orchestration platform into a modular, semi-standalone ecosystem for intelligent network automation. With the Paris-R16 release and the forward-looking ONAP in 2025 vision, ONAP is positioned to deliver declarative, intent-based orchestration, integrate advanced GenAI and ML capabilities, and maintain strong alignment with global telecom standards. Its modular components are now exposed as LFN functions, enabling seamless integration with other open-source communities. This expanded whitepaper consolidates technical, architectural, operational, and strategic insights from both the [ONAP in 2025 roadmap] and the Paris Release Architecture documentation, providing comprehensive guidance for architects, operators, and ecosystem partners.



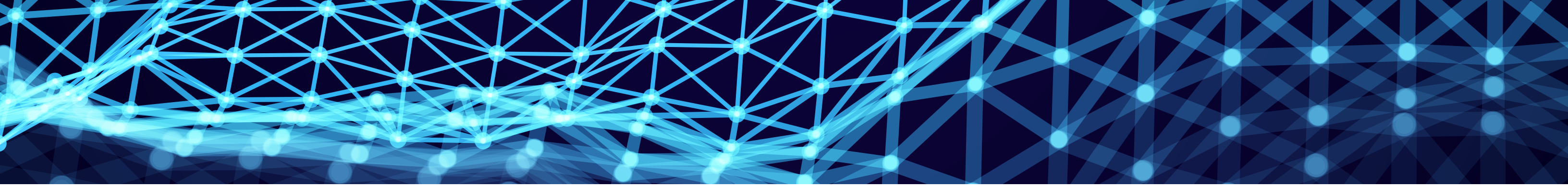


Table of Contents

Authors

Byung-Woo Jun - Ericsson, ONAP TSC Chair

Contributors

Keguang He - CMCC

Fiete Ostkamp - DT

Marek Szwalkiewicz - DT

Toine Siebelink - Ericsson

Ramesh Murugan Lyer - Ericsson

N.K. Shankar - Individual

Dan Timoney - AT&T, ONAP TSC and PTLs

ONAP SECCOM

Pawel Pawlak - Individual

Amy Zwarico - AT&T

Maggie Cogde - DoD

Muddasar Ahmed - MITRE

Tony Hansen - AT&T

ONAP ARCCOM

Matthew Wakins, Kevin Sandi - LF IT

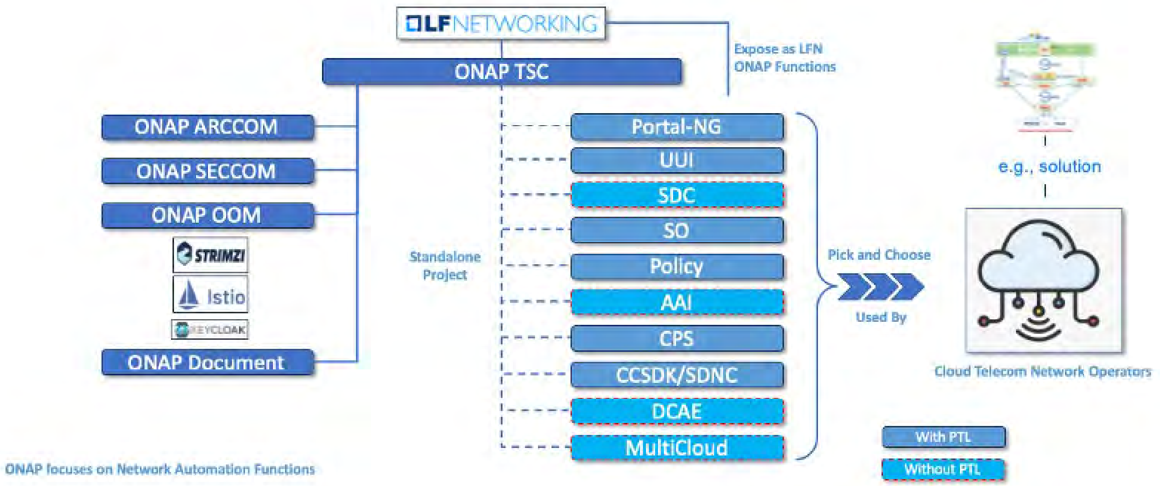
Jill Lovato - LF Marketing

LJ Illuzi - ONAP PMO

1. Evolutionary Path

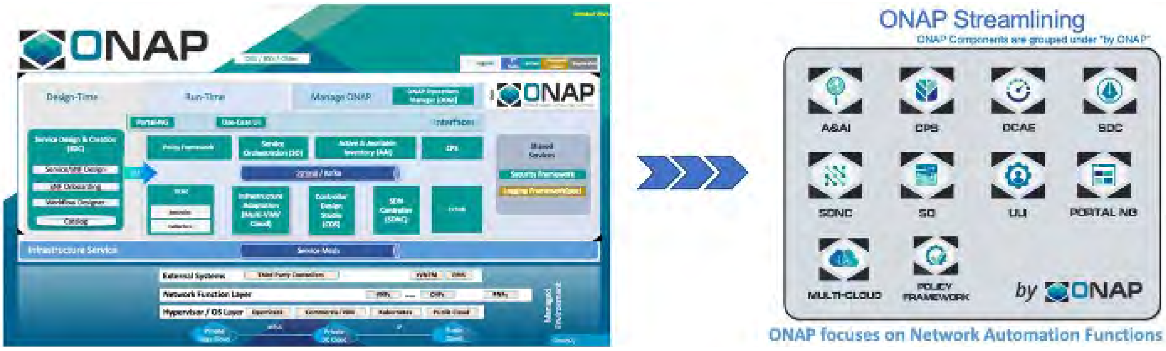
1.1 ONAP Organization

- A new ONAP organization structure is in place.
- The governance and common services teams continue to guild the projects toward coherence.
- ONAP functions are exposed individually and directly to consumers.
- Each ONAP project reports key updates to the ONAP governance committees to ensure cohesive and unified evolution.



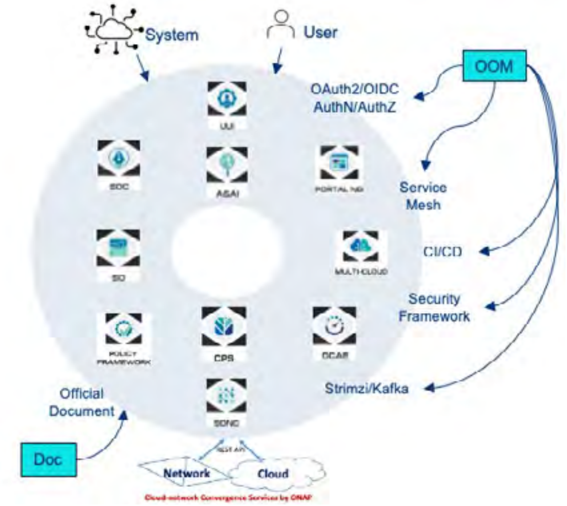
1.2 Monolithic to Modular Transition

- **Initial Architecture**: Centralized, tightly coupled platform for orchestration, management, and policy enforcement.
- **Transformation Strategy**: Component decoupling, independent lifecycle management, API-driven integration.
- **Benefits**: Rapid adoption in hybrid environments, flexible deployment patterns, reduced maintenance overhead.



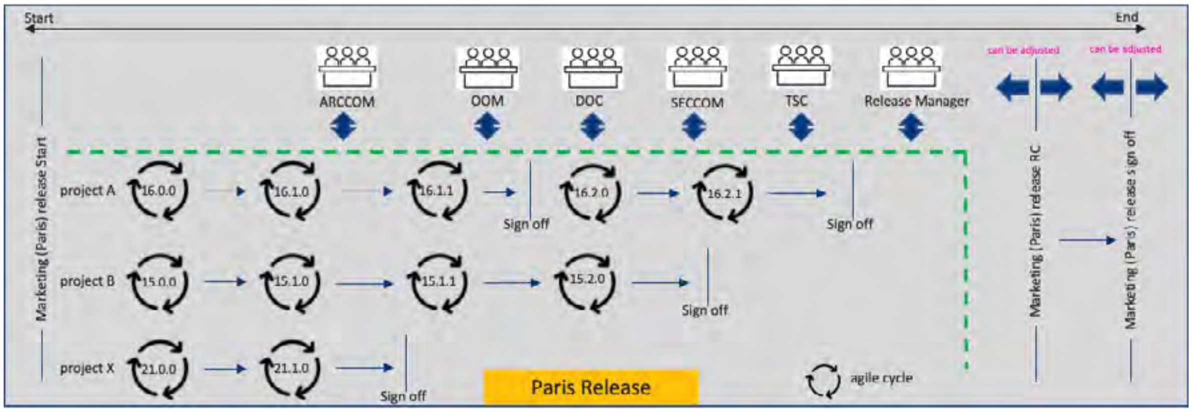
1.3 Semi-Standalone Deployment Model

- Modular components - SO, SDC, Policy, SDNC, CPS, Portal-NG, UUI, A&AI, DCAE, MultiCloud - function independently.
- Enhanced compatibility with cloud-native environments.
- Interoperability frameworks (Service Mesh for secure inter-module communications and other common services) designed and maintained by ONAP governance bodies and OOM.



1.4 Semi-Standalone Release Cycles

ONAP Governance and common services will maintain their own recommendation and consultation cycles, aligned with the marketing release schedule, where individual ONAP projects manage their own features and lifecycles. This flexible release cadence allows projects to deliver components as often as needed within the marketing cycle.



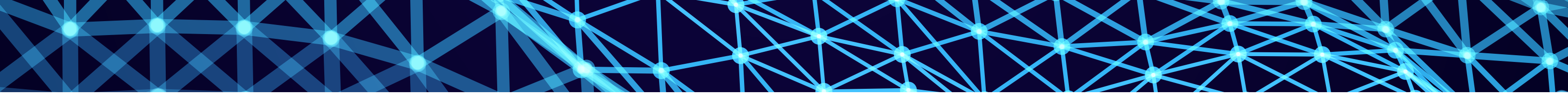
2. Architectural Foundations

1. **Intent-Based Orchestration**

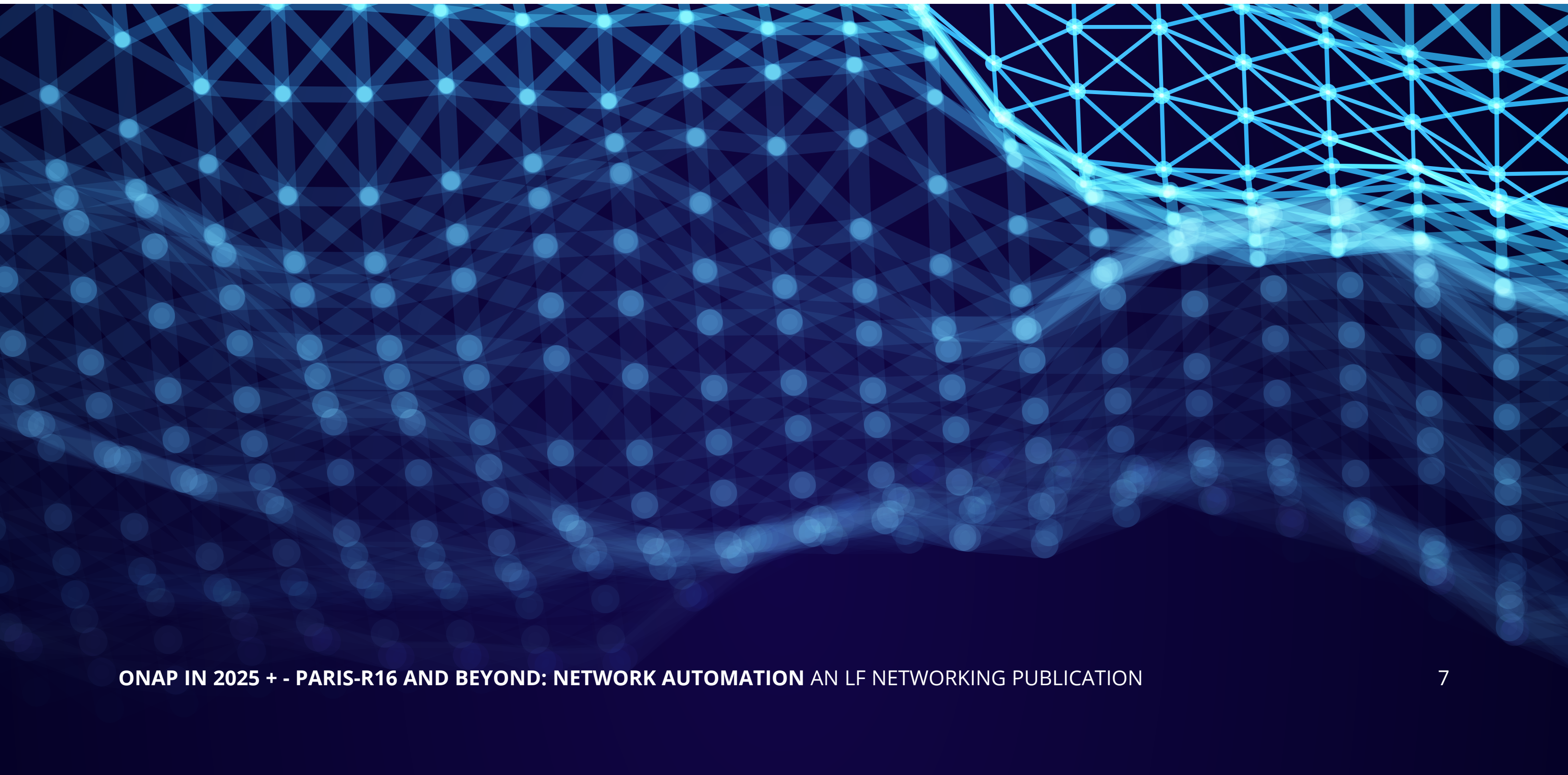
   - **Intent Processing**: Natural language service requests are translated into automation workflows through domain-specific LLMs.
   - **Human-Readable Intents**: Accepts user intents via GUI or NLP/GenAI interfaces for seamless integration.
   - **LLM Integration**: Collaborates with the Intent Analysis Server and LLM Adaptation layer to convert natural language inputs into structured intent specifications.
   - **Intent Decomposition**: Performs parsing, validation, and decomposition of high-level intents into domain-specific sub-intents across network domains.

2. **Standards Alignment**

   - **Standards Compliance**: Alignment with ETSI NFV MANO, 3GPP specifications, IETF, TMForum Open APIs, O-RAN standards.
   - **5G Network Slicing**: Orchestration maps to 3GPP specifications (TS 28.530, TS28.531, TS 28.541) for slice lifecycle management.
   - **O-RAN SMO integration**: Support for O1/O2 interfaces, enabling ONAP to orchestrate RAN elements within an open, disaggregated RAN environment.
   - **Community Engagement**: Active participation (IE Active Participation) within LFN for architecture, security, and CI/CD best practices.
   - **Model-Driven Configuration**: Adoption of ™ Forum YANG models for service and device configuration via NETCONF/RESTCONF.
   - **Zero Trust Architecture**: Implementation aligned with NIST SP 800-207 principles.
   - **Software Supply Chain Security**: Conformance with OpenSSF best practices and SLSA requirements.
   - **SBOM Transparency**: SBOM generation following the SPDX ISO/IEC standard.
   - **Cryptography Transparency**: Exploration of CBOM (Cryptography Bill of Materials) for enhanced cryptographic visibility and compliance



3. **Security-First Design**
    - **Service Mesh Security**: Istio-based service mesh with mutual TLS (mTLS 1.3) for secure inter-component communication.
    - **Authentication and Authorization**: OAuth2/OIDC integration with Keycloak for centralized identity and access management.
    - **Open Source Security Compliance**: Alignment with OpenSSF best practices - ONAP CPS and Policy components have achieved OpenSSF Gold Badging.
    - **Centralized Administration**: Portal-NG provides unified and secure administrative access across ONAP components.
    - **Hardened Deployments**: Enforced HTTPS-only communication, non-root pod execution, and proactive CVE mitigation for enhanced runtime security.
4. **Cloud-Native Microservices**
    - **Kubernetes Deployment**: Managed through OOM and MultiCloud with full support for hybrid and multi-cloud infrastructures.
5. **Continuous Delivery and GitOps**
    - **CD-based Deployment and Reconciliation**: Utilize ArgoCD, (with FluxCD under future consideration) for automated individual component deployment and seamless runtime orchestration upgrades.



3. Detailed Functional Architecture

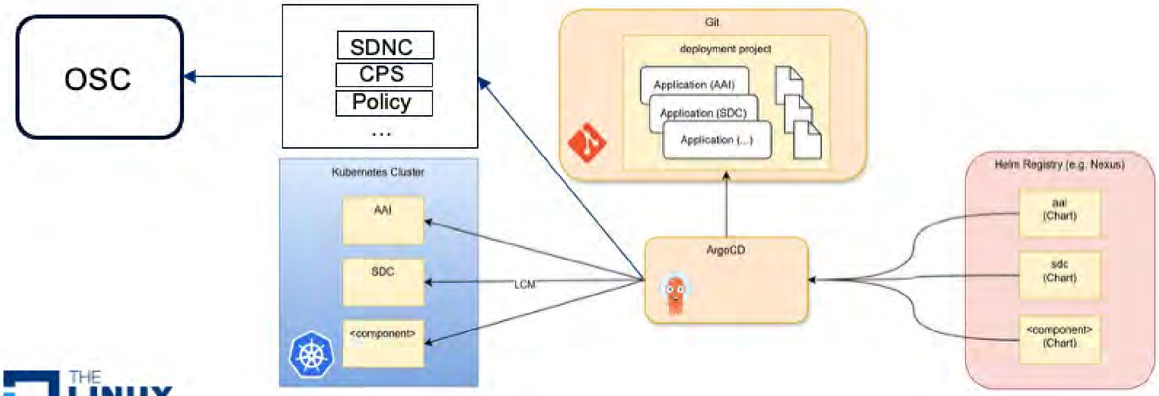
3.1 Core Components

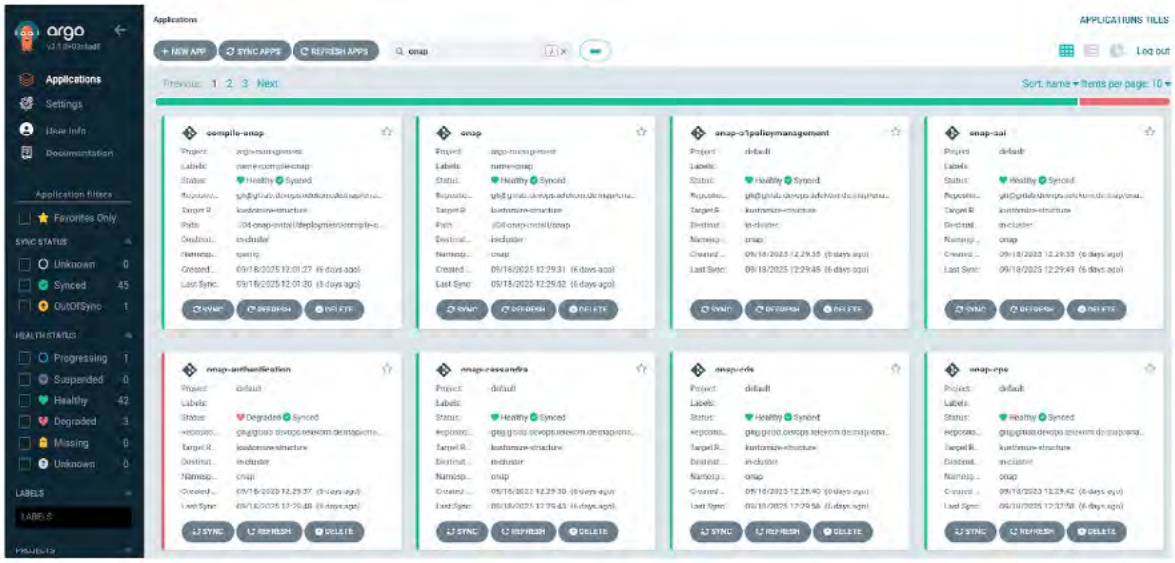
- **SDC**: Service design, onboarding for VNFs/CNFs; ASD and ETSI SOL compliance. It is the design-time and onboarding environment for ONAP. It allows operators to model, onboard, certify, and distribute services and resources into the ONAP ecosystem, ensuring that orchestration (SO), policies, and inventory all work from a consistent set of artifacts.
- **SO**: Orchestration engine for end-to-end services, network slicing. It is the execution engine that turns service designs (from SDC) into running services. It manages instantiation, scaling, healing, modification, and termination of network functions across multi-cloud, multi-vendor, hybrid environments - enabling ONAP's intent-based, closed-loop automation.
- **SDNC**: Multi-domain network configuration and orchestration. It is the domain controller responsible for configuring and managing transport and network connectivity services. It bridges ONAP's orchestration (SO, Policy) with the actual network devices and controllers, enabling automated, closed-loop, intent-driven network operations. Note that this component is also used by the OSC OAM component - a good example of cross-community collaboration.
- **Multi-Cloud**: Abstraction for diverse VIM and Kubernetes environments. It is the cloud abstraction and integration layer of ONAP, by providing an abstraction layer for interacting with different cloud environments. It enables ONAP to orchestrate services seamlessly across multiple clouds and infrastructures, making hybrid, multi-cloud telecom deployments possible.
- **DCAE**: Analytics, telemetry ingestion, closed-loop triggers. It is the telemetry and analytics engine of ONAP. It collects network/service data, analyzes it in real time, and produces events that trigger policies and orchestrations - enabling closed-loop, intent-driven automation in telecom networks.
- **Policy Framework**: The ONAP Policy Framework is a comprehensive policy design, deployment, and execution environment. The Policy Framework is the decision making component in an ONAP system. It allows you to specify, deploy, and execute the governance of the features and functions in your ONAP system, be they closed loop, orchestration, or more traditional open loop use case implementations.
- **CPS-Core**: Is a YANG-modeled service that provides a model-driven persistence layer for storing any data or configuration defined in YANG format.

- **CPS-NCMP**: Serves as a transparent proxy to multiple RAN OAM CM SMOS. It exposes the 3GPP ProvMnS, which forms the foundation for RAN OAM CM, and provides a lightweight, scalable, model-driven platform to store, retrieve, change and manage configuration data for network functions and services.
- **A&AI**: Real-time topology and inventory. It is the central real-time inventory and knowledge graph of the ONAP ecosystem. It ensures that orchestration, policy, and closed-loop automation all operate on a consistent, up-to-date view of the network.
- **Portal-NG**: Unified GUI for ONAP, acts as the primary UI hub for ONAP users and administrators. It is the modern, centralized UI framework for ONAP. It enables a single point of access with role-based control, integrates UIs from all ONAP components, and provides a consistent, extensible, and secure user experience for operators, designers, and admins.
- **UUI**: User Interfaces UI with Intent-based automation support, Model-As-A-Service, NLP server, Intent-Analysis server, LLM Adaptation, User Centric GenAI/NLP front-end. This component's AI capabilities are a good example of ONAP's GenAI/NLP integration and could serve as a stepping stone toward future Agentic AI-based workflows.
- **CDS**: A centralized mechanism for designing and managing Day 0/1/2 configurations across heterogeneous network environments. It provides model-driven configuration, TOSCA alignment, a self-service design studio, and an execution engine that interacts with controllers such as SDNC, SO, and others.

3.2 OOM Support of Git and CD-based ONAP Component Installation

- **GitOps-Based Deployments**: Since the ONAP Paris release, OOM supports individual deployments using the GitOps approach with tools such as ArgoCD are already in use at Deutsche Telekom and are included in the ONAP Paris release.
- For more details, refer to the official ONAP documentation: ONAP OOM ArgoCD Deployment Guide.





compile-onap
Project: argo-management
Labels: name=compile-onap
Status: Healthy Synced
Reposito...: git@gitlab.devops.telekom.de:onap/ona...
Target R: kustomize-structure
Path: /04-onap-install/deployment/compile-o...
Destinat...: in-cluster
Namesp...: [illegible]
Created...: 09/18/2025 12:01:27 (6 days ago)
Last Sync: 09/18/2025 12:01:30 (6 days ago)

onap
Project: argo-management
Labels: name=onap
Status: Healthy Synced
Reposito...: git@gitlab.devops.telekom.de:onap/ona...
Target R: kustomize-structure
Path: /04-onap-install/onap
Destinat...: in-cluster
Namesp...: onap
Created...: 09/18/2025 12:29:31 (6 days ago)
Last Sync: 09/18/2025 12:29:32 (6 days ago)

onap-a1policymanagement
Project: default
Labels:
Status: Healthy Synced
Reposito...: git@gitlab.devops.telekom.de:onap/ona...
Target R: kustomize-structure
Destinat...: in-cluster
Namesp...: onap
Created...: 09/18/2025 12:29:35 (6 days ago)
Last Sync: 09/18/2025 12:29:45 (6 days ago)

onap-aai
Project: default
Labels:
Status: Healthy Synced
Reposito...: git@gitlab.devops.telekom.de:onap/ona...
Target R: kustomize-structure
Destinat...: in-cluster
Namesp...: onap
Created...: 09/18/2025 12:29:35 (6 days ago)
Last Sync: 09/18/2025 12:29:49 (6 days ago)

onap-authentication
Project: default
Labels:
Status: Degraded Synced
Reposito...: git@gitlab.devops.telekom.de:onap/ona...
Target R...: kustomize-structure
Destinat...: in-cluster
Namesp...: onap
Created...: 09/18/2025 12:29:37 (6 days ago)
Last Sync: 09/18/2025 12:29:48 (6 days ago)

onap-cassandra
Project: default
Labels:
Status: Healthy Synced
Reposito...: git@gitlab.devops.telekom.de:onap/ona...
Target R...: kustomize-structure
Destinat...: in-cluster
Namesp...: onap
Created...: 09/18/2025 12:29:30 (6 days ago)
Last Sync: 09/18/2025 12:29:43 (6 days ago)

onap-cds
Project: default
Labels:
Status: Healthy Synced
Reposito...: git@gitlab.devops.telekom.de:onap/ona...
Target R...: kustomize-structure
Destinat...: in-cluster
Namesp...: onap
Created...: 09/18/2025 12:29:40 (6 days ago)
Last Sync: 09/18/2025 12:29:58 (6 days ago)

onap-cps
Project: default
Labels:
Status: Healthy Synced
Reposito...: git@gitlab.devops.telekom.de:onap/ona...
Target R...: kustomize-structure
Destinat...: in-cluster
Namesp...: onap
Created...: 09/18/2025 12:29:42 (6 days ago)
Last Sync: 09/18/2025 12:27:58 (6 days ago)

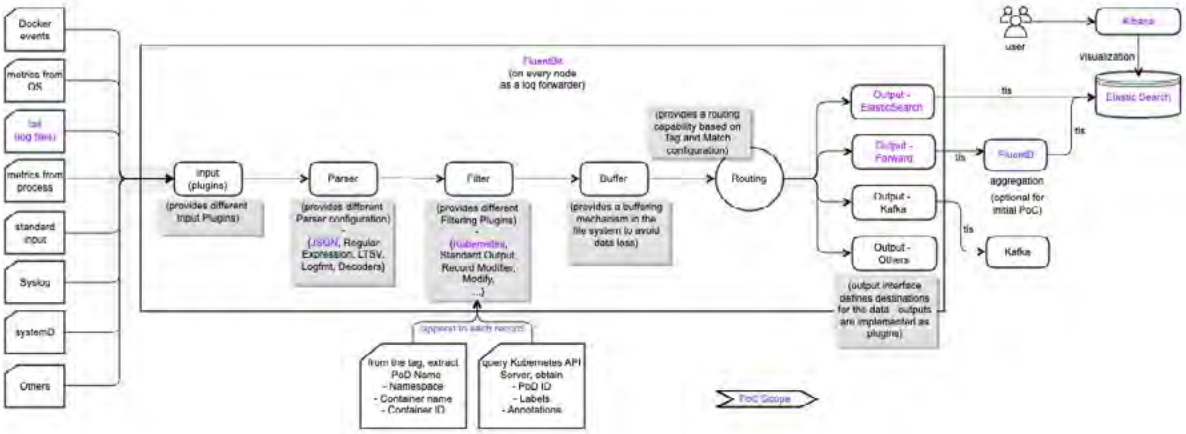
3.3 Shared Services & Security Layers

- **Logging and Tracing Framework (PoC)**: Designed for PoC implementations, adopting an open-source, standards-based logging architecture.
- **Unified Log Output**: Once all ONAP components output logs to STDOUT/STDERR, any standard log pipeline can be integrated, allowing vendor-specific implementations of the logging stack.
- **Ingress Security**: Ingress controllers integrated with OAuth2 proxy to securely expose ONAP microservices to users and external systems.
- **Authentication & Authorization Layer**: OAuth2 proxy adds OAuth2/OIDC authentication and authorization in front of services, typically using Keycloak for identity and access management.
- **Secure Inter-Component Communication**: ONAP components communicate securely over REST APIs through the Service Mesh. When needed, the Istio Ingress Gateway is configured to manage and protect incoming traffic.
- **API Protection**: APIs are secured through mTLS 1.3 and role-based access control (RBAC) enforced by the service mesh.

3.4 Observability

- ONAP observability provides end-to-end visibility across ONAP's orchestration, control, and assurance layers, enabling faster fault detection and telecom-grade service assurance.
- Metrics, logs, and traces can be exported through endpoints exposed for OpenTelemetry and Prometheus, enhancing monitoring, efficiency, and scalability.
- DCAE collects VES telemetry and performs analytics and event correlation. The Policy framework defines dynamic response to metrics and anomaly patterns. CPS/NCMP provides telemetry data persistence, and SO and SDNC export performance metrics and tracing data for workflow visibility.
- ONAP-generated logs are collected by log collectors (such as FluentBit), and can be aggregated, stored, and visualized using the operators' observability stack (e.g., FluentD, ElasticSearch, Kibana, Prometheus, Kafka, etc.).

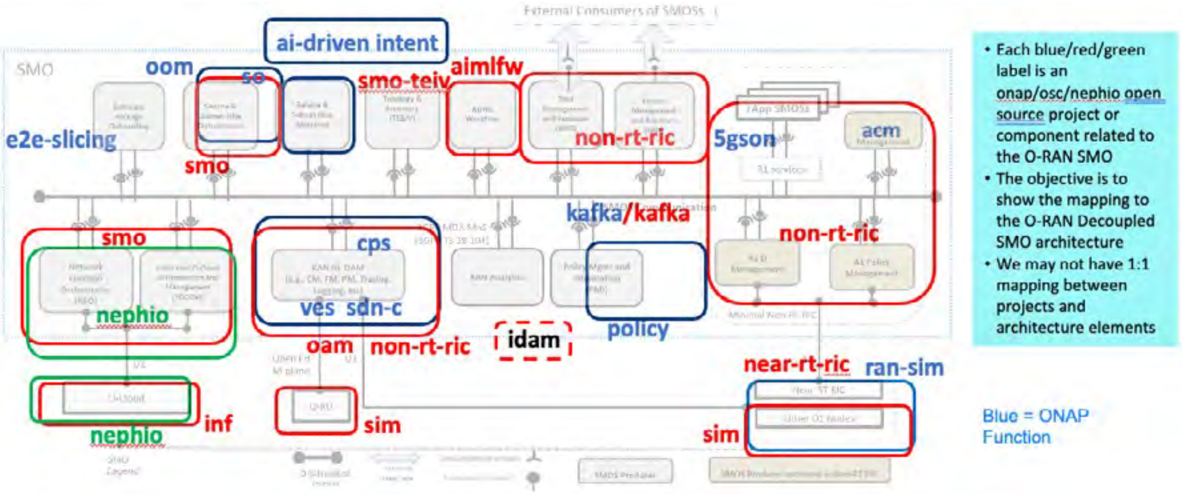
Finally, ONAP CI/CD pipelines incorporate SBOM and CBOM generation to ensure a secure and transparent software supply chain.


Docker events
metrics from OS
tail (log files)
metrics from process
standard input
Syslog
systemD
Others
FluentBit (on every node as a log forwarder)
input (plugins)
(provides different Input Plugins)
Parser
(provides different Parser configuration) - (JSON, Regular Expression, LTSV, Logfmt, Decoders)
Filter
(provides different Filtering Plugins) - (Kubernetes, Standard Output, Record Modifier, Modify, ...)
Buffer
(provides a buffering mechanism in the file system to avoid data loss)
(provides a routing capability based on Tag and Match configuration)
Routing
Output - ElasticSearch
Output - Forward
Output - Kafka
Output - Others
(output interface defines destinations for the data outputs are implemented as plugins)
append to each record
from the tag, extract PoD Name - Namespace - Container name - Container ID
query Kubernetes API Server, obtain - PoD ID - Labels - Annotations
user
Kibana
visualization
Elastic Search
tls
tls
FluentD
aggregation (optional for initial PoC)
tls
tls
Kafka
PoC Scope

4. ONAP, O-RAN SC and Nephio Collaborations for O-RAN SMO

ONAP, O-RAN SC (OSC), and Nephio are collaborating to build the OSC SMO ecosystem as outlined below (with input from N.K. Shankar). Within this collaboration, several modular ONAP functions can be utilized, while OSC SMO FOCOM and NFO are developed by leveraging Nephio's capabilities, alongside ETSI-compliant OSC SMO components.

ONAP's security capabilities (such as OOM's Service Mesh, Istio Ingress Gateway, OAuth2/OIDC Authentication and Authorization) can be leveraged to secure OSC SMO components with some integration effort. In addition, ONAP's automated CVE detection and secure software supply chain processes can further strengthen the overall ecosystem.



- Each blue/red/green label is an onap/osc/nephio open source project or component related to the O-RAN SMO
- The objective is to show the mapping to the O-RAN Decoupled SMO architecture
- We may not have 1:1 mapping between projects and architecture elements

Blue = ONAP Function

5. AI and GenAI Integration

- **Model-as-a-Service for Telecom**: Deploying AI models for orchestration and fault management.
- **AI-Driven Intent Parsing**: Converting human-readable intents to technical configurations.
- **Future Considerations**:
    - **Predictive Capabilities**: Network anomaly detection, capacity forecasting.
    - **Adaptive Policy Execution**: AI-based dynamic policy enforcement.

6. Use Cases & Real-World Deployments

6.1 Global Operator Implementations

- **Deutsche Telekom**: SMO and NonRT-RIC.
    - Deutsche Telekom adopted ONAP core components as part of its TNAP automation solution in its production environment this year. Based on specific use cases, components such as SO, AAI, CPS-Core, CDS and Policy, Portal-NG, and others are being selected. Development is centered around SO, AAI, CDS, CPS, Policy Framework, and Portal-NG.
    - Deutsche Telekom is also developing an SMO solution, which enables RAN automation, including network slicing, RAN optimization with NonRT-RIC / rApp capabilities. This solution aims to manage the O-RAN network stack within Deutsche Telekom.
- **China Mobile**: GenAI integration in MaaS.
    - China Mobile has contributed to large model-related developments in the New Delhi and Oslo releases of ONAP, introducing large model technologies into the ONAP community to enable intelligent decision-making, optimization capabilities, and enhanced customer experiences in network orchestration. Additionally, China Mobile has provided an intent-driven, end-to-end autonomous network reference implementation as a demonstration application.
    - Notably, in the Oslo release, China Mobile developed the Knowledge Assistant Project, based on the MaaS (Model-as-a-Service) platform. This project includes capabilities for knowledge base management, knowledge assistant management, and interfaces for invoking knowledge assistants. By encapsulating large model capabilities into standardized service interfaces, the project lowers the barriers to adopting large model technologies. This initiative expands ONAP’s application scope in network automation and lays the groundwork for future innovations in large models and MaaS-related technologies.

- **China Telecom**: 6G orchestration research.
    - China Telecom is a founding member of ONAP. From R8 to R14, the company focused on researching and developing intent-based networking to support autonomous networks, particularly through the CCVPN and E2E Slicing use cases.
    - Currently, China Telecom is focusing on 6G network research, aiming to enhance orchestration capabilities by integrating network, sensing, intelligence, and computing. In 2024, the company built a lightweight orchestration platform inspired by the ONAP architecture. Now, it is developing an end-to-end experimental platform to support both research and standardization efforts for 6G.

- **Ericsson**: Policy Framework + CPS.
    - Ericsson's SMO-related offerings - EIAP (Ericsson Intelligent Automation Platform) and ESOA (Ericsson Service Orchestration and Assurance) - provide advanced automation and orchestration capabilities for diverse RAN environments, including both traditional and O-RAN.
    - The Policy-Clamp component from the ONAP's Policy Framework plays a major role in the EIC functionality within EIAP. Policy-Clamp is responsible for the lifecycle management of rApps in EIC and works in conjunction with EIC adapter microservices to ensure complete rApps lifecycle management. Additionally, EIAP is also considering the use of the OPA-PDP component from ONAP's Policy Framework within its coordination-management component. This discussion is currently in its early stage; however, OPA-PDP has strong potential for integration into the coordination-management use case.
    - The CPS-Core Is a YANG-modeled service that provides a model-driven persistence layer for storing any data or configuration defined in YANG format.
    - The CPS-NCMP component, which is part of Ericsson EIAP, serves as a transparent proxy to multiple RAN OAM CM SMOS. It exposes the 3GPP ProvMns, which forms the foundation for RAN OAM CM.

6.2 Blueprint Implementations

- 5G Network Slicing.
- vCPE/BBS.
- VoLTE orchestration.
- Optical Transport Automation (CCVPN & MDONS).
- AI-powered intent networks.

7. Strategic Roadmap Beyond Paris

Note: The following roadmap plan is still under discussion and has not been finalized.

- API harmonization across modules.
- Broader AI integration via LF AI & Data.
- Operator-ready AI toolkits
- Strengthened security (Ambient Mesh, CVE automation).
- Cross-community synergies with O-RAN SC and Nephio.
- Sustainability and energy efficiency.

7.1 AI Roadmap

Short Term (2025 Q4)

- **AI-Assisted Intent Parsing**: Deploy AI-driven intent parsing for selected use cases to enhance automation and contextual understanding.
- **Predictive Maintenance Integration (PoC)**: Incorporate predictive maintenance models into DCAE to enable proactive network monitoring, optimization and anomaly detection capabilities (PoC implementation). E.g., 5G Anomaly detection PoC implemented by Georgia Tech in collaboration with the DoD.
- **Open-Source Collaboration**: Expose ONAP GenAI functions (e.g., UUI NLP, MaaS) to other open-source communities to promote interoperability and ecosystem growth.

Mid-Term (2026 - 2027) - Under Discussion

- Achieve advanced AI-driven orchestration across multiple domains.
- Enable cross-domain AI decision-making for end-to-end service optimization.
- Explore the LF Agentic AI framework candidate (e.g., Essedum) to support autonomous orchestration. Other Agentic AI frameworks could be considered.
- Integrate, coordinate, and manage AI Agents for coordinated and intelligent network operations.

Long-Term (2028+) - Under Discussion

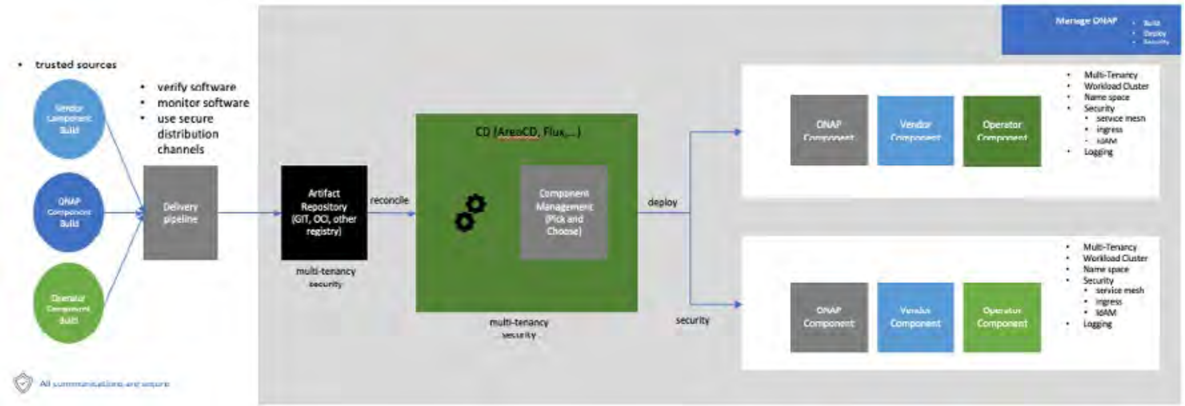
- ONAP serves as an autonomous network automation collection, interoperating with other AI-driven domains.

7.2 AI Key Capabilities Exploration - Under Discussion

- AI-driven Intent Parsing
  - Translates natural language into machine-executable workflows.
  - Supports multiple languages and telecom-specific ontologies.
- Predictive Network Management
  - Employs AI models to predict faults, congestion, or SLA violations.
  - Executes automated mitigation actions through the Policy framework.
- Closed-Loop Automation with AI
  - Performs real-time analysis of telemetry via DCAE.
  - Adapts policies dynamically based on predictive insights.
- Generative AI for Service Design
  - Auto-generates service templates within SDC.
  - Suggests optimal configurations using historical and contextual data.
- AI-Driven Security
  - Detects threats and anomalies through AI-based behavioral models.
- Automated CI/CD Pipelines
  - Integrates automated SBOM and CBOM scanning within build workflows.
  - Provides CVE remediation recommendations powered by AI insights.

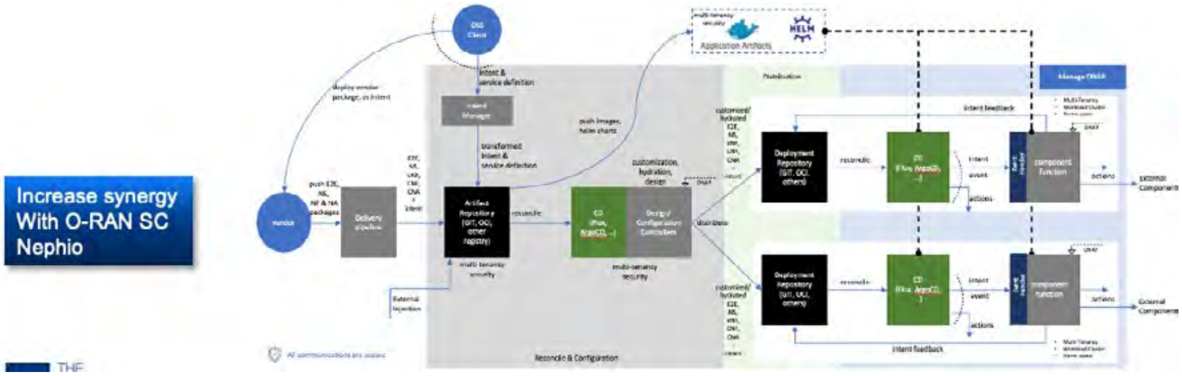
7.3 Generic Repository-Based Component Build and Deployment - Under Discussion

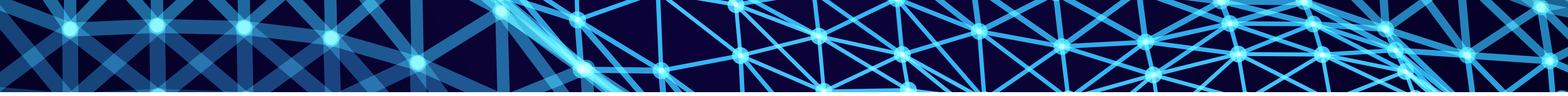
- **Multi-Tenancy and Multi-Workload Support**: Enables multi-tenancy, multi-workload, and multi-namespace environments for flexible deployments.
- **Hybrid Component Deployment**: ONAP components can be deployed alongside other vendor or operator components through GitOps workflows using ArgoCD (with FluxCD under consideration).



7.4 Generic Repository-Based Packages/Intents & CD-based Orchestration - Under Discussion

- **GitOps-Driven Onboarding**: Packages and intents are onboarded through Git triggers that initiate ONAP function operations via continuous delivery tools (ArgoCD / Flux).
- **Operator-Based Execution**: Corresponding operators invoke individual ONAP functions based on the defined intent targets.
- **Multi-Tenant Runtime Environment**: Applications, packages, and intents run within a multi-tenancy, multi-workload cluster and multi-namespace runtime environment.


Increase synergy With O-RAN SC Nephio
OSS Client
deploy vendor package, as intent
intent & service definition
Intent Manager
transformed intent & service definition
push images, helm charts
Application Artifacts
HELM
vendor
push E2E, NS, NF & NA packages
Delivery pipeline
Artifact Repository (GIT, OCI, other registry)
multi tenancy security
External Injection
reconcile
CD (Flux, ArgoCD, ...)
Design/ Configuration Controllers
customization, hydration, design
multi-tenancy security
distribute
Distribution
customized/ hydrated E2E, NS, ...
Deployment Repository (GIT, OCI, others)
reconcile
CD (Flux, ArgoCD, ...)
intent
event
actions
component function
actions
External Component
intent feedback
Manage ONAP
Multi-Tenancy
Workload Cluster
Name space
Reconcile & Configuration
All communications are secure



8. Conclusion

The Paris-R16 release reinforces ONAP's position as the most comprehensive open-source network automation solution, laying a strong foundation for the AI-driven, secure, and intent-based networks of the future. With its modular microservice architecture, service-mesh-based security, AI/ML-enhanced orchestration, and deep alignment with global telecom standards, ONAP is strategically positioned to meet the operational and business demands of next-generation networks.

As operators face increasing complexity across 5G deployments, cloud-native network functions, and emerging 6G use cases, ONAP's 2025 roadmap positions it as a cornerstone for fully autonomous network operations. Its modular components are designed to interoperate with and provide network automation capabilities to other open-source communities, extending ONAP's impact beyond its traditional boundaries.

By converging AI, automation, and open standards, ONAP enables telecom operators to streamline operations, accelerate innovation, and thrive in an increasingly dynamic and competitive digital ecosystem.