ETSI GR ZSM 004 V2.1.1 (2022-01)

Zero-touch network and Service Management (ZSM); Landscape

Disclaimer

The present document has been produced and approved by the Zero-touch network and Service Management (ZSM) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
RGR/ZSM-004ed211_Landscape

Keywords
management, network, service

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Zero-touch network and Service Management (ZSM).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document updates the existing landscape report for Zero-touch network and Service Management (ZSM) based on its current and future developments. It identifies and includes information about activities in other bodies (such as Standards Developing Organizations, Open Source Communities, and Industry Associations) that are relevant to the work in ISG ZSM. Recommendations will be derived for the ISG ZSM work.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS ZSM 007: "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".

[i.2] ETSI GS ZSM 001: "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios".

[i.3] ETSI GR NFV 001 (V1.2.1): "Network Functions Virtualisation (NFV); Use Cases".

[i.4] ETSI GS NFV 004 (V1.1.1): "Network Functions Virtualisation (NFV); Virtualisation Requirements".

[i.5] ETSI GS NFV 002 (V1.2.1): "Network Functions Virtualisation (NFV); Architectural Framework".

[i.6] ETSI GS NFV-MAN 001 (V1.1.1): "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.7] ETSI GS NFV-IFA 013 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification".

[i.8] ETSI GS NFV-IFA 014 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Network Service Templates Specification".

[i.9] ETSI GS NFV-IFA 011 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; VNF Descriptor and Packaging Specification".

[i.10] ETSI GR NFV-IFA 023 (V3.1.1): "Network Functions Virtualisation (NFV); Management and Orchestration; Report on Policy Management in Mano; Release 3".

[i.11] ETSI GR NFV-IFA 015 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on NFV Information Model".

[i.12] ETSI GR NFV-IFA 024 (V2.1.1): "Network Function Virtualisation (NFV) Release 2; Information Modeling; Report on External Touchpoints related to NFV Information Model".

[i.13] ETSI GS NFV-IFA 027 (V2.4.1): "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Performance Measurements Specification".

[i.14] ETSI GR NFV-IFA 021 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on management of NFV-MANO and automated deployment of EM and other OSS functions".

[i.15] ETSI GS NFV-IFA 031 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Requirements and interfaces specification for management of NFV-MANO".

[i.16] ETSI GR NFV-IFA 022 (V3.1.1): "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services".

[i.17] ETSI GS NFV-SOL 004 (V2.5.1): "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; VNF Package specification".

[i.18] ETSI GS NFV-SOL 005 (V2.4.1): "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; RESTful protocols specification for the Os-Ma-nfvo Reference Point".

[i.19] ETSI GR NFV-IFA 028: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on architecture options to support multiple administrative domains".

[i.20] ETSI GS NFV-IFA 030: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Multiple Administrative Domain Aspect Interfaces Specification".

[i.21] ETSI GS NFV-IFA 032: "Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Interface and Information Model Specification for Multi-Site Connectivity Services".

[i.22] ETSI GS MEC 002 (V2.1.1): "Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements".

[i.23] ETSI GS MEC 003 (V2.1.1): "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[i.24] ETSI GS MEC 010-1 (V1.1.1): "Mobile Edge Computing (MEC); Mobile Edge Management; Part 1: System, host and platform management".

[i.25] ETSI GS MEC 010-2 (V2.1.1): "Multi-access Edge Computing (MEC); MEC Management; Part 2: Application lifecycle, rules and requirements management".

[i.26] ETSI GS MEC 012 (V1.1.1): "Mobile Edge Computing (MEC); Radio Network Information API".

[i.27] ETSI GS MEC 013 (V1.1.1): "Mobile Edge Computing (MEC); Location API".

[i.28] ETSI GS MEC 014 (V1.1.1): "Mobile Edge Computing (MEC); UE Identity API".

[i.29] ETSI GS MEC 015 (V1.1.1): "Mobile Edge Computing (MEC); Bandwidth Management API".

[i.30] ETSI GS MEC 028 (V2.1.1): "Multi-access Edge Computing (MEC); WLAN Information API".

[i.31] ETSI GS MEC 029 (V2.1.1): "Multi-access Edge Computing (MEC); Fixed Access Information API".

[i.32] ETSI GS MEC 030 (V2.1.1): "Multi-access Edge Computing (MEC); V2X Information Service API".

[i.33] ETSI GR ENI 001 (V1.1.1): "Experiential Networked Intelligence (ENI); ENI use cases".

[i.34] ETSI GS ENI 002 (V2.1.1): "Experiential Networked Intelligence (ENI); ENI requirements".

[i.35] ETSI GS ENI 005 (V1.1.1): "Experiential Networked Intelligence (ENI); System Architecture".

[i.36] TM Forum Frameworx™.

NOTE: Available at https://www.tmforum.org/frameworx-homepage/.

[i.37] TM Forum Open Digital Architecture.

NOTE: Available at https://www.tmforum.org/collaboration/open-digital-architecture-oda-project/.

[i.38] TM Forum Open APIs.

NOTE: Available at https://www.tmforum.org/open-apis/.

[i.39] TM Forum Catalyst Program.

NOTE: Available at https://www.tmforum.org/collaboration/catalyst-program/catalyst-program-benefits/.

[i.40] LF ONAP External APIs Framework Project.

NOTE: Available at https://wiki.onap.org/display/DW/External+API+Framework+Project.

[i.41] TMF Open Digital Lab project.

NOTE: Available at https://www.tmforum.org/open-digital-lab/.

[i.42] Open API Map portal.

NOTE: Available at https://projects.tmforum.org/wiki/display/API/Open+API+Table?-ga=2.120461313.863093364.1543419979-18401513.1531316873.

[i.43] TM Forum IG1166: "ODA Architecture Vision R18.0.0".

NOTE: Available at https://www.tmforum.org/resources/exploratory-report/ig1166-oda-architecture-vision-r18-0-0/.

[i.44] TM Forum IG1167: "ODA Functional Architecture R19.0.1".

NOTE: Available at https://www.tmforum.org/resources/standard/ig1167-oda-functional-architecture-r19-0-0/.

[i.45] TM Forum GB998: "Open Digital Architecture (ODA) Concepts & Principles R19.0.1".

NOTE: Available at https://www.tmforum.org/resources/reference/gb998-open-digital-architecture-oda-concepts-principles-r19-0-0/.

[i.46] TM Forum GB921: "Business Process Framework (eTOM) Suite Release 18.5".

NOTE: Available at https://www.tmforum.org/resources/suite/gb921-business-process-framework-etom-suite-release-18-5/.

[i.47] TM Forum GB922: "Standards Addenda for Information Framework R18.5".

NOTE: Available at https://www.tmforum.org/resources/suite/gb922-standards-addenda-information-framework-r18-5/.

[i.48] TM Forum IG1171: "ODA Component Definition R19.0.1".

NOTE: Available at https://www.tmforum.org/resources/exploratory-report/ig1171-oda-component-definition-r19-0-0/.

[i.49] TM Forum TMF071: "ODA Terminology R19.0.1".

NOTE: Available at https://www.tmforum.org/resources/reference/tmf071-oda-terminology-r19-0-0/.

[i.50] TM Forum TMF633: "Service Catalog API REST Specification R18.5.1".

NOTE: Available at https://www.tmforum.org/resources/specification/tmf633-service-catalog-api-rest-specification-r18-5-0/.

[i.51] TM Forum TMF641: "Service Ordering API REST Specification R18.5.1".

NOTE: Available at https://www.tmforum.org/resources/specification/tmf641-service-ordering-api-rest-specification-r18-5-0/.

[i.52] TM Forum TMF652: "Resource Ordering Management API REST Specification R16.5.1".

NOTE: Available at https://www.tmforum.org/resources/specification/tmf652-resource-ordering-management-api-rest-specification-r16-5-1/.

[i.53] TM Forum TMF640: "Service Activation and Configuration API REST Specification R18.5.1".

NOTE: Available at https://www.tmforum.org/resources/specification/tmf640-service-activation-and-configuration-api-rest-specification-r18-5-0/.

[i.54] TM Forum TMF638: "Service Inventory API REST Specification R18.5.1".

NOTE: Available at https://www.tmforum.org/resources/specification/tmf638-service-inventory-api-rest-specification-r18-5-0/.

[i.55] TM Forum TR262: "Management Platform Blueprint and Application to Hybrid Infrastructure R17.5.1".

NOTE: Available at https://www.tmforum.org/resources/technical-report/tr262-management-platform-blueprint-and-application-to-hybrid-infrastructure-r17-5-0/.

[i.56] TM Forum TR229A: "User Stories for Hybrid Infrastructure Platform R17.0.1".

NOTE 1: Available at https://www.tmforum.org/resources/technical-report/tr229a-user-stories-for-hybrid-infrastructure-platform-r17-0-1/.

NOTE 2: A list of all public TM Forum documents (currently over 500) can be found here - https://www.tmforum.org/resources/?filter_security=2597.

NOTE 3: All "member only" TM Forum documents are available for formal Liaison.

[i.57] MEF 55: "Lifecycle Service Orchestration (LSO): Reference Architecture and Framework", March 2016.

NOTE: Available at https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_55.pdf.

[i.58] MEF 55.0.1: "Amendment to MEF 55 - Operational Threads", October 2017.

NOTE: Available at http://www.mef.net/resources/technical-specifications/download?id=99&fileid=file1.

[i.59] 3GPP TR 23.791 (V16.1.0): "Study of Enablers for Network Automation for 5G (Release 16)".

[i.60] ETSI TS 123 501 (V15.4.0): "5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.4.0 Release 15)".

[i.61] ETSI TS 123 503 (V15.4.0): "5G; Policy and Charging Control Framework for the 5G System; Stage 2 (3GPP TS 23.503 version 15.4.0 Release 15)".

[i.62] 3GPP TR 23.742 (V1.1.0): "Study on Enhancements to the Service-Based Architecture (Release 16)".

[i.63] ETSI TS 128 521 (V15.0.0): "LTE; Telecommunication management; Performance Management (PM) for mobile networks that include virtualized network functions; Procedures (3GPP TS 28.521 version 15.0.0 Release 15)".

[i.64] ETSI TS 128 550 (V15.0.0): "5G; Management and orchestration; Performance assurance (3GPP TS 28.550 version 15.0.0 Release 15)".

[i.65] ETSI TS 128 552 (V16.6.0): "5G; Management and orchestration; 5G performance measurements (3GPP TS 28.552 version 16.6.0 Release 16)".

[i.66] ETSI TS 128 554 (V15.1.0): "5G; Management and orchestration; 5G end to end Key Performance Indicators (KPI) (3GPP TS 28.554 version 15.1.0 Release 15)".

[i.67] ETSI TS 128 515 (V15.0.0): "LTE; Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Requirements (3GPP TS 28.515 version 15.0.0 Release 15)".

[i.68] ETSI TS 128 516 (V15.0.0): "LTE; Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Procedures (3GPP TS 28.516 version 15.0.0 Release 15)".

[i.69] ETSI TS 128 517 (V15.0.0): "LTE; Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Stage 2 (3GPP TS 28.517 version 15.0.0 Release 15)".

[i.70] ETSI TS 128 518 (V15.0.0): "LTE; Telecommunication management; Fault Management (FM) for mobile networks that include virtualized network functions; Stage 3 (3GPP TS 28.518 version 15.0.0 Release 15)".

[i.71] ETSI TS 128 545 (V15.1.0): "5G; Management and orchestration; Fault Supervision (FS) (3GPP TS 28.545 version 15.1.0 Release 15)".

[i.72] ETSI TS 128 510 (V15.0.0): "LTE; Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Requirements (3GPP TS 28.510 version 15.0.0 Release 15)".

[i.73] ETSI TS 128 511 (V15.0.0): "LTE; Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Procedures (3GPP TS 28.511 version 15.0.0 Release 15)".

[i.74] ETSI TS 128 512 (V15.0.0): "LTE; Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Stage 2 (3GPP TS 28.512 version 15.0.0 Release 15)".

[i.75] ETSI TS 128 513 (V15.0.0): "LTE; Telecommunication management; Configuration Management (CM) for mobile networks that include virtualized network functions; Stage 3 (3GPP TS 28.513 version 15.0.0 Release 15)".

[i.76] ETSI TS 128 311: "5G; LTE; Management and orchestration; Network policy management for mobile networks based on Network Function Virtualization (NFV) scenarios (3GPP TS 28.311)".

[i.77] 3GPP TR 32.871 (V15.0.0): "Study on policy management for mobile networks based on Network Function Virtualization (NFV) scenarios (Release 15)".

[i.78] 3GPP TR 28.812 (V0.1.0): "Telecommunication management; Study on scenarios for Intent driven management services for mobile networks (Release 16)".

[i.79] 3GPP TR 28.861 (V0.1.0): "Telecommunication management; Study on the Self-Organizing Networks (SON) for 5G networks (Release 16)".

[i.80] ETSI TS 128 530 (V15.1.0): "5G; Management and orchestration; Concepts, use cases and requirements (3GPP TS 28.530 version 15.1.0 Release 15)".

[i.81] ETSI TS 128 531 (V16.6.0): "5G; Management and orchestration; Provisioning (3GPP TS 28.531 version 16.6.0 Release 16)".

[i.82] ETSI TS 128 532 (V15.1.0): "5G; Management and orchestration; Generic management services (3GPP TS 28.532 version 15.1.0 Release 15)".

[i.83] ETSI TS 128 533 (V15.0.0): "5G; Management and orchestration;Architecture framework (3GPP TS 28.533 version 15.0.0 Release 15)".

[i.84] ETSI TS 128 540 (V15.1.0): "5G; Management and orchestration; 5G Network Resource Model (NRM); Stage 1 (3GPP TS 28.540 version 15.1.0 Release 15)".

[i.85] ETSI TS 128 541 (V15.1.0): "5G; Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3 (3GPP TS 28.541 version 15.1.0 Release 15)".

[i.86] 3GPP TR 28.801 (V15.1.0): "Telecommunication management; Study on management and orchestration of network slicing for next generation network (Release 15)".

[i.87] CORD®.

NOTE: Available at https://www.opennetworking.org/cord/.

[i.88] R-CORD.

NOTE: Available at https://www.opennetworking.org/r-cord/.

[i.89] M-CORD.

NOTE: Available at https://www.opennetworking.org/m-cord/.

[i.90] E-CORD.

NOTE: Available at https://www.opennetworking.org/e-cord/.

[i.91] ONF TR-512: "CoreModel".

NOTE: Available at https://www.opennetworking.org/wp-content/uploads/2018/12/TR-512_v1.4_OnfCoreIm-info.zip.

[i.92] ONF TR-514: "UML".

NOTE: Available at https://www.opennetworking.org/wp-content/uploads/2018/08/TR-514_UML_Modeling_Guidelines_v1.3-1-1.pdf.

[i.93] ONF TR-515: "Papyrus".

NOTE: Available at https://www.opennetworking.org/wp-content/uploads/2018/08/TR-515_Papyrus_Guidelines_v1.3-1-1.pdf.

[i.94] ONF TR-513: "CIM".

NOTE: Available at https://www.opennetworking.org/wp-content/uploads/2014/10/TR-513_CIM_Overview_1.2.pdf

[i.95] ONF TR-523: "Intent".

NOTE: Available at https://www.opennetworking.org/wp-content/uploads/2014/10/TR-523_Intent_Definition_Principles.pdf.

[i.96] FG-ML5G ToR.

NOTE: Available at https://www.itu.int/en/ITU-T/focusgroups/ml5g/Documents/FG-ML5G_ToRs.docx.

[i.97] Recommendation ITU-T Y.Sup55: "ITU-T Y.3170-series - Machine learning in future networks including 5G IMT-2020: Use cases".

[i.98] Recommendation ITU-T Y.3172: "Architectural framework for machine learning in future networks including IMT-2020".

NOTE: Available athttps://www.itu.int/rec/T-REC-Y.3172-201906-I/en.

[i.99] Recommendation ITU-T Y.3173: "Framework for evaluating intelligence levels of future networks including IMT-2020".

NOTE: Available at https://www.itu.int/rec/T-REC-Y.3173/en.

[i.100] Recommendation ITU-T Y.3174: "Framework for data handling to enable machine learning in future networks including IMT-2020".

NOTE: Available at https://www.itu.int/rec/T-REC-Y.3174/en.

[i.101] Recommendation ITU-T Y.3176/ITU-T Y.ML-IMT2020-MP: "ML marketplace integration in future networks including IMT-2020".

[i.102] ANIMA WG.

NOTE: Available at https://datatracker.ietf.org/wg/anima/about/.

[i.103] NETCONF WG.

NOTE: Available at https://datatracker.ietf.org/group/netconf/about/.

[i.104] NETMOD WG.

NOTE: Available at https://datatracker.ietf.org/wg/netmod/about/.

[i.105] OPSAWG WG.

NOTE: Available at https://datatracker.ietf.org/wg/opsawg/about/.

[i.106] L2SM WG.

NOTE: Available at https://datatracker.ietf.org/wg/l2sm/about/.

[i.107] ALTO WG.

NOTE: Available at https://datatracker.ietf.org/wg/alto/about/.

[i.108] HOMENET WG (more remote but still relevant).

NOTE: Available at https://datatracker.ietf.org/wg/homenet/about/.

[i.109] NMRG.

NOTE: Available at https://datatracker.ietf.org/rg/nmrg/about/.

[i.110] IETF RFC 8993: "A Reference Model for Autonomic Networking".

NOTE: Available at https://datatracker.ietf.org/doc/rfc8993/.

[i.111] IETF RFC 8994: "An Autonomic Control Plane (ACP)".

NOTE: Available at https://datatracker.ietf.org/doc/rfc8994/.

[i.112] IETF RFC 8995: "Bootstrapping Remote Secure Key Infrastructures (BRSKI)".

NOTE: Available at https://datatracker.ietf.org/doc/rfc8995.

[i.113] draft-ietf-anima-constrained-voucher-15: "Constrained Bootstrapping Remote Secure Key Infrastructure (BRSKI)".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-anima-constrained-voucher/.

[i.114] IETF RFC 8990: "A Generic Autonomic Signaling Protocol (GRASP)".

NOTE: Available at https://datatracker.ietf.org/doc/rfc8990.

[i.115] IETF RFC 8991: "Generic Autonomic Signaling Protocol Application Program Interface (GRASP API)".

NOTE: Available at https://datatracker.ietf.org/doc/RFC8991.

[i.116] IETF RFC 6241: "NETCONF Protocol".

NOTE: Available at https://www.rfc-editor.org/rfc/rfc6241.txt.

[i.117] IETF RFC 8040: "RESTCONF Protocol".

NOTE: Available at https://www.rfc-editor.org/rfc/rfc8040.txt.

[i.118] IETF RFC 8526: "NETCONF Extensions to Support the Network Management Datastore Architecture".

NOTE: Available at https://datatracker.ietf.org/doc/RFC8526.

[i.119] IETF RFC 8527: "RESTCONF Extensions to Support the Network Management Datastore Architecture".

NOTE: Available at https://datatracker.ietf.org/doc/RFC8527.

[i.120] IETF RFC 8342: "Network Management Datastore Architecture (NMDA)".

NOTE: Available at https://www.rfc-editor.org/info/rfc8342.

[i.121] IETF RFC 8640: "Dynamic Subscription to YANG Events and Datastores over NETCONF".

NOTE: Available at https://www.rfc-editor.org/info/rfc8640.

[i.122] draft-ietf-netconf-notification-capabilities-00: "YangPush Notification Capabilities".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-netconf-notification-capabilities/.

[i.123] draft-ietf-netconf-notification-messages-04: "Notification Message Headers and Bundles".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-netconf-notification-messages/.

[i.124] IETF RFC 8650: "Dynamic Subscription to YANG Events and Datastores over RESTCONF".

NOTE: Available at https://datatracker.ietf.org/doc/rfc8650.

[i.125] IETF RFC 8639: "Subscription to YANG Notifications".

NOTE: Available at https://datatracker.ietf.org/doc/RFC8639.

[i.126] IETF RFC 5277: "NETCONF Event Notifications".

NOTE: Available at https://datatracker.ietf.org/doc/rfc5277/.

[i.127] IETF RFC 6470: "Network Configuration Protocol (NETCONF) Base Notifications".

NOTE: Available at https://datatracker.ietf.org/doc/rfc6470/.

[i.128] draft-bryskin-netconf-automation-yang-02: "Generalized Network Control Automation YANG Model".

NOTE: Available at https://datatracker.ietf.org/doc/draft-bryskin-netconf-automation-yang/?include_text=1.

[i.129] IETF RFC 7950: "The YANG 1.1 Data Modeling Language".

NOTE: Available at http://www.rfc-editor.org/info/rfc7950.

[i.130] draft-ietf-netmod-syslog-model-26: "A YANG Data Model for Syslog Configuration".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-netmod-syslog-model/.

[i.131] IETF RFC 6020: "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)".

[i.132] IETF RFC 6244: "An Architecture for Network Management Using NETCONF and YANG".

NOTE: Available at https://datatracker.ietf.org/doc/rfc6244/.

[i.133] IETF RFC 8343: "A YANG Data Model for Interface Management".

NOTE: Available at https://www.rfc-editor.org/rfc/rfc8343.txt.

[i.134] IETF RFC 7317: "A YANG Data Model for System Management".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7317/.

[i.135] IETF RFC 7407: "A YANG Data Model for SNMP Configuration".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7407/.

[i.136] draft-wwx-netmod-event-yang-00: "A YANG Data model for ECA Policy Management".

NOTE: Available at https://datatracker.ietf.org/doc/draft-wwx-netmod-event-yang/.

[i.137] draft-wu-netmod-base-notification-nmda-00: "NMDA Base Notification for Intent based configuration update".

NOTE: Available at https://datatracker.ietf.org/doc/draft-wu-netmod-base-notification-nmda/.

[i.138] IETF RFC 7788: "Home Networking Control Protocol".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7788/.

[i.139] IETF RFC 7368: "IPv6 Home Networking Architecture Principles".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7368/.

[i.140] draft-ietf-homenet-simple-naming-03: "Homenet Naming and Service Discovery Architecture".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-homenet-simple-naming/.

[i.141] IETF RFC 5345: "Simple Network Management Protocol (SNMP) Traffic Measurements and Trace Exchange Formats".

NOTE: Available at https://datatracker.ietf.org/doc/rfc5345/.

[i.142] IETF RFC 8316: "Autonomic Networking Use Case for Distributed Detection of Service Level Agreement (SLA) Violations".

NOTE: Available at https://datatracker.ietf.org/doc/rfc8316/.

[i.143] IETF RFC 7575: "Autonomic Networking: Definitions and Design Goals".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7575/.

[i.144] IETF RFC 7576: "General Gap Analysis for Autonomic Networking".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7576/.

[i.145] draft-irtf-nmrg-ibn-concepts-definitions-06: " Intent-Based Networking - Concepts and Overview".

NOTE: Available at https://datatracker.ietf.org/doc/draft-irtf-nmrg-ibn-concepts-definitions/.

[i.146] draft-homma-nmrg-slice-gateway-00: "Gateway Function for Network Slicing".

NOTE: Available at https://datatracker.ietf.org/doc/draft-homma-nmrg-slice-gateway/.

[i.147] draft-kim-nmrg-rl-05: "Intelligent Reinforcement-Learning-based Network Management".

NOTE: Available at https://datatracker.ietf.org/doc/draft-kim-nmrg-rl/.

[i.148] IETF RFC 5674: "Alarms in Syslog".

NOTE: Available at https://datatracker.ietf.org/doc/rfc5674/.

[i.149] IETF RFC 5675: "Mapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages".

NOTE: Available at https://datatracker.ietf.org/doc/rfc5675/.

[i.150] IETF RFC 5676: "Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications".

NOTE: Available at https://datatracker.ietf.org/doc/rfc5676/.

[i.151] IETF RFC 7276: "An Overview of Operations, Administration, and Maintenance (OAM) Tools".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7276/.

[i.152] draft-jilongwang-opsawg-nrc-00: "Framework for Network Resources Categorization".

NOTE: Available at https://datatracker.ietf.org/doc/draft-jilongwang-opsawg-nrc/.

[i.153] draft-sun-opsawg-sdwan-service-model-01: "A YANG Data Model for SD-WAN Service Delivery".

NOTE: Available at https://datatracker.ietf.org/doc/draft-sun-opsawg-sdwan-service-model/.

[i.154] IETF RFC 8466: "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery".

NOTE: Available at https://datatracker.ietf.org/doc/rfc8466/.

[i.155] IETF RFC 5693: "Application-Layer Traffic Optimization (ALTO) Problem Statement".

NOTE: Available at https://datatracker.ietf.org/doc/rfc5693/.

[i.156] IETF RFC 6708: "Application-Layer Traffic Optimization (ALTO) Requirements".

NOTE: Available at https://datatracker.ietf.org/doc/rfc6708/.

[i.157] IETF RFC 7285: "Application-Layer Traffic Optimization (ALTO) Protocol".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7285/.

[i.158] IETF RFC 7286: "Application-Layer Traffic Optimization (ALTO) Server Discovery".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7286/.

[i.159] IETF RFC 7971: "Application-Layer Traffic Optimization (ALTO) Deployment Considerations".

NOTE: Available at https://datatracker.ietf.org/doc/rfc7971/.

[i.160] draft-ietf-alto-xdom-disc-04: "Application Layer Traffic Optimization (ALTO) Cross-Domain Server Discovery".

NOTE: Available at https://datatracker.ietf.org/doc/draft-ietf-alto-xdom-disc/.

[i.161] draft-irtf-nmrg-intent-classification-01: "Intent Classification".

NOTE: Available at https://datatracker.ietf.org/doc/draft-irtf-nmrg-ibn-intent-classification/.

[i.162] draft-du-anima-an-intent-05: "ANIMA Intent Policy and Format".

NOTE: Available at https://datatracker.ietf.org/doc/draft-du-anima-an-intent/.

[i.163] draft-liu-anima-intent-distribution-00: "Intent Distribution for Autonomic Networking".

NOTE: Available at https://datatracker.ietf.org/doc/draft-liu-anima-intent-distribution/.

[i.164] draft-moulchan-nmrg-network-intent-concepts-00: "Concepts of Network Intent".

NOTE: Available at https://datatracker.ietf.org/doc/draft-moulchan-nmrg-network-intent-concepts/.

[i.165] draft-bernardos-nmrg-multidomain-00: "Multi-domain Network Virtualization".

NOTE: Available at https://datatracker.ietf.org/doc/draft-bernardos-nmrg-multidomain/.

[i.166] GSMA™: "Network Slicing Use Case Requirements, April 2018".

NOTE: Available at https://www.gsma.com/futurenetworks/wp-content/uploads/2018/03/Network-Slicing-Use-Cases-Requirements-Wrapper.pdf.

[i.167] GSMA: "Generic Network Slice Template Version 1.0".

NOTE: Available at https://www.gsma.com/newsroom/wp-content/uploads/NG.116-v1.0-4.pdf.

[i.168] BBF SD-406: "End-to-End Network Slicing".

[i.169] BBF SD-407: "5G Fixed Mobile Convergence Study".

[i.170] OASIS: "AMQPv1.0".

NOTE: Available at https://www.oasis-open.org/standards#amqpv1.0.

[i.171] OASIS: "CAMPv1.2".

NOTE: Available at http://docs.oasis-open.org/camp/camp-spec/v1.2/camp-spec-v1.2.pdf.

[i.172] OASIS: "MQTTv3.1.1".

NOTE: Available at http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html.

[i.173] OASIS: "ODATAv4.01".

NOTE: Available at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=odata.

[i.174] OASIS: "TOSCAv1.0".

NOTE: Available at http://docs.oasis-open.org/tosca/TOSCA/v1.0/os/TOSCA-v1.0-os.html.

[i.175] OASIS: "TOSCA-YAMLv1.2".

NOTE: Available at http://docs.oasis-open.org/tosca/TOSCA-Simple-Profile-YAML/v1.2/cs01/TOSCA-Simple-Profile-YAML-v1.2-cs01.pdf.

[i.176] OSM Release Five.

NOTE: Available at https://osm.etsi.org/wikipub/index.php/OSM_Release_FIVE_Documentation.

[i.177] OPNFV® Platform overview.

[i.178] OPNFV Hunter 8.1.

NOTE: Available at https://www.opnfv.org/software/downloads/release-archives/hunter-8-1.

[i.179] OPNFV Pharos Project.

NOTE: Available at https://www.opnfv.org/community/projects/pharos.

[i.180] Openstack® Rocky Release.

NOTE: Available at https://www.openstack.org/software/rocky/.

[i.181] OpenStack® Services.

NOTE 1: Available at https://www.openstack.org/software/project-navigator/openstack-components#openstack-services.

NOTE 2: OpenStack® is a registered trademark of the OpenStack Foundation and is used with the OpenStack Foundation's permission. ETSI in not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

[i.182] ONAP®.

NOTE: Available at https://www.onap.org/wp-content/uploads/sites/20/2018/11/ONAP_CaseSolution_Architecture_112918FNL.pdf.

[i.183] ETSI GR ENI 007: "Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks".

[i.184] ETSI GR ENI 008: "Experiential Networked Intelligence (ENI); InTent Aware Network Autonomicity (ITANA)".

[i.185] LSO Reference Points.

NOTE: Available at https://wiki.mef.net/pages/viewpage.action?pageId=53154082.

[i.186] LSO Capabilities.

NOTE: Available at https://wiki.mef.net/display/CESG/LSO+Reference+Architecture+and+Capabilities.

[i.187] ETSI GS ZSM 002: "Zero-touch network and Service Management (ZSM); Reference Architecture".

[i.188] k8s (Kubernetes).

NOTE: Available at https://kubernetes.io/.

[i.189] TRex.

NOTE: Available at https://trex-tgn.cisco.com/.

[i.190] CLAMP in ONAP Architecture.

NOTE: Available at https://docs.onap.org/projects/onap-clamp/en/latest/.

[i.191] Edge Automation through ONAP.

NOTE: Available at https://wiki.onap.org/display/DW/Edge+Automation+through+ONAP.

[i.192] Edge Architecture & Work Items.

NOTE: Available at https://wiki.onap.org/pages/viewpage.action?pageId=28381325.

[i.193] DCAE.

NOTE: Available at https://wiki.onap.org/pages/viewpage.action?pageId=1015831.

[i.194] DCAE APIs.

NOTE: Available at https://wiki.onap.org/pages/viewpage.action?pageId=84642215.

[i.195] ML5G-O-034: "Gap Analysis: next steps in integrating machine learning in future networks including IMT-2020".

[i.196] ML5G-O-035 / ML5G-I-232-R2: "Machine Learning Sandbox for future networks including IMT-2020: requirements and architecture framework".

[i.197] ML5G-O-036 / ML5G-I-227-R2: "Serving framework for ML models in future networks including IMT-2020".

[i.198] ML5G-O-037 / ML5G-I-247: "Machine learning based end-to-end network slice management and orchestration".

[i.199] ML5G-O-038 / ML5G-I-248: "Requirements, architecture, and design for machine learning function orchestrator".

[i.200] ML5G-O-039 / ML5G-I-242-R1: "Vertical-assisted Network Slicing Based on a Cognitive Framework".

[i.201] GSMA White Paper: "An Introduction to Network Slicing", 2017.

NOTE: Available at https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf.

[i.202] ETSI GS ZSM 009-1: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 1: Enablers".

[i.203] ETSI GR F5G 001: "Fifth Generation Fixed Network (F5G); F5G Generation Definition Release #1".

[i.204] ETSI GS F5G 005: "F5G high-quality service experience factors F5G high-quality service experience factors".

[i.205] ETSI GR SAI 001: "Securing Artificial Intelligence (SAI); AI Threat Ontology".

[i.206] ETSI GR SAI 002: "Securing Artificial Intelligence (SAI); Data Supply Chain Security".

[i.207] ETSI GR SAI 004: "Securing Artificial Intelligence (SAI); Problem Statement".

[i.208] ETSI GR SAI 005: "Securing Artificial Intelligence (SAI); Mitigation Strategy Report".

[i.209] AN WP: "Autonomous Networks: Empowering Digital Transformation For Telecoms Industry".

[i.210] IG1193: "Cross-Industry Autonomous Networks - Vision and Roadmap".

[i.211] IG1218: "Autonomous Networks Business Requirements & Architecture".

[i.212] IG1230: "Autonomous Networks Technical Architecture".

[i.213] IG1190: "AIOps Service Management".

[i.214] IG1190A: "AIOps Configuration Management".

[i.215] IG1190B: "AIOps Change Management".

[i.216] IG1190C: "AIOps Release Management".

[i.217] IG1190D: "AIOps Acceptance Testing".

[i.218] IG1190E: "AIOps Knowledge Management".

[i.219] IG1190F: "AIOps Monitoring and Event Management".

[i.220] IG1190G: "AIOps Incident Management".

[i.221] IG1190H: "AIOps Problem Management".

[i.222] GB1021: "AI & DA Management Standards Guidebook: AI Checklists".

[i.223] IG1180: "AI Data Training Repository".

[i.224] IG1184: "Service Management Standards for AI".

[i.225] IG1232: "AI Model Data Sheet Specification".

[i.226] TMF915: "AI Management API Component Suite User Guide".

[i.227] TMF915A: "AI Management Component Suite Profile".

[i.228] TMF915B: "AI Management API Conformance Profile".

[i.229] DSP0266: "Redfish Specification".

[i.230] DSP0263: "Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol".

[i.231] DSP0243: "Open Virtualization Format Specification".

[i.232] DSP0262: "Cloud Auditing Data Federation (CADF) - 5 Data Format and Interface Definitions Specification".

[i.233] IG1219: "AI Closed Loop Automation Anomaly Detection and Resolution".

[i.234] TR284: "AI Closed Loop Automation Reference Architecture".

[i.235] 5G-VINNI deliverable D3.1: "Specification of services delivered by each of the 5G-VINNI facilities", July 2019.

NOTE: Available at https://zenodo.org/record/3345612#.YIfyqy2w1TY.

[i.236] Openslice official documentation.

NOTE: Available at http://openslice.io/.

[i.237] ZSM PoC#2 showcase.

NOTE: Available at https://www.etsi.org/events/1905-webinar-zsm-poc-2-showcase-automated-network-slice-scaling-in-multi-site-environments.

[i.238] FG-AN website.

NOTE: Available at https://www.itu.int/en/ITU-T/focusgroups/an/Pages/default.aspx.

[i.239] FG-AN ToR.

NOTE: Available at https://www.itu.int/en/ITU-T/focusgroups/an/Documents/FG-AN_Terms_of_Reference.pdf?csf=1&e=dRZrwa.

[i.240] TMF634: "Resource Catalog Management API".

[i.241] TMF909: "Network as a Service (Naas) Management REST API Specification".

NOTE: Available at https://projects.tmforum.org/wiki/download/attachments/134777012/TMF909%20_API_Suite_Specification_for_NaaS_v3.pdf?api=v2.

[i.242] TMF642: "Alarm Management API".

[i.243] TMF653: "Service Test Management API".

[i.244] ENI Vision: "Improved Network Experience using Experiential Networked Intelligence".

NOTE: Available at https://www.etsi.org/images/files/ETSIWhitePapers/etsi-wp44_ENI_Vision.pdf.

[i.245] ETSI GS ZSM 008: "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management".

[i.246] ETSI GS ZSM 003 (V1.1.1): "Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing".

[i.247] ETSI GS ZSM 009-2: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 2: Solutions for automation of E2E service and network management use cases".

[i.248] ETSI GR ZSM 009-3: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 3: Advanced topics".

[i.249] ETSI GR ZSM 011: "Zero-touch network and Service Management (ZSM); Intent-driven autonomous networks; Generic aspects".

[i.250] ETSI GS ZSM 012: "Zero-touch network and Service Management (ZSM); Enablers for Artificial Intelligence-based Network and Service Automation".

[i.251] ETSI GR ZSM 013: "Zero-touch network and Service Management (ZSM); Automation of CI/CD for ZSM services and managed services".

[i.252] TMF632: "Party Management API REST Specification R19.0.1".

NOTE: Available at https://www.tmforum.org/resources/specification/tmf632-party-management-api-rest-specification-r19-0-0/#.

[i.253] TMF628: "Performance Management API REST Specification R14.5.1".

NOTE: Available at https://www.tmforum.org/resources/interface/tmf628-performance-management-api-rest-specification-r14-5-0/#.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS ZSM 007 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ZSM 007 [i.1] and the following apply:

AI	Artificial Intelligence
BBF	BroadBand Forum
CDS	Common Data Services
CI/CD	Continuous Integration and Continuous Delivery
CORD	Central Office Re-architected as a Datacentre
CP	Cloud Provider
DNS	Domain Name System
ENI	Experiential Network Intelligence
GR	Group Report
IT	Information Technology
LSO	Lifecycle Services Orchestration
MAMS	Multiple Access Management Services
MANO	Management and Orchestration
MEC	Multi-access Edge Computing
MEF	Metro Ethernet Forum
NFV	Network Functions Virtualisation
NFVI	Network Functions Virtualisation Infrastructure
NFVO	Network Functions Virtualisation Orchestrator
NS	Network Service
NSI	Network Service Instance
NWDAF	NetWork Data Analytics Function
OASIS	Organization for the Advancement of Structured Information Standards
ONAP	Open Network Automation Platform
ONF	Open Networking Foundation
OPNFV	Open Platform for NFV
OSC	Open Source Community
OSM	Open Source MANO
OSS	Operations Support System
QoE	Quality of Experience
QOS	Quality of Service
SDN	Software Defined Network
SDO	Standards Developing Organization
SLA	Service Level Agreement
SON	Self-Organization Network

SP	Service Provider
TCP	Transmission Control Protocol
UE	User Equipment
VIM	Virtualised Infrastructure Manager
VNF	Virtualised Network Function
VNFFG	VNF Forwarding Graph
VNFM	VNF Manager
WAN	Wide Area Network
WIM	WAN Infrastructure Manager
WLAN	Wireless Local Area Network
ZSM	Zero-touch network and Service Management

4 Void

5 Landscape of ZSM Related Standards Developing Organizations (SDOs)

5.1 Introduction

Clause 5 identifies work done in other Standards Developing Organizations (SDOs) in industry that may be relevant to the work in ZSM.

5.2 ETSI ISG NFV

5.2.1 Use Cases and Requirements relevant to ZSM in ISG NFV

Network Functions Virtualisation (NFV) aims to transform the way that network operators architect networks by evolving standard IT virtualisation technology to consolidate fixed and mobile network equipments onto industry standard high volume servers, switches and storage, which could be located in a variety of NFVI-PoPs including datacentres, network nodes and in end user premises.

The use cases and the derived requirements on NFV are specified in ETSI GR NFV 001 [i.3] and ETSI GS NFV 004 [i.4].

As described in ETSI GR NFV 001 [i.3], the service models and use cases that are relevant to ZSM include:

- Use Case #1: Network Function Virtualisation Infrastructure as a Service (NFVIaaS).
  In this use case, it is desired that a Service Provider can provide the ability to offer its NFV Infrastructure as a service to other Service Providers in addition to existing catalogue of network services. The other Service Providers use the ability to remotely deploy and run virtualised network functions inside the NFV Infrastructure provided as a service by the Service Provider.
  The requirements that are relevant to ZSM in this use case include network service performance objectives (e.g. latency, reliability), remotely deploy and run VNFs inside an NFV Infrastructure, offer network connectivity services, service abstraction, service resiliency, failure notification and diagnostics, failure recovery, and SLA management.

- Use Case #2: VNF Forwarding Graphs.
  In this use case, the VNF Forwarding Graph (VNFFG) may be used by a Service Provider at an abstract level for its network service design. VNFFG is a template which describes the interconnection (forwarding) topology along with related management and dependency relationships between VNFs inside a network service. Compared with Physical Appliance Forwarding Graph, VNFFG provides more efficient, resilient, flexible way to deploy network services and help to reduce complexity.
  The requirements that are relevant to ZSM in this use case include connectivity related information models, monitoring, resiliency, performance management, testing, and e2e services across administrative boundaries.

- Use Case #9: Network Slicing.
  Network slicing is commonly described as a logical instantiation of the network between a set of network devices and some back end applications to deliver services for users or a set of users. The automation of the lifecycle management of a network slice is required to shorten time to deploy new slices and provides closed loop monitoring and self-healing to meet SLA.
  The requirements that are relevant to ZSM in this use case include allocating resources to a slice dynamically, scaling automatically, self-healing, deploying a slice automatically, providing network and Services management capabilities, etc.

- Use Case #10: Virtualisation of Internet of Things (IoT).
  In this use case, it demonstrates the fact that different IoT use case scenarios may require different combinations of network functions (such as control, connectivity, applications, authentication, analytics engine, gateway, vCPE, storage). Since different IoT services may have significant variation in their requirements and/or how they are configured. It is required that the realization of IoT network topologies, the creation of functions at optimal locations, independent scaling of different functions composing an IoT service to be implemented automatically and without manual intervention.
  The requirements that are relevant to ZSM in this use case include network slicing provisioning, massive data analytics, widely varying requirements on processing complexity, storage, QoS, signalling priority, latency, bandwidth, availability, and permissible geographic areas.

- Use Case #12: Devops/CI/CD, Use Case #13: A/B testing.
  In this use case, the software development and upgrade processes for a network service permit rapid service innovation through software-based development, testing and deployment/operationalization to implement the business objective of NFV.

- Use Case #14: VNF composition across multiple administrative domains.
  This use case specifies proper ways of composing services across multiple administrative domains in a dynamic manner.
  The requirements that are relevant to ZSM in this use case include Multi-Domain Orchestrator (similar to the end-to-end service management in ZSM), various domain orchestrators, and connectivity over multiple domains, etc.

NOTE: The derived requirements from the use cases on NFV in ETSI GS NFV 004 [i.4] address following areas, such as network service related portability/interoperability, performance, management and orchestration, operations, migration, assurance, elasticity, resiliency, stability, energy efficiency, service continuity, security/regulatory. The fulfilment of those requirements can help to implement the automation of end-to-end network services management in ZSM.

5.2.2 Architecture Framework relevant to ZSM in ISG NFV

Figure 5.2.2-1 describes the high-level functional architectural framework of NFV as specified in ETSI GS NFV 002 [i.5] and ETSI GS NFV-MAN 001 [i.6].

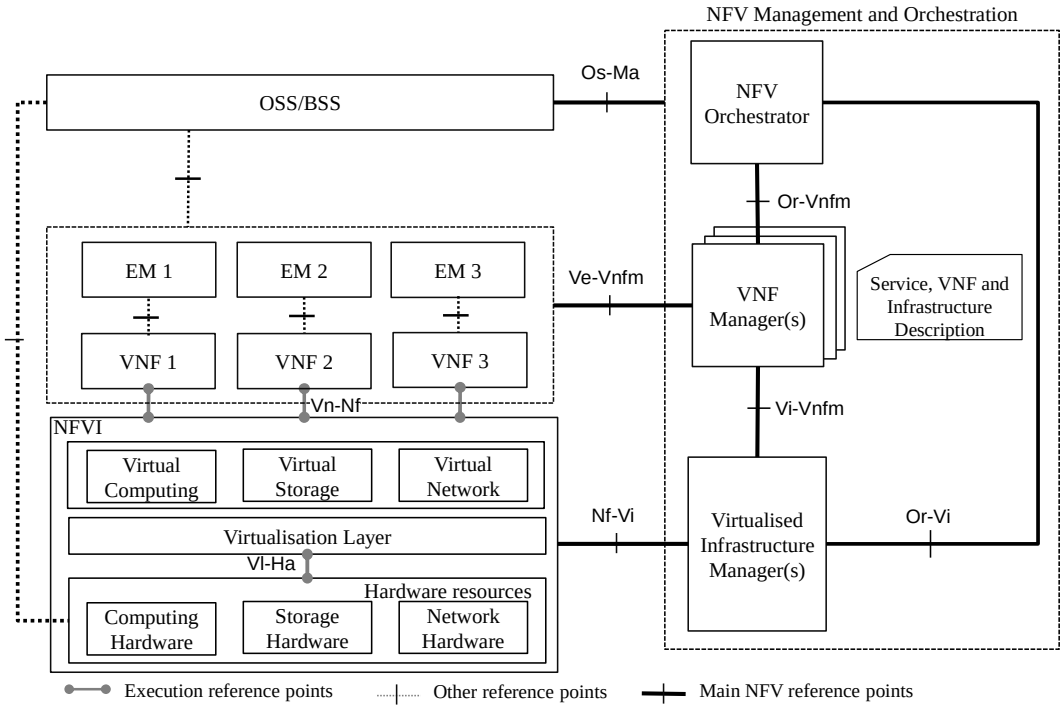


Figure 5.2.2-1: NFV reference architectural framework
(source: from ETSI GS NFV 002 [i.5])

The following shows the Functional Blocks which are relevant to ZSM for end-to-end network service management:

- **NFV Orchestrator (NFVO):** in charge of the orchestration and management of NFV infrastructure and software resources, and realizing network services on NFVI.
- **VNF Manager (VNFM):** responsible for the lifecycle management of VNF instances.
- **Virtualised Infrastructure Manager (VIM):** responsible for controlling and managing the NFVI compute, storage and network resources, usually within one operator's Infrastructure Domain.
- **NFV Infrastructure (NFVI):** the totality of all hardware and software components which build up the environment in which VNFs are deployed, managed and executed.

NOTE: A NFV reference architecture can be leveraged by ZSM to implement the management of end-to-end network service or be as a management domain to deploy part of the end-to-end network service.

5.2.3 Interfaces, Information Models, and Templates relevant to ZSM in ISG NFV

As specified in ETSI GS NFV-IFA 013 [i.7] and ETSI GS NFV-SOL 005 [i.18], the Interfaces and Information Models related to Os-Ma-Nfvo reference point exposed by NFVO to support the management of Network Service descriptor, Network Service lifecycle, fault, performance, policy, VNF package, and multi-site, etc. The Performance Measurements is further described in ETSI GS NFV-IFA 027 [i.13]. The Policy Management is further described in ETSI GR NFV-IFA 023 [i.10]. The VNF package management is further specified in ETSI GS NFV-IFA 011 [i.9]. The multi-site is further described in ETSI GR NFV-IFA 022 [i.16].

As specified in ETSI GS NFV-IFA 014 [i.8], the Network Service Template describes the meta-data information that can be used by the NFVO for NS deployment and lifecycle management.

As specified in ETSI GS NFV-IFA 011 [i.9] and ETSI GS NFV-SOL 004 [i.17], the VNF Descriptor and Packaging focus on the holistic end-to-end view of the VNF Package lifecycle, from design to runtime.

As specified in ETSI GR NFV-IFA 015 [i.11], ETSI GR NFV-IFA 024 [i.12], the approach of federating NFV Information Model with other external models is proposed with the definition of interaction points between the NFV Information Model and some models from other organizations, allowing all organizations to extend their model based on the interaction points as they see needed.

As specified in ETSI GR NFV-IFA 021 [i.14] and in ETSI GS NFV-IFA 031 [i.15], the requirement, framework, interfaces and the necessary information elements on the management and deployment of NFV-MANO functions are described to enable their fault, configuration and information, performance, state and log management.

As specified in ETSI GR NFV-IFA 028 [i.19], it provides a report on potential architecture options to support the offering of NFV-MANO services across multiple administrative domains. The following use cases are analysed in the present document:

1) NFVIaaS;

2) Network Services provided using multiple administrative domains.

As specified in ETSI GS NFV-IFA 030 [i.20], the functional requirements, interfaces and operations to support the provision of network services across multiple administrative domains based on the interactions between NFVOs in different administrative domains (supported over the Or-Or reference point) are provided, and also the information elements exchanged over the specified interfaces.

As specified in ETSI GS NFV-IFA 032 [i.21], the interfaces for management of multi-site connectivity services which are produced by a WAN Infrastructure Manager (WIM) are provided, and also the operations and the information elements that are exchanged over these interfaces.

NOTE 1: Group specifications and group reports identified above in ISG NFV can be leveraged by ZSM to management the end-to-end network services. Further corporation can be performed between ZSM and ISG NFV in implementing customized requirement of network services.

NOTE 2: The interfaces provided by NFV are not serviced-based, whether they can be leveraged by ZSM need further study.

5.3 ETSI ISG MEC

5.3.1 Use Cases and Requirements relevant to ZSM in ISG MEC

The use cases and the derived requirements for Multi-access Edge Computing (MEC) are to promote interoperability and deployments of MEC applications as specified in ETSI GS MEC 002 [i.22].

The MEC use cases that are relevant to ZSM are listed as follows:

- A.2 Mobile video delivery optimization using throughput guidance for TCP.
  In this use case, a radio analytics MEC application, which uses services of Multi-access Edge Computing, provides a suitably equipped backend video server with a near real-time indication on the throughput estimated to be available at the radio downlink interface in the next time instant. The video server can use this information to assist TCP congestion control decisions. With this additional information, TCP does not need to overload the network when probing for available resources, nor does it need to rely on heuristics to reduce its sending rate after a congestion episode.

- A.4 Security, safety, data analytics.
  This use case groups a number of innovative services based on the gathering of huge amounts of data (video, sensor information, etc.) from devices analysed through a certain amount of processing to extract meaningful information before being sent towards central servers.

- A.9 SLA management.
  If an application is instantiated on a MEC host, which has certain performance requirements regarding the virtualisation environment of the host and the allocated virtual resources. These requirements are typically agreed and specified in Service Level Agreements (SLAs). In order to verify how well the SLAs are met, performance data regarding the virtualisation environment of the MEC host has to be collected and made available for further processing.

- A.11 Mobile backhaul optimization.
  The intention in this use case is to combine information from the radio network together with information from the backhaul network to optimize the resources in the backhaul. The analytic application uses services of Multi-access Edge Computing (like traffic monitoring, performance monitoring) to provide real time information about the traffic requirements of the radio network (taking into account the radio access scheduling, the application and backhaul condition). The analytics application gets real time information from a monitoring application within the backhaul, and sends the traffic requirement to an optimization application within the backhaul network.

- A.24 Optimizing QoE and resource utilization in multi-access network.
  In a MEC environment, the overall QoE perceived by the end users as well as utilization of the resources can be optimized with smart selection and combination of the paths used for the user plane. In an advanced solution, the network paths can be dynamically selected based on knowledge of current conditions in the relevant access networks. The ongoing work on Multiple Access Management Services (MAMS) in IETF can be used to manage smart and flexible user plane path selections in multi-access networks.

- A.28 Factories of the Future.
  Several application areas are characterized with automation:

  1) Factory automation deals with the automated control, monitoring and optimization of processes and workflows within a factory. This includes aspects like closed-loop control applications (e.g. based on programmable logic or motion controllers), robotics, as well as aspects of computer-integrated manufacturing.

  2) Monitoring and maintenance particularly includes applications such as condition monitoring and predictive maintenance based on sensor data, but also big data analytics for optimizing future parameter sets of a certain process.

NOTE 1: ZSM can provide radio and data analytics, optimization, and SLA management services to satisfy the above identified MEC use cases.

As captured in ETSI GS MEC 002 [i.22], the requirements can be categorized into following areas:

- General requirements on framework, application lifecycle, application environment, etc.

- Service requirements on Platform essential functionality (such as MEC services, connectivity, storage, traffic routing, etc.), features (such as *User Apps, Smart Relocation, Radio Network Information [i.26], Location Service [i.27], Bandwidth Manager [i.29], and UE Identity [i.28], Fixed Access Information [i.31], WLAN Information [i.30], V2XService [i.32], 5GCoreConnect),* O&M, security, regulation, charging.

NOTE 2: The features provided by MEC can be leveraged by ZSM to deploy an E2E service or part of the E2E service that has such kind of requirements as identified in MEC.

5.3.2 Architecture Framework relevant to ZSM in ISG MEC

As specified in ETSI GS MEC 003 [i.23], the Multi-access edge system reference architecture is depicted in Figure 5.3.2-1.

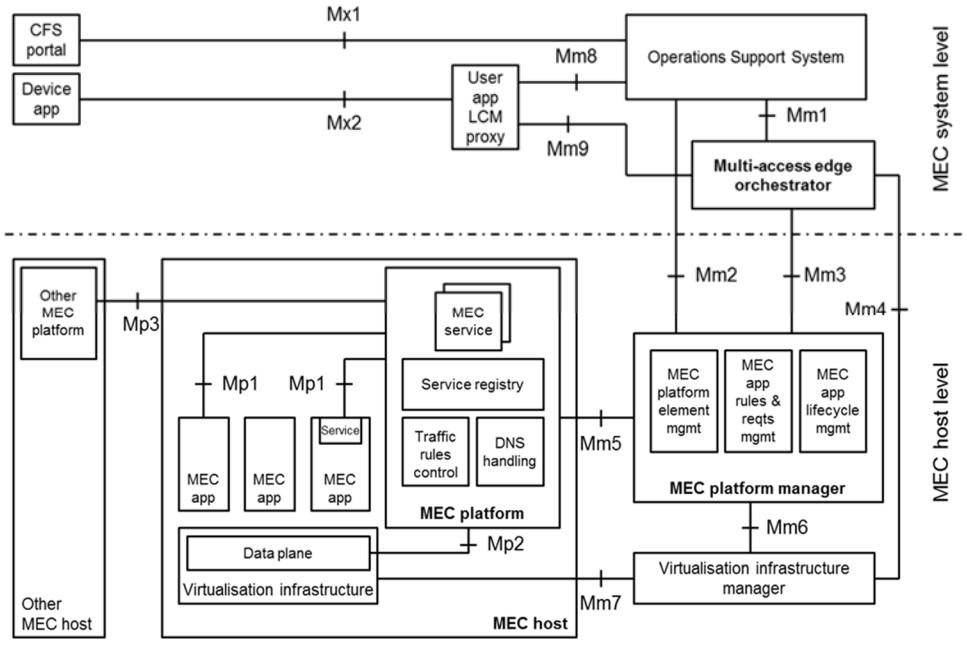


Figure 5.3.2-1: Multi-access edge system reference architecture
(source: from ETSI GS MEC 003 [i.23])

The following shows the MEC Architectural Functional Elements which are relevant to ZSM:

- **MEC host:** an entity that contains the MEC platform and a virtualisation infrastructure which provides compute, storage, and network resources for the MEC applications. The virtualisation infrastructure includes a data plane that executes the traffic rules received by the MEC platform, and routes the traffic among applications, services, DNS server/proxy, 3GPP network, other access networks, local networks and external networks.

- **MEC platform:** responsible for the following functions as offering an environment for MEC applications, receiving traffic rules from the MEC platform manager, applications, or services, receiving DNS records from the MEC platform manager and configuring a DNS proxy/server accordingly, hosting MEC services, and providing access to persistent storage, etc.

- **MEC application:** MEC applications can have a certain number of rules and requirements associated to them, such as required resources, maximum latency, required or useful services, etc.

- **MEC system level management:** such as Multi-access edge orchestrator, Operations Support System (OSS), and user application lifecycle management proxy.

- **MEC host level management:** such as MEC platform manager, and virtualisation infrastructure manager.

- **Customer facing service portal:** allows operators' third-party customers (e.g. commercial enterprises) to select and order a set of MEC applications that meet their particular needs, and to receive back service level information from the provisioned applications.

ETSI GS MEC 010-1 [i.24] defines the management of the mobile edge system, mobile edge hosts and mobile edge platforms. This includes platform configuration, performance and fault management, application monitoring, remote service configuration and service control, information gathering regarding the platform features, available services, and available virtualised resources.

ETSI GS MEC 010-2 [i.25] provides information flows for lifecycle management of applications running on a MEC host, and describes interfaces over the reference points to support application lifecycle management. It also describes application rules and requirements, application-related events and mobility handling.

ISG MEC focuses on the MEC platform with a number of MEC services to satisfy the requirements of deploying MEC applications in a multi-access network, while ISG ZSM focuses on automation techniques, service management, management functions, and full automation.

NOTE: There are no overlapping areas between ISG MEC and ISG ZSM. But the MEC system specified in ISG MEC can be regarded as a management domain that the ISG ZSM can be leveraged to enhance the automation of network and service management. E.g. if the E2E service or part of it is MEC related, ZSM can use the platform functionalities, such as the exposed MEC services to deploy it on a MEC system.

5.4 ETSI ISG ENI

5.4.1 Use Cases and Requirements relevant to ZSM in ISG ENI

The ENI system can be applied to the fixed network, the mobile network, or both, to improve the operator experience and network operation through the use of network intelligence and to cope with the human-machine interaction challenges.

The ENI system automatically collects network status and associated metrics, faults, and errors, and then uses artificial intelligence to ensure network performance and quality of service are met at the highest possible efficiency (e.g. with the minimum required resources). An ENI system can also be used to perform network optimization by finding bottlenecks of service and/or failure of network. Both of these benefits are realized on-demand, in response to changing contextual information.

The ENI use cases and the derived requirements are documented in ETSI GR ENI 001 [i.33] and ETSI GS ENI 002 [i.34].

The ENI use cases that are relevant to ZSM are listed as follows:

- Use Case #2-8: Automatic service and resource design framework for cloud service. With an increasing number of cloud services and functions deployed on the virtualised platform, the Service Providers (SP) are concerned about the service requirements, such as the functionality of the service, the levels of security and reliability, and the ability to handle workloads. The Cloud Provider (CP) needs to know the composition and amount of resources to be allocated when fulfilling the service orders from SP. Therefore, cloud resource composition and amount need to be designed in various phases of cloud service delivery automatically.
  The ENI system is required to support service requirement analysis, resource composition design, and resource amount design for this use case. And with the design result, the resource management and orchestration system is enforced to implement the service request.

- Use Case #3-2: Intelligent network slicing management. With the emergence of dynamic instantiation of NSIs or runtime adaptation of the deployed NSI, the ENI system can be applied to enhance and optimize the network slice management and control operations.
  The ENI system is required to provide slice anomaly analysis and report, producing proper context-aware policy for this use case.

- Use Case #3-3: Intelligent carrier-managed SD-WAN. Through the use of AI and context-awareness, the ENI System can monitor the network and help enterprises to optimize their services and resources, hence allowing enterprises to focus more on their businesses. The ENI System may also use AI methods in order to optimize the service and suggest policies adaptations to Network Administrators.
  The ENI system is required to provide Intent policies management, services/connections monitoring and optimization, policy/configuration generation based on analysis of history data for this use case.

- Use Case #4-1: Network fault identification and prediction. The ENI system provides the capability to proactively identify and forecast status of a device/service that is not performing as expected in order for network operation and maintenance management to be able to repair the service before customer requirements are violated.
  The ENI system is required to provide network information collection, network status monitoring, intelligent analysing and prediction, network performance evaluation, and producing detailed fault report for this use case.

- Use Case #4-2: Assurance of Tight Service Requirements. The ENI system is used to predict or detect requirements change also involving possible competition for the same shared resources as well as to enforce slice prioritization.
  The ENI system is required to provide service abnormal behaviour monitoring, fault prediction, customized SLA management, slice prioritization enforcement, carrier grade assurance for this use case.

- Use Case #4-3: Network fault root-cause analysis and intelligent recovery. Traditional fault maintenance requires manual processing. The cost is high, and the fault locating efficiency is low and the period is long. It is hoped that applying machine learning algorithms in network fault root-cause analysis and intelligent recovery to form a more efficient solution, shorten the time of fault recovery and improve the efficiency of network maintenance.
  The ENI system is required to support data collection and analysis on fault data, fault self-recovery policy, data mining model, decision-making model, and RCA&SIA (Root Cause Analysis & Service Impact Analysis).

- Use Case #5-1: Policy-based network slicing for IoT security. When a DDoS attack happens, the ENI System will be able to detect and learn from the occurrence by using AI methods. If the new traffic pattern is identified as an attack based on past history, the ENI System will be able to trigger appropriate responses from the related management components.
  The ENI system is required to provide service monitoring, abnormity analysis and notification for this use case.

As captured in ETSI GS ENI 002 [i.34], the requirements identified from the above scenarios require intelligence applied to the network to improve operators' experience of service provision and network operation as well as to enable dynamic autonomous behaviour and adaptive policy driven operation in a changing context.

The requirements can be categorized into following areas:

- Service and network requirements on general requirements, service orchestration and management, network planning and deployment, network optimization, resilience and reliability, and security and privacy.

- Functional requirements on data collection and analysis, policy management, data learning, interworking with other systems, and mode of operations.

- Non-functional requirements on performance, operations, regulations, and non-functional policies.

ISG ENI focuses on AI techniques, real-time & near real-time operational control, resource policies (moving from imperative though declarative to intent policies), and closed-loop mechanisms, while ISG ZSM focuses on automation techniques, service management, management functions, and full automation.

ISG ENI and ISG ZSM are not doing the same technical things. The capabilities provided by the ENI system such as the AI/machine learning algorithms, intent policies, SLA management can be leveraged by ISG ZSM to enhance the automation of network and service management, especially for service assurance and service intelligence.

5.4.2 Architecture relevant to ZSM in ISG ENI

5.4.2.1 Introduction

The ENI functional architecture is a high-level decomposition of an ENI System into its major components, along with a characterization of the externally visible behaviour (e.g. as defined by a set of reference points) of the components. This includes functionality and behaviour, functional architecture, functional blocks, external reference points of an ENI system.

A primary goal of ENI is to provide a robust, distributed, context-aware platform that uses modelling, policy management, and AI to enable the Assisted System to perform more accurate and efficient decision making.

5.4.2.2 Functional Architecture

ENI system applies policy-driven closed control loops that use emerging technologies, such as big data analysis, analytics, and artificial intelligence mechanisms, to adjust the configuration and monitoring of networks and networked applications, and dynamically updates its acquired knowledge to understand the environment, including the needs of end-users and the goals of the operator, by learning from actions taken under its direction as well as those from other machines and humans (i.e. it is an experiential architecture).

Figure 5.4.2.2-1 is a high-level Functional Block diagram with the use of an API Broker. This is a simplified view of the main processing components of an ENI System. While, Figure 5.4.2.2-2 shows the high-level functional architecture of ENI with no API Broker utilized.

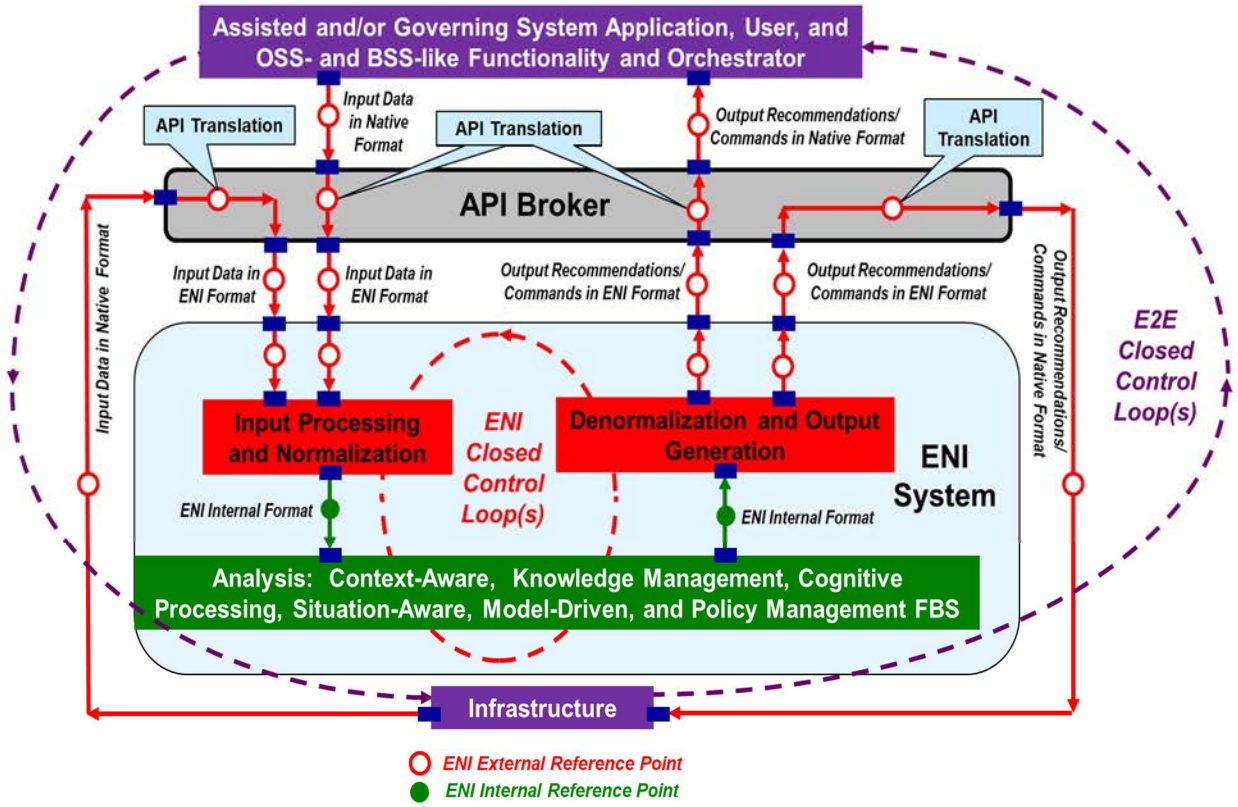


Figure 5.4.2.2-1: High-Level Functional Architecture of ENI When an API Broker Is Used
(source: from ETSI GS ENI 005 [i.35])

The purpose of the API Broker is to serve as a gateway (i.e. translation mechanism) between different systems, which is used to translate between the APIs and data formats used external to the ENI System and the APIs and data formats used internally by the ENI System. The use of API Broker is able to simplify integration with external systems, such as architectures of other ETSI groups and SDOs.

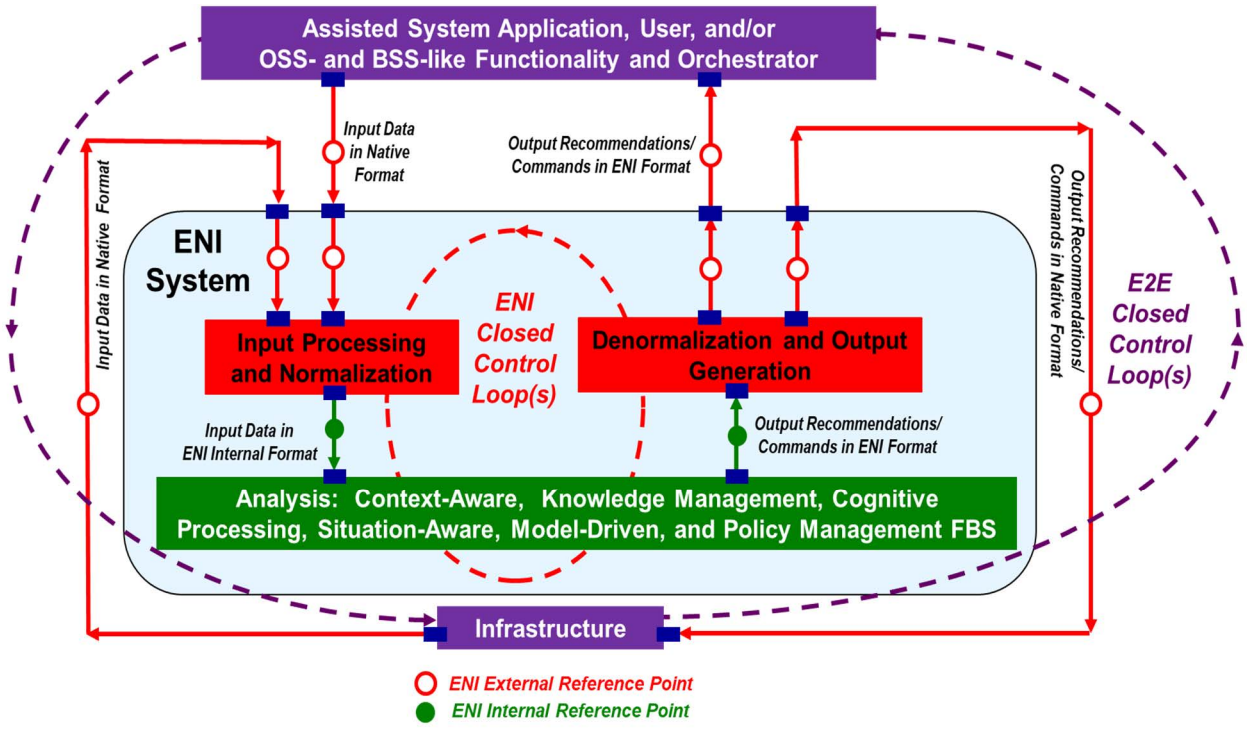


Figure 5.4.2.2-2: High-Level Functional Architecture of ENI When an API Broker is Not Used
(source: from ETSI GS ENI 005 [i.35])

There are two closed control loops in Figure 5.4.2.2-1 and Figure 5.4.2.2-2. Both closed control loops operate to achieve a set of goals. The outer loop adjusts for context and situation changes, and the inner loop optimizes business goals when the outer loop is stable as described in ETSI-WP44 ENI vision [i.244].

Three types of Functional Blocks are included in the ENI System:

- Input Processing. It consists of Data Ingestion Functional Block and Data Normalization Functional Block.
- Analysis. It includes Knowledge Management and Processing, Situation-based, Model-driven, Policy Generation:
  - The Knowledge Management and Processing further consists of three Functional Blocks: Knowledge Management, Context Awareness, and Cognition Management Functional Blocks.
  - The Situation-based, Model-driven, Policy Generation further consists of three Functional Blocks: Situation Awareness, Model-Driven Engineering, and Policy Management Functional Blocks.
- Output Generation. It consists of two Functional Blocks: Denormalisation and Output Generation Functional Blocks.

5.4.2.3 Technologies Applied in Architecture

1) The Assisted System

It is the system that the ENI System requires data from and provides recommendations and/or management commands to. Within the current scope of ENI, there are three classes of Assisted Systems:

Class 1: An Assisted System with No AI-based decision-making Capabilities. For this class of Assisted System, ENI operates as an external system that communicates with the Assisted System through standard Reference Points and APIs defined by ENI. The ENI System is not involved in making decisions in the real-time control loop of the Assisted System.

Class 2: An Assisted System with AI-based decision-making Capabilities but Not in the Control Loop. For this class of Assisted System, the ENI System is not involved in making decisions in the real-time control loop of the Assisted System. This class of system works as an extension of class 1.

Class 3: An Assisted System with AI-based decision-making Capabilities in its Control Loop. For this type of Assisted System, the ENI System is involved in making decisions for any function performed by the Assisted System, significantly, this includes real-time decisions.

2) Mode of Operation

The ENI System operates in two different modes, called "recommendation mode" and "management mode". The operation of the ENI System in recommendation mode is that it provides recommendations to the Assisted System. In contrast, when the ENI System is operating in management mode, the ENI System provides decisions and commands to be implemented by the Assisted System.

Setting the mode of Operation need be negotiated between the ENI System and the Assisted System based on applicable information (e.g. regulatory policies, status of the infrastructure, and goals input by the operator) in a given context or situation.

3) Communication

The communication between the ENI System and the Assisted System (or its Designated Entity) can be applied for discovery (a new started-up device, application, or system to find its peers), direct configuration and negotiation of control and management parameters, and Switching the Mode of Operation.

5.4.2.4 Architecture Requirements

In clause 5, it specifies the requirements for functional architecture, reference point, mode of operation, and non-functional aspects. Some key requirements supported by ENI that are also relevant to ZSM include: model-driven, (one or more) closed control loops, data ingestion and normalization, telemetry data ingestion in streaming and batch modes, ENI Policies, cognition processing, etc.

5.4.2.5 Reference Points

Figure 5.4.2.5-1 shows a more detailed Functional Block Diagram that contains all of its input Reference Points.

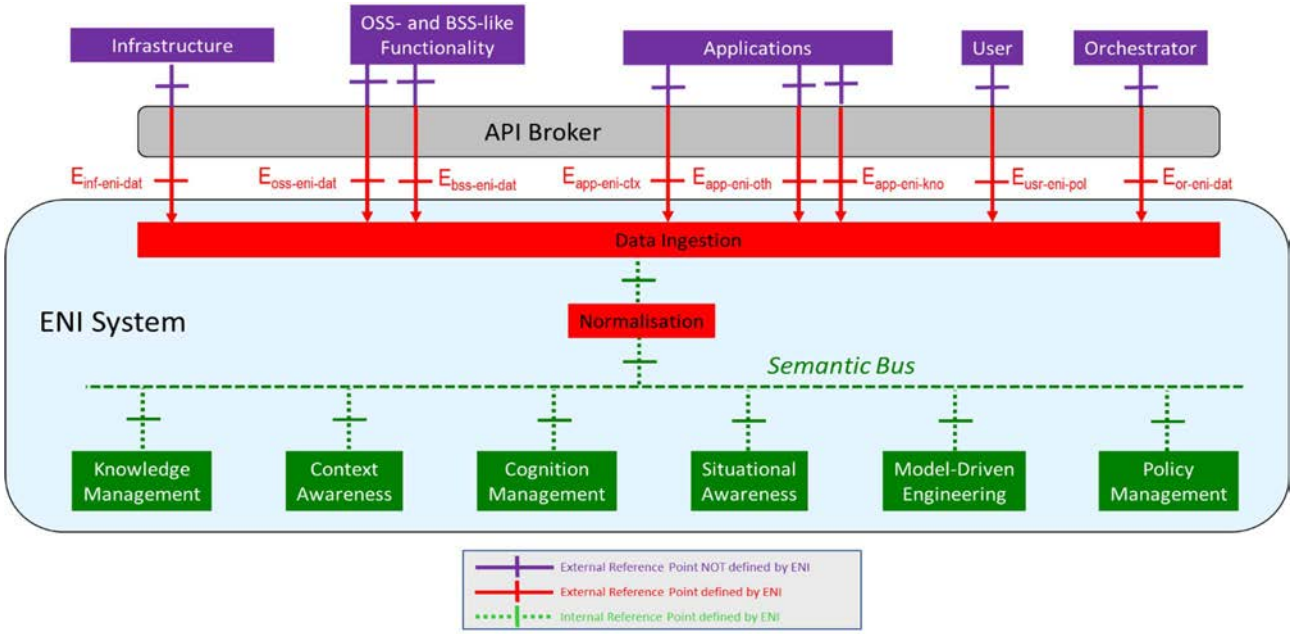


Figure 5.4.2.5-1: Functional Architecture with its Input Reference Points
(source: from ETSI GS ENI 005 [i.35])

Figure 5.4.2.5-2 shows a more detailed Functional Block Diagram that contains all of its output Reference Points.

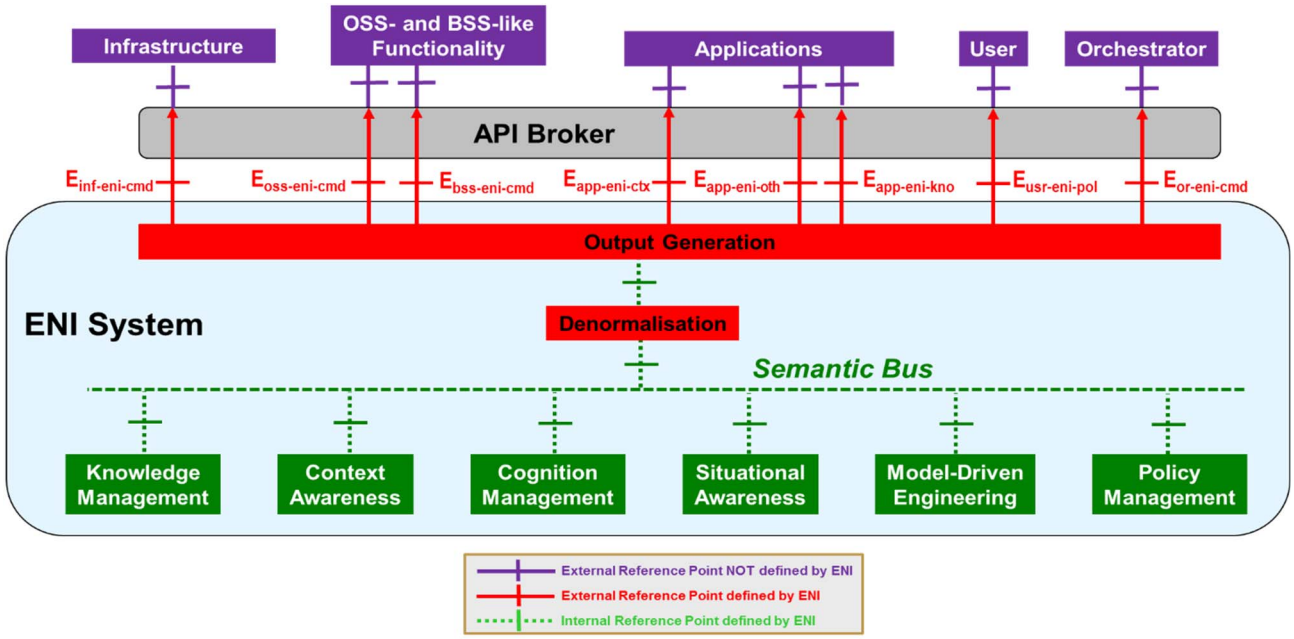


Figure 5.4.2.5-2: Functional Architecture with its Output Reference Points
(source: from ETSI GS ENI 005 [i.35])

Some of the reference points that may be relevant to ZSM are listed as follow:

- Reference Point $E_{oss\text{-}eni\text{-}dat}$. It is used by the OSS-like functionality of the Assisted System to provide data and information for ENI to ingest and process.

- Reference Point $E_{oss\text{-}eni\text{-}cmd}$. It is used by ENI to send recommendations and/or commands, as well as acknowledgements, to the OSS-like functionality.
- Reference Point $E_{bss\text{-}eni\text{-}dat}$. It is used by the BSS-like functionality to send data to ENI.
- Reference Point $E_{bss\text{-}eni\text{-}cmd}$. It is used to define data and acknowledgements exchanged between the BSS-like functionality and ENI.
- Reference Point $E_{usr\text{-}eni\text{-}pol}$. It is used to define policies exchanged between external entities and ENI that control behaviour (including services and resources) for a user (or an agent acting on behalf of the user).
- Reference Point $E_{or\text{-}eni\text{-}dat}$. It is used to define data and information sent from the Orchestrator to ENI.
- Reference Point $E_{or\text{-}eni\text{-}cmd}$. It is used to define recommendations and commands sent from ENI to the Orchestrator.

NOTE 1: ZSM can be regarded as an assisted system, and can interact with an ENI system to get recommendations and/or requests from it to improve the ZSM decision-making capabilities. The identified reference points above may be applied for the interactions between the ZSM framework architecture and the ENI system for exchanging data/information, policies, as well as recommendations and/or requests, etc.

NOTE 2: As mentioned in annex A: SDO and Open Source Interactions [i.35], ENI will further study the integration of ENI with ZSM in Release 2.

5.4.3 ENI application relevant to ZSM

As specified in ETSI GR ENI 007 [i.183], it defines various categories for the level of application of Artificial Intelligence techniques to the management of the network, going from basic limited aspects, to the complete AI based network management. The definition of network autonomicity categories may be useful to quickly guide users in choosing a specific implementation of AI assisted network, and understanding the self-adaptation capabilities to, i.e. changed service conditions, faults, deployment of new services and the autonomicity of operation and overall management. Table 1 given in ETSI GR ENI 007 [i.183] shows how the technical factors impact the categories of network autonomicity from a technical point of view.

NOTE 1: Whether the categories of network autonomicity defined in ETSI GR ENI 007 [i.183] can be leveraged/referenced by ZSM need further investigation.

ETSI GR ENI 008 [i.184] describes the motivation, requirements, and key issues of using intent policies to manage the operation of networks and networked applications in various domains. A new functional block named Intent Translator is introduced to the existing architecture of ENI system (ETSI GS ENI 005 [i.35]), which is responsible for translating the Intent Policy to the target DSL or software.

NOTE 2: ENI is exploring how to define and use intent policies within the ENI System Architecture, whether their work can be leveraged/referenced by ZSM in supporting the intent-based management needs further study.

5.5 Void

5.6 TM Forum

5.6.1 Open Digital Architecture

5.6.1.1 Introduction

Supported by most of Tier-1 operators (AT&T, Orange, Verizon, T-Mobile, Telstra TIM, BT, Telefonica, etc.), TM Forum's Open Digital Architecture (ODA) project [i.37] is envisioned as a more agile replacement for traditional operational and business support systems (OSS/BSS) architecture.

The project addresses the ODA Vision (IG1166 [i.43], public) of a model driven ODA lifecycle for business agility. It extends the Open Group TOGAF™ Architecture Development Methodology by identifying for each ODA lifecycle the stakeholders, their activities, the tools and TM Forum artefacts they need to perform their Lifecycle roles. It uses existing TMForum artefact including OPEN APIs, Information Framework (a.k.a SID), Business Process Framework (a.k.a eTOM), and augmented with new features as detailed in the specific new artefacts dealing with:

- **Key Requirements and Principles:** this task has created a Concepts and Principles Document (GB998 [i.45], member) that is used to evaluate current and future artefact such as to demonstrating the principle of high cohesion between data and process but loose coupling between components.

- **Functional Architecture:** a new architecture diagram with introductory text. Agree Level 0 & Level 1 functional architecture/framework with L1 capabilities mapped to each L0 layer - use eTOM & SID together to define functional groupings (i.e. capabilities) on the map.

- **Ecosystem Capabilities:** contribute ecosystem requirements and principles to Requirements and Principles Workstream. Provide requirements to ensure that ODA enables CSPs to become a contributor to an ecosystem platform and/or a curator of such a platform (on-boarding, etc.). Develop an IoT ecosystem scenario and requirements to prove the ecosystem capabilities of ODA (harvest from Catalysts where appropriate).

- **ODA Production:** covers the functional scope of what is commonly referred to as Service and Resource Management and patterns for realization. It defines what services are exposed while decoupling them form the details of how they are realized and evolve.

  It has been derived from more than 6 Catalyst Proof of Concept demonstrators.

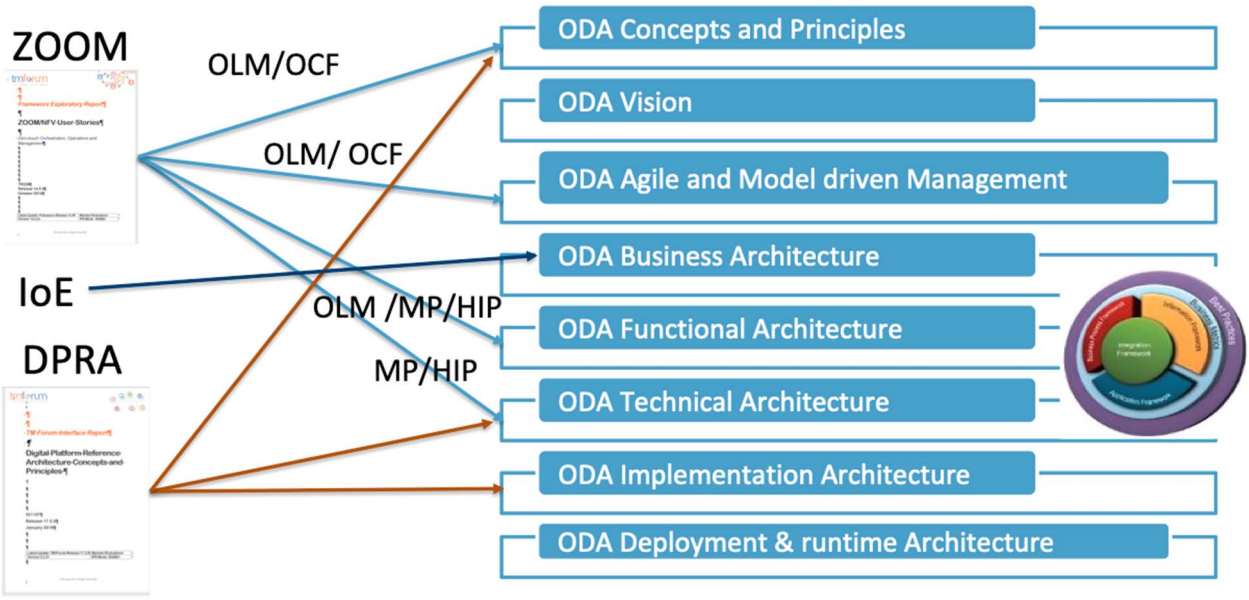
5.6.1.2 ODA High Level Description

A quick description of ODA is mandatory to prove its relevance to ZSM activity.

The principles on top of ODA are the ones that drive the Digital Transformation in terms of flexibility, business agility, cloud nativeness, multi-vendor capability, leading to a model overcoming the separation of OSS/BSS functionalities: even they remain in separate operational domains, they are designed as part of a single architecture.

ODA is the natural evolution of several TM Forum projects that integrates within ODA to provide a complete E2E view of service provisioning. ODA will progressively encapsulate all activities related to the evolution of Management Systems and the provisioning of Digital Services and will strictly cooperate with all other TMF collaborative projects in particular with Frameworx [i.36] and Open API projects [i.38].

It strongly relies on the newly delivered with Apache 2.0 licence. TMF Open APIs and it is consistent with Frameworx definitions and domains. ODA includes key concepts from platform architectures work (TR262 [i.55], member) and is based on initial OSS and BSS of the future work with requirements gathered from several Tier 1 CSPs, incorporating concepts such as model driven orchestration and automated onboarding coming from TM Forum ZOOM project are being progressively merge into ODA.



Acronyms:
ZOOM - Zero touch Operation Orchestration and Management
DPRA - Digital Platform Reference Architecture
OLM - On boarding and Life cycle Management
OCF - Operation Center of the Future
MP - Management Platform
HIP - Hybrid Infrastructure Platform

Figure 5.6.1.2-1: Convergence of developing threads into ODA activities
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from IG1167 [i.44])

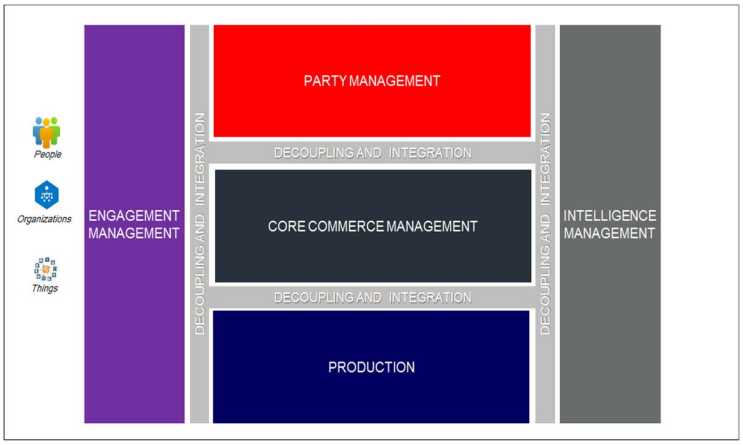


Figure 5.6.1.2-2: ODA realized through a Functional Architecture
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from IG1167 [i.44])

In the ODA model there are 6 main disjoint functional blocks that represent its 0-level view:

- Engagement Management for a single coherent customer experience.
- Party Management supporting complex business models.
- Core Commerce Management supporting third party and marketplace offers and service composition and orchestration.
- Production abstracting the complexity of infrastructure.

- Intelligence Management to support systems of insight, AI, Machine Learning and Cognitive capabilities.
- The de-coupling construct is critical as well as it allows all function blocks to communicate directly removing any concept of hierarchy or traditional layering.

ODA Production provides a systematic model driven approach to mapping the technology domains defined by suppliers and technology SDOs to the multiple operational domains (defined by individual CSPs) and the services they expose, such as the TM Forum Network as a Service (NaaS) API Component Suite. Derived from more than 6 NaaS and 5G Catalyst/PoC projects it defines management requirements (Stages 1 and 2), and it is developing a NaaS resource neutral connectivity service data model specification (Stage 3) integrated with the TM Forum Information Framework (a.k.a SID).

It is underpinned by industry models for lifecycle management OASIS TOSCA and a range of hybrid infrastructure realizations - based on prior ZOOM project work - including NFV, Multi-cloud and network appliances and use of TM Forum Open APIs.

ODA is component based with Open APIs integrating them dynamically and not necessarily the only ones developed within TM Forum: it relies on loosely coupled standardized components (micro-services) with industry agreed boundaries, supporting multi-vendor and multi-tenant ready, and leveraging on Open Source projects. Components expose metadata to automate lifecycle management (packaging, automatic discovery, etc.).

TM Forum is working on an extension of Frameworx to provide an industry standard language to define components.

ODA has design-time and run-time capabilities integrated within the functional blocks. There is no need to 'stop the machine' when adding new products and services or resources.

All Components expose their capabilities in catalogues, so that service designers (and orchestrators) have visibility of capabilities (internally and externally).

Virtual and cloud networks rely on orchestration to chain service elements as needed. The same principle should apply to the support systems, a new service/product design is necessary to orchestrate supporting functions as required. Moreover, all layers should work in real time: customer information such as usage, billing and partner/ecosystem settlement are updated in real time from self-service web based interactions. Similarly, performance and fault data are provided in real time to allow rapid automated response and possibly the auto-healing of the services.

5.6.1.3 ODA deliverables

The following deliverables deployed with Frameworx R18 on July 2018 seem relevant for the ongoing work in ZSM:

- GB998 ODA Concepts and Principles [i.45]:
  - This document proposes a set of architecture principles as general rules and guidelines.
  - This document outlines some high level principles agreed by all stakeholders, that guide in the implementation of target architectures.

➔ This work, together with the User Stories document developed in ZOOM "TR229 ZOOM/NFV User Stories Suite R17.0.1 [i.56] ", can be a useful complement of what developed in the ETSI GS ZSM 001 [i.2], Requirements document.

- IG1166 ODA Vision [i.43]:
  - Blueprint that provide pragmatic pathways for the journey from maintaining monolithic, legacy software solutions, towards managing nimble, cloud-based capabilities that can be orchestrated using AI. It includes:
    - Eight key Architecture Framework artefact groupings that are needed to achieve business agility and zero touch automated operations based on TOGAF® concepts.
    - Methods for Agile Model Driven Management to achieve agile service lifecycle management.

➔ Sets out all the dimensions that need to be addressed by ZSM to achieve Zero touch automation using TOGAF™ Enterprise architecture best practice and is an exemplar for linking vision to concrete artefacts.

- TMF071 ODA Terminology [i.49]:
  - This document provides a glossary of terminology relevant within ODA documentation.
  - In addition to ODA native terminology, there are other taken or derived from external industry publications, or existing TM Forum documents.

➔ This document is the natural complement of "ETSI GS ZSM 007 [i.1] Terminology for concepts in ZSM" and a place where several common terms can be fruitfully shared and aligned for a better context management.

- IG1167 ODA Functional Architecture (public) [i.44]:
  - The Purpose of this document is to provide a set of structured, implementation-neutral and simplified views for the Information and Systems environment.
  - It is intended to help enterprises looking to become digital to acquire and implement information and systems architectures that meet an industry agreed model.
  - The functional architecture view enforces the principles established in the previous mentioned documents GB998 [i.45] and references Frameworx Business Process Framework (eTOM GB921 [i.46]) and Information Framework (SID GB922 [i.47]).

➔ A full set of examples is provided on how different production scenarios can be compared to the ODA big picture and also the ZSM architecture has been mapped to it (see Figure 5.6.1.3-1).

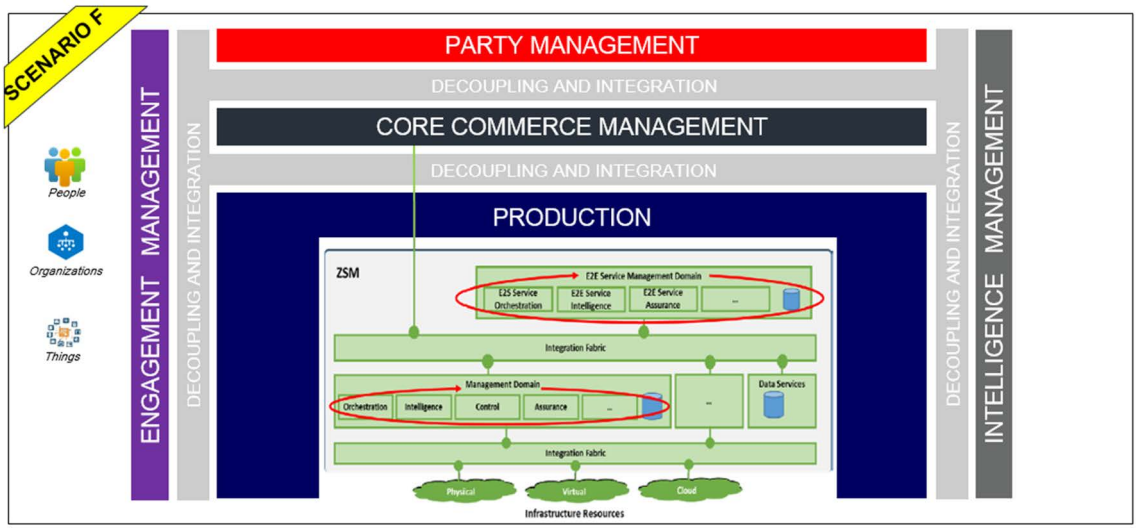


Figure 5.6.1.3-1: Mapping ZSM architecture to ODA big picture
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from IG1167 [i.44])

- IG1171 ODA Component Definition (public) [i.48]:
  - This document describes reasons for defining an ODA Component, which stems from the need for an agile approach that encompass business needs, network structure and operational challenges. It then describes the structure of a component, its sub parts and their functionality as well as suggesting ways of exposing the functionalities. The documents also address the lifecycle of the component and its composability aspects. Another section is devoted to the relation of the components the existing Frameworx including to the Open APIs. Subsequent releases are expected to materially enhance the connection to digital business, the use of a component on existing industry platforms, compose scenarios and examples.

➔ In the Architecture document ETSI GS ZSM 002 [i.187] it is largely discussed on the Functional Components and how they perform tasks and expose services via APIs. So it seems that the work on-going within TMF in IG1171 [i.48] can be useful for providing a model representing how these components interacts each other thus adding value to the work in ZSM.

Ongoing activities in ODA, as well as providing evolution of the above mentioned documents, will work on a "User Guide for Network Slice Management" that seems relevant to ZSM activity since it aims at providing a user's guide concerning how to manage network slices at an abstracted simplified level using TM Forum artefacts to support multiple and changing business models.

It wants to show how to design 5G enabled services using a common CFS specification (service level abstractions of the resources) for network slice management solutions - together with the features that need to be exposed including those where customer self-control is needed. It can result as proficient comparison for what done in this Project.

5.6.2 TM Forum Open API Program

5.6.2.1 Description

TM Forum's Open API program [i.38] is a global initiative to enable end-to-end seamless connectivity, interoperability and portability across complex ecosystem based services.

The program is creating an Open API suite which is a set of standard REST based APIs enabling rapid, repeatable, and flexible integration among operations and management systems, making it easier to create, build and operate complex innovative services.

TM Forum REST based APIs are technology agnostic and can be used in any digital service scenario, including B2B value fabrics, Internet of Things, Smart Health, Smart Grid, Big Data, NFV, Next Generation OSS/BSS and much more. Recently, to enable diffusion of Open APIs, TMF announced its partnership with the Linux Foundation to foster Communications Service Providers' (CSPs) adoption of new technology in open source projects and facilitate the emergence of an industry marketplace of compatible open source and commercial applications.

TMF Open API Apache project will develop the "code" part of the TM Forum Open APIs to be licensed under the Apache 2.0 license mode. This will include re-releasing API previously released under RAND (Reasonable and non-discriminatory) license mode.

As a first result, some of TMF Open APIs are included in the "External APIs Framework Project [i.40]" of LF ONAP Project (starting from ONAP B release), specifically:

- Service Catalog (TMF633 [i.50]).
- Service Order (TMF641 [i.51]).
- Resource Order (TMF652 [i.52]).
- Service & Resource Activation & Configuration (TMF640 [i.53]).
- Service Inventory (TMF638 [i.54]).

The full list of available Open API can be inspected in the Open API Map portal [i.42], public but requires one to register on the TM Forum website as non-members. The Purpose of TMF Open APIs is to provide a collection of interfaces to enable E2E management solutions, covering all phases of service provisioning, from the set-up of the consortium offering the service, to its proposition, activation, operation and monetization.

TMF is also working for providing an Open Implementation Toolkit for the APIs: the Open Digital Lab project [i.41] is working to create a sandbox container (Docker, Kubernetes) which has (Node-RED, Node.js, Mongo DB, OpenWhisk, MQTT) and a sample starter kit microservice application using TMForum API's.

The goal is to give this as a starter template to catalyst teams and others to jump start their work and to expose their micro-services via API Connect for testing and learning (be mindful of the limitations associated with the lite account listed next). The container based environment will be staged in IBM Cloud to build code patterns, sample use case ideas, to showcase how AI, Deep Learning, other services like Weather API's, etc. can be leveraged to build innovative applications and create a collaborative monetization ecosystem.

The recently approved NaaS API Component Suite (TMF909 [i.241]) which is s composition of Open APIs with an associated profile for use between ODA Production and other ODA Function Blocks such as Core commerce:

- The analysis of what on-going in this TMF API project, can be useful for providing reference implementations of the Exposure Services within ZSM.

- NaaS API Component Suite should be considered as the preferred definition of the capabilities /interface end points between ZSM e2e Service Management and Automated Customer and Business Management (Digital Storefront).

5.6.3 TMF Forum Open Source Activities

5.6.3.1 TMF Business Operation System (BOS)

This pioneer project is developing in phases an open source reference implementation of a core part of the TM Forum Open Digital Architecture (ODA).

The primary focus for demonstration at Digital Transformation World 2019 is on a subset of the ODA Core Commerce, Engagement and Party Function Blocks (additional information can be provided on request).

It provides a reference componentization of this functionality where the components exposed TM Forum Open APIs and is documenting practical guidance on implementation considerations and can be used for interoperability testing with commercial products also using TMForum Open APIs.

The initial implementation is using the Open Digital Lab [i.41].

5.6.3.2 Use of Industry Open Source

Catalyst projects [i.39] are the primary users of industry open source and the main Open Source implementations that has been used are:

- LF ONAP.
- ETSI MANO OSM.

These are mainly used to realize Service and Resource Management functions and are the primary basis of feedback from our programs to the open source groups developing them.

About five Digital Transformation World 2019 catalysts are planning to use ONAP as it has support for TM Forum Service Catalog, Service Order and Service Inventory APIs embedded in the open source since the Casablanca release. This makes it convenient to integrate with other commercial implementations based on the same TM Forum Open APIs.

5.6.4 Autonomous Networks

TM Forum started the Autonomous Networks Project (ANP) since July 2019 with the scope consisting of:

- User stories/use cases.
- Vision & roadmap.
- Business requirements and architecture.
- Technical architecture.

The Autonomous Networks (AN) aims to define fully automated zero wait, zero touch, zero trouble innovative network/ICT services for vertical industries' users and consumers, supporting self-configuration, self-healing, self-optimizing and self-evolving telecom network infrastructures for telecom internal users: planning, service/marketing, operations and management. Autonomous Networks incorporate a simplified network architecture, autonomous domains and automated intelligent business/network operations for the closed-loop control of digital business, offering the best-possible user experience, full lifecycle operations automation/autonomy and maximum resource utilization.

As documented in AN WP [i.209], it develops a common understanding and consensus on the autonomous network concept and automation classification for the simplification of telecom network infrastructure, automated & intelligent operations and innovative services. Mapping of autonomous network use cases with the autonomous network levels is given in a table in section 3 to illustrate and clarify how the O&M efficiency, energy efficiency, resource efficiency, user experience are improved.

As documented in IG1193 [i.210], it shares the vision and roadmap of autonomous networks, including the motivation, vision, requirements and principles, new ecosystem, collaboration and business models, overarching framework and autonomous levels, roadmap and industry collaboration.

As documented in IG1218 [i.211], it provides business requirements and business architecture of services and infrastructure supported by autonomous networks, including the user requirements per user stories, key business capabilities and architecture, and related key metrics for measuring autonomous levels, as well as new business models of production, ecosystem, collaboration.

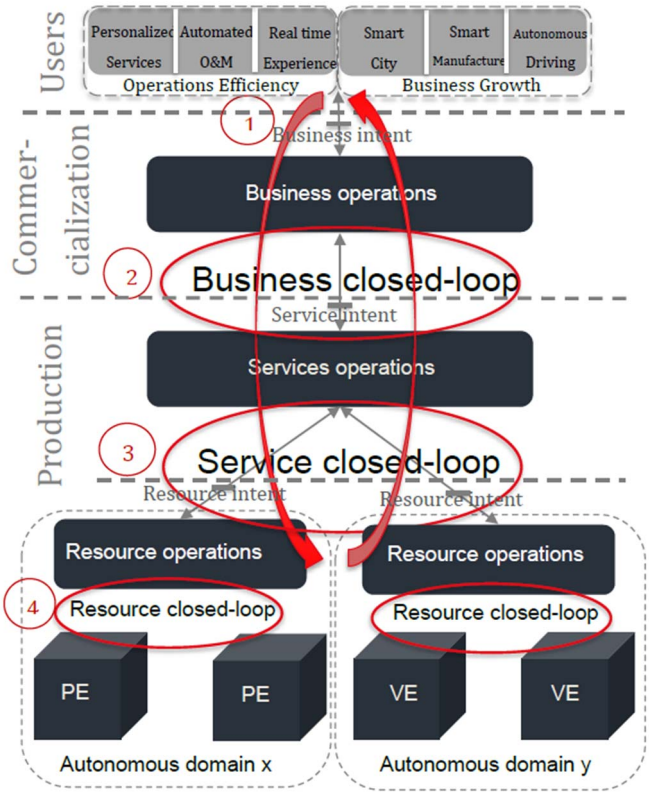


Figure 5.6.4-1: Autonomous Networks closed loops
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from IG1218 [i.211])

The framework of Autonomous Networks consists of "3-layer, 4-closed-loop".

3-layers: represent a group of common capabilities and business logics that can be utilized to support all scenarios, as well as business relationships between the groups of atomic capabilities:

- **Network resources layer:** mainly provides the capabilities and business logics of network resources and automation in each autonomous domain level.
- **Network operations layer:** mainly provides the capabilities and business logics of network planning, design, roll-out, provisioning, assurance and optimization operations across multiple autonomous domains.
- **Business operations layer:** mainly provides the capabilities and business logics of customer, ecosystem and partner business enabling and operations for autonomous networks services.

4-closed loops: represent the execution/fulfilment of the full lifecycle of the operations that can use the select capabilities of above layers upon corresponding business process:

- **Network resource closed loop:** the interaction of network resource operations in the granularity of autonomous domains. The network needs to be upgraded from fragmented, siloed network element level integration towards a closed loop of network autonomous domain based on an extremely simplified network architecture.

- **Network operations closed loop:** the interaction between service and network resource operations. The operations need to be upgraded from legacy customized project-centric approach to a data/knowledge driven platform based on full lifecycle operations automation.
- **Business operations closed loop:** the interaction between business and service operations. The operations needs to be upgraded from isolated business to on demand, automated business collaboration and ecosystem.
- **Cross layer user service closed loop:** the interaction across the above three layers' and three closed loop processes to support the user service fulfilment.

As documented in IG1230 [i.212], it is structured into three parts:

- Part I: definition of an autonomous network:
  - It further includes the scope and objectives of the autonomous networks, and architecture overview. The ultimate goal is to simplify network architecture enabling efficient intelligent operations, and rapid and agile integration of intelligent network innovation.
- Part II: reference architecture of autonomous network framework:
  - It further details the autonomous networks technical architecture as shown in Figure 5.6.4-2, and architecture building blocks (AN levels, Autonomous Domains, Intent-driven Interactions, Closed Loop Mechanisms, Knowledge and Intelligence, and Simplified Infrastructure).
- Part III: realizing the autonomous network (implementation exemplars):
  - It provides some autonomous networks scenarios, standards and next steps.

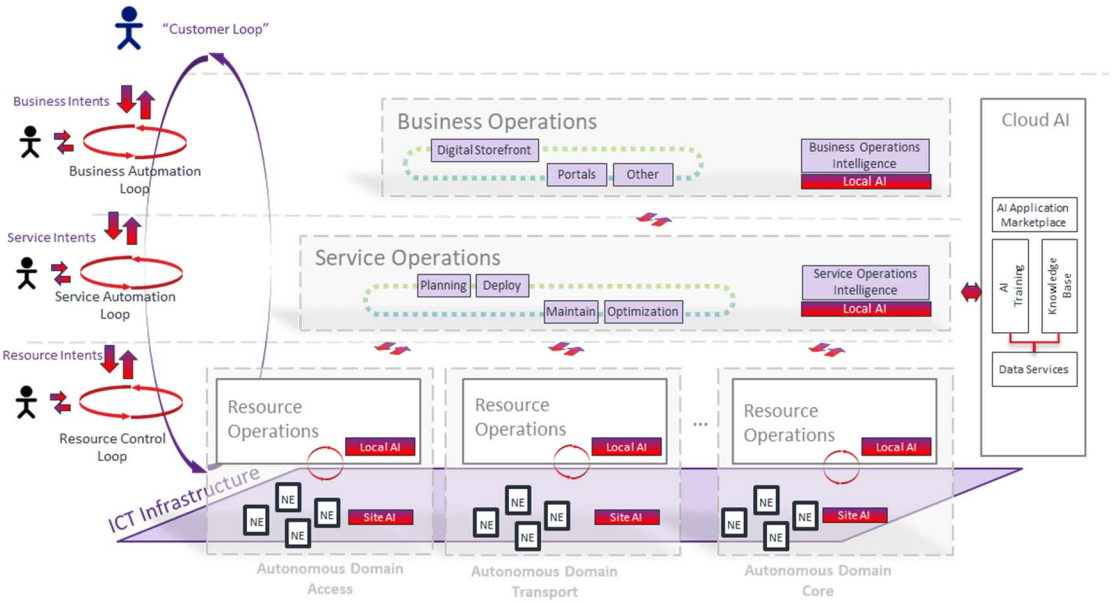


Figure 5.6.4-2: Autonomous Networks Technical Architecture
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from IG1230 [i.212])

As shown in Figure 5.6.4-3, a very high level harmonization of their AN technical architecture with our ZSM framework is provided as an example.

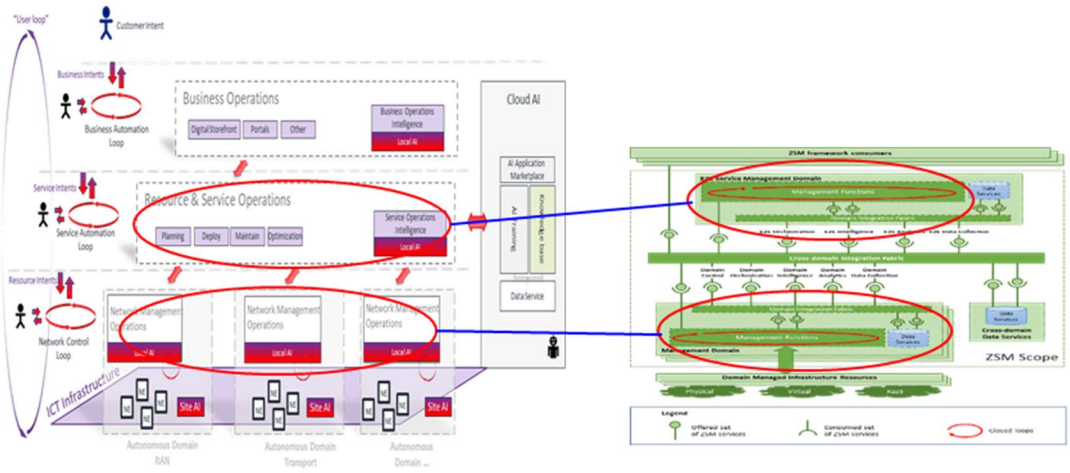


Figure 5.6.4-3: AN Technical Architecture Mapping with ZSM
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from IG1230 [i.212])

NOTE 1: Closed loops, intent driven interaction, and self-X operating capabilities are the key requirements of AN; ZSM can work with TM Forum on how to provide these capabilities in a standard and coordinated way.

NOTE 2: TM Forum calls for the alignment on AN concept, vision, AN framework and key topics cross-SDOs. ZSM can work with TM Forum and other SDOs in a coordinated way on these topics.

NOTE 3: As indicated in AN blueprint and next steps, TM Forums AN Project will dive deeper into the information modeling aspects of Intent and Control Loops (Control Loop mechanisms, unified Intent Meta-model, etc.) but also explore the API side of these concepts (AN level evaluation, TMF Intent APIs, TMF Control Loop APIs, etc.).

5.6.5 AIOps Service Management

TM Forum AI for IT & Network Operations (AIOps) explores multiple AI-based use cases within IT and network operations around how to improve customer experience, service quality, and efficiency by automating and optimizing communications service providers' (CSPs') processes and services. The project redesigns and reengineers AIOps service management frameworks and processes in order to support agile deployment and efficient operations of AI components, helping operations teams and process owners to exploit AI safely maximizing the business value, mitigating risks and ensuring expected level of quality.

As documented in IG1190 [i.213], it addresses the challenge on how to govern, deploy, operate, control and maintain hundreds or even thousands of AI models and AI components within CSP's IT and network systems architecture by redesigning and reengineering the complex processes of service lifecycle and operations management, in order to prepare them to handle and govern massive AI software deployment at scale and to operate safely and correctly.

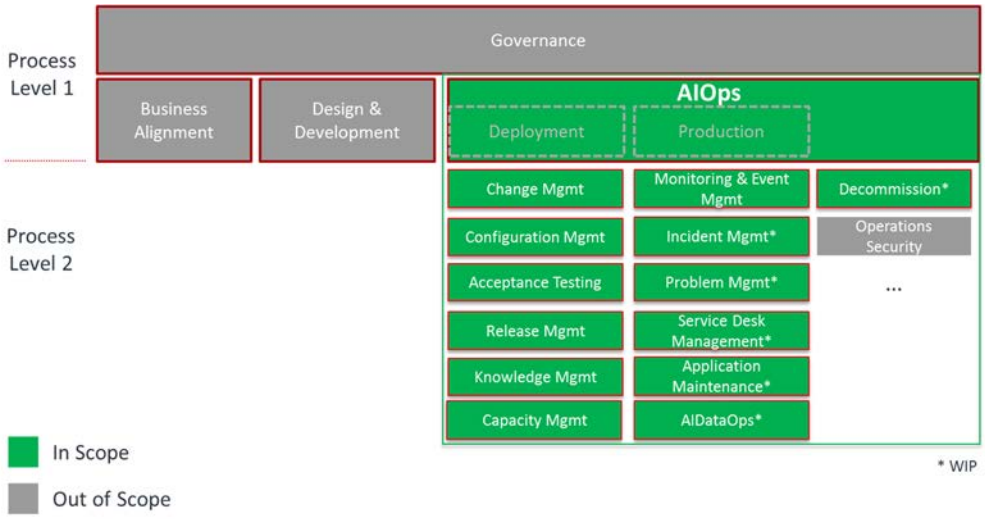


Figure 5.6.5-1: Services Management processes in scope
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from IG1190 [i.213])

As shown in Figure 5.6.5-1, the list of processes shown in green is in scope and will be redesigned and reengineered:

- Configuration Management (IG1190A [i.214]).
- Change Management (IG1190B [i.215]).
- Release Management (IG1190C [i.216]).
- Acceptance Testing (IG1190D [i.217]).
- Knowledge Management (IG1190E [i.218]).
- Monitoring & Event Management (IG1190F [i.219]).
- Incident Management (IG11906G [i.220]).
- Problem Management (IG11906H [i.221]).
- Service Desk Management.
- Application Maintenance (Preventive and Perfective Maintenance).
- Capacity Management.
- AIDataOps.

Configuration Management ensures that all components (also called Configuration Items, CIs) of systems and services are uniquely identified, baselined and maintained and that changes to them are controlled across the whole service lifecycle. The process scope, gaps and challenges, and Process Reengineering Principles of configuration management in AIOps are identified in IG1190A [i.214].

Change Management ensures a smooth transition of all changes to Production live environments. It minimizes the risks, preserves the quality of service, avoiding incidents and outage, and prepares the final users/consumers to adopt the new capabilities/features. The process scope, gaps and challenges, and Process Reengineering Principles of change management in AIOps are identified in IG1190B [i.215].

Release Management plans and manages the deployment of any software release from Development to Production environments (and in general, to any relevant environment). The process scope, gaps and challenges, and Process Reengineering Principles of Release Management in AIOps are identified in IG1190D [i.216].

Acceptance Testing ensures the overall quality against the expected targets of all new and existing updated software and services, before declaring and certifying them as "operations ready" and "deployable" to the Production live environment. The process scope, gaps and challenges, and Process Reengineering Principles of Acceptance Testing in AIOps are identified in IG1190C [i.217].

Knowledge Management ensures that reliable and complete information and knowledge is available to the right parties (people, consumers, 3rd parties...) at the right time throughout the service lifecycle. The process scope, gaps and challenges, and Process Reengineering Principles of knowledge management in AIOps are identified in IG1190E [i.218].

Monitoring & Event Management monitors, detects, filters and correlates all relevant events occurring throughout the Production environments and initiates the corresponding activities to respond to and address those events, when necessary and appropriate. The process scope, gaps and challenges, and Process Reengineering Principles of Monitoring & Event management in AIOps are identified in IG1190F [i.219].

Incident Management addresses all events that have or could have relevant impacts (outages, incidents, defects/bugs, operational issues, quality degradation ...) on the services and, in line with their priority, manages the recovery of the service operations according to the agreed SLAs, minimizing the impacts on users and business processes and managing the necessary communication. The process scope, gaps and challenges, and Process Reengineering Principles of Incident management in AIOps are identified in IG1190G [i.220].

Problem Management is responsible for the diagnosis of the root cause of incidents, issues, vulnerabilities and weaknesses related to systems and services, and, in line with their priority, ensures the permanent resolution of those problems, when appropriate. The key activities involved in a typical IT Problem Management process, the gaps and challenges between traditional Problem Management and AIOps Problem Management, and the Process Reengineering Principles in AIOps Problem Management are identified in IG1190H [i.221].

Service Desk Management is the process responsible for managing the lifecycle of all different types of demands (Service or User Requests) submitted by the end-users to the Service Desk.

Application Maintenance ensures the proper modifications of software and its components after delivery to Production in order to improve their performance, quality, efficiency or other relevant attributes.

Capacity Management ensures that cost-justifiable capacity of services and related components (software, hardware, network, etc.) is able to deliver, the agreed service level targets, presently and in the future, in a timely and effective manner in the specific context of the CSP.

AI Data Operations management (AIDataOps) is vital to ensure that the right data in Production are properly collected, processed, transformed, stored, safeguarded, available and accessible at the right time, according to the business needs, laws, regulations, security policies and efficiency drivers.

NOTE: The redesign and reengineering of service management processes and operations motivated by the introduction of AI technologies (AIOps) may have implications on ZSM work items, such as ETSI GS ZSM 003 [i.246], ETSI GS ZSM 008 [i.245], and ETSI GS ZSM 012 [i.250]. Further analysis and assessment of theses implications would need to be handled by and at the level of each work item.

5.6.6 Closed-Loop & Anomaly Detection & Resolution Automation

AI driven closed-loop automation can be used by CSPs to transform network operations to detect anomalies, determine resolution and implement the required changes to the network within a continuous highly automated framework. The network and service operations of the future can detect anomalous patterns in real time, automate majority of the operations, reduce human error, improve operational efficiency, continue to learn and improve over the lifecycle of network and service, and help deliver innovative, uninterrupted superior quality services to their consumers by applying OODA closed-loop method, AI training models, and AI & Data Analytics.

IG1219 [i.233] (AI Closed Loop Automation - Anomaly Detection and Resolution) documents the definitions, user stories and use cases, and AI & Data Analytics Key Requirements of Closed Loop Anomaly Detection and Resolution Automation (CLADRA).

Based on the work in IG1219 [i.233], TR284 [i.234] (AI Closed Loop Automation - Reference Architecture) defines a vendor- and technology-agnostic reference architecture which can be used to automate anomaly detection and resolution through standard functions, components and interfaces. The reference architecture defined here is created based on reference to several actual use cases contributed by members, which can be found in IG1219 [i.233], such as fault detection in RAN, FTTH Fault Diagnosis, traffic flow optimization, system performance prediction by trend, alert correlation for operations, CDN root cause analysis, charging service anomaly detection.

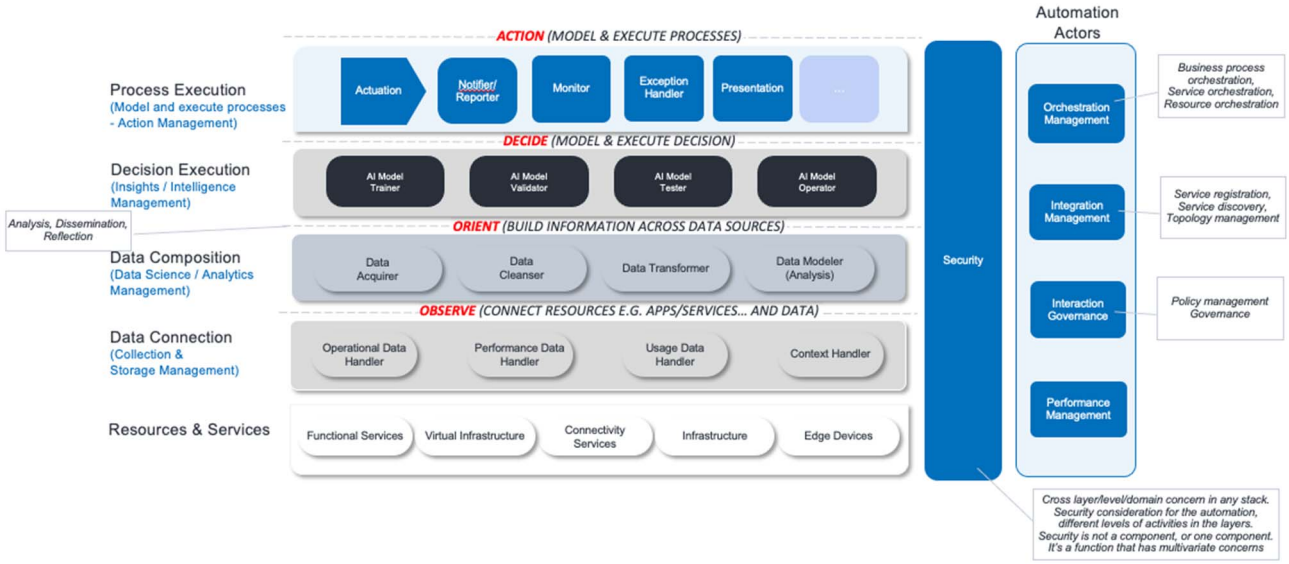


Figure 5.6.6-1: Logical Architecture of CLADRA
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from TR284 [i.234])

As shown in Figure 5.6.6-1, four key functional layers and their logical components constitute the basis of the CLADRA architecture:

- Data Connection;
- Data Composition;
- Decision Execution; and
- Process Execution.

The logical architecture also supports a number of cross-cutting capabilities (security, automation) that need to be enabled in every layer and governed consistently for all layers.

5.6.7 AI Governance

To safely deploy AI at scale, TMF AI Governance defines a set of components, APIs, and operations to assists CSPs to control and govern the AI solutions deployed within a framework.

GB1021 [i.222] provides six AI lifecycle Checklists to support practitioners in the safe and effective deployment of AI systems at scale. The checklists span the lifecycle of AI from procurement and (pre- & post-) development, through deployment and in-life operation, to end-of-life.

GB1180 [i.223] aims to develop an AI data training repository in providing support to the members to quickly design, implement, maintain and manage AI-based data sets and data registries and integrate them into their overall AI architecture. The project focuses specifically on the data sets and information knowledge requisite to support AI models or AI-based inferences by establishing a series of repositories to help the management of data supplied, generated and used.

IG1184 [i.224] defines AI management requirements, interfaces, architectural components and reference architecture to address the problems of accountability, audit and maintenance brought by managing AI at scale. The model depicted in Figure 5.6.7-1 frames the scope and provides a general view of the capabilities from an AI management perspective.

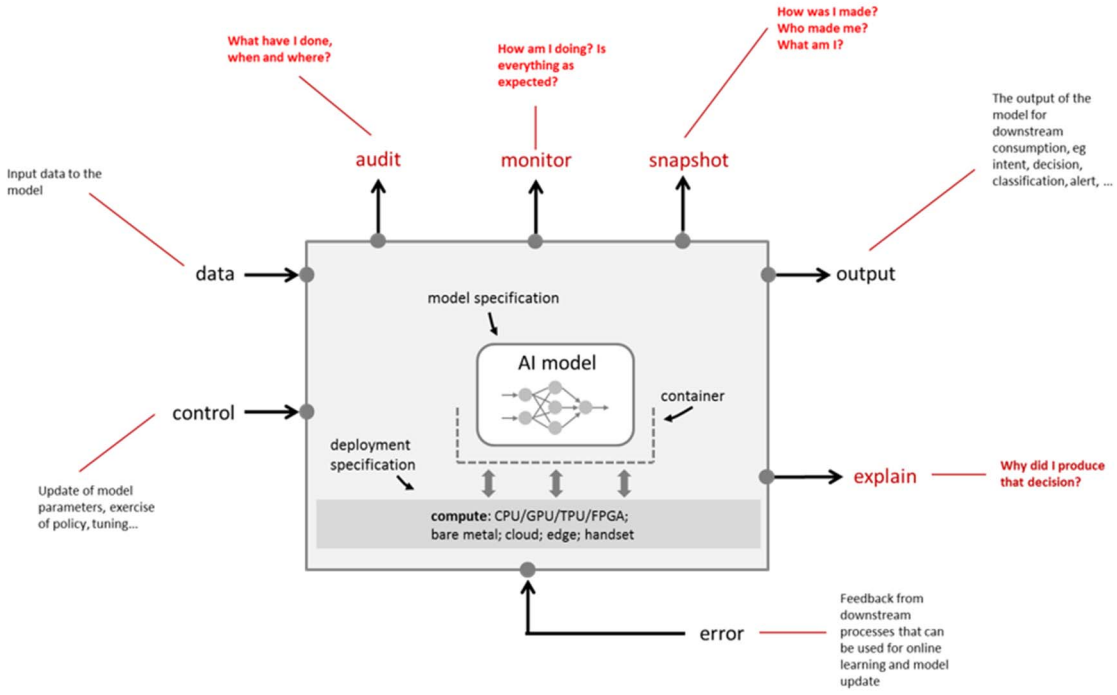


Figure 5.6.7-1: High Level Model for AI Management
(Copyright © TM Forum 2020. All Rights Reserved.)
(source: from IG1184 [i.224])

IG1232 [i.225] provides a specification for an AI Model Data Sheet which captures pertinent information about AI models in a consistent manner, such that potential consumers of the model can determine whether it suits their purpose and, if so, how to deploy the model safely and effectively.

TMF915 [i.226] provides the user guide of the REST API for the AI Management Suite, which includes the resource model definition as well as all API operations for the managed entities and resource models such as AI model, AI model specification, AI contract, AI contract specification, AI contract violation, alarm, rule, event, monitor, etc.

TMF915A [i.227] concerns the API Component Suite for AI Management and defines the set of operations that provide functionality to allow CSPs to govern AI systems deployed at scale. The requirements, component capabilities, flows and sequence diagram on models and contrast are specified.

TMF915B [i.228] focuses on the AI Management API which is restricted to the in-life aspects of AI and in particular on the management of 'model contracts'.

5.7 MEF

5.7.1 Overview

MEF introduced the MEF 3.0 transformational global services framework for defining, delivering, and certifying agile, assured, and orchestrated services across a global ecosystem of automated networks. MEF 3.0 services provide an on-demand, cloud-centric experience with unprecedented user- and application-directed control over network resources and service capabilities. MEF 3.0 services will be delivered over automated, virtualised, and interconnected networks powered by LSO, SDN, and NFV.

MEF is developing LSO (Lifecycle Services Orchestration) specifications with open APIs to automate the entire lifecycle for services orchestrated across multiple provider networks and multiple technology domains within a provider network.

LSO aims to streamline and automate the service lifecycle for coordinated management and control across all network domains responsible for delivering an end-to-end orchestrated service. The LSO Reference Architecture describes the management entities needed to support LSO and the Management Interface Reference Points between them. The Management Interface Reference Points are described such that they can be realized by Interface Profiles and further by open APIs, which can be used to automate and orchestrate services. LSO provides open and interoperable automation of management operations that include fulfilment, performance, control, assurance, usage, analytics, security, and policy capabilities.

5.7.2 LSO Reference Architecture and Framework

MEF currently is building upon the LSO Reference Architecture [i.57] to advance work related to LSO interfaces, standardized open APIs, operational processes, and information models required for orchestrating services across multiple providers and multiple technology domains.

In LSO, Connectivity Services are orchestrated by Service Providers across all internal and external network domains from one or more network operators. These network domains may be operated by communications Service Providers, data centre operators, enterprises, wireless network operators, virtual network operators, or content providers. LSO encompasses all network domains that require coordinated end-to-end management and control to deliver Connectivity Services. Within each provider domain, the network infrastructure may be implemented with traditional WAN technologies, as well as NFV and/or SDN.

As a specification the LSO Reference Architecture and Framework:

- Describes the LSO engineering methodology.
- Provides high level requirements associated with LSO functional areas.
- Defines the LSO reference architecture.
- Outlines operational threads for LSO.
- Identifies the LSO Management Abstractions and constructs.

The reference points in the LSO Architecture represent sets of APIs, defined by Interface Profile Specifications (IPS), for which there is ongoing active collaborative development by MEF members. Until official publication of the respective IPS, APIs will be experimental and subject to change.

Operational Threads describe the high level Use Cases of LSO behaviour as well as the series of interactions among LSO management entities, helping to express the vision of the LSO capabilities.

Operational Threads identified for LSO [i.58] include:

- Partners on-boarding (to be defined in future version).
- Product Ordering and Service Activation Orchestration.
- Controlling a Service.
- Customer Viewing Service Performance and Fault Reports and Metrics.
- Placing and Tracking Trouble Reports.
- Assessing Service Quality Based on SLS.
- Collection and Reporting of Billing and Usage.
- Securing Management and Control Mechanisms.
- Providing Connectivity Services for Cloud.

5.7.3 LSO APIs and LSO Capabilities

As shown in LSO Reference Architecture [i.57], there are seven reference points defined in MEF Reference Architecture and Framework, that is, LSO Cantata (CUS:BUS), LSO Allegro (CUS:SOF), LSO Sonata (BUS:BUS), LSO Interlude (SOF:SOF), LSO Legato (BUS:SOF), LSO Presto (SOF:ICM), and LSO ADAGIO (ICM:ECM). Detailed information on the APIs and associated SDKs for the respective reference points can be found in [i.185].

The MEF Reference Architecture and Framework [i.57] also provides eight open and interoperable management capabilities, that is, LSO Analytics, LSO Assurance, LSO Control, LSO Fulfillment, LSO Performance, LSO Policy, LSO Security, and LSO Usage. Detailed information on these LSO Capabilities can be found in [i.186].

5.8 3GPP SA2

5.8.1 5G Network Automation relevant to ZSM in 3GPP SA2

NetWork Data Analytics Function (NWDAF) is introduced in the 5G phase1 to automatically provide slice specific network data analytics to the network. In Rel15, NWDAF only notifies or publishes slice specific network status analytic information to the PCF(s) that are subscribed to it.

However, other network functions may also benefit from NWDAF reporting. In order to improve the NWDAF related work initiated in Release 15, the work in 3GPP TR 23.791 [i.59] further investigates solutions for supporting network automation deployment with information exposure across technical domains for context mining.

The objective of the work includes:

- Specify architecture enhancements for 5G System to support network data analytics service.
- Specify framework to enable data collection and provide analytics to consumers.
- Define extensions to existing Nnwdaf services to support the analytics that are required for e.g. QoS Profile Provisioning, Traffic Routing, Future Background Data Transfer, Slice SLA, Performance Improvement and Supervision of mIoT Terminals, Support of Northbound Network Status Exposure and Customizing Mobility Management.

As specified in ETSI TS 123 501 [i.60] and ETSI TS 123 503 [i.61], the NWDAF represents operator managed network analytics logical function to provide slice specific network data analytics to the 5GS Network Functions on network slice instance level. NWDAF notifies slice specific network status analytic information to the 5GS NFs that are subscribed to it, and the 5GS NFs decide how to use the data analytics provided by NWDAF to improve the network performance.

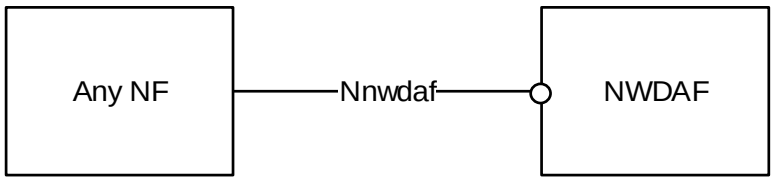


Figure 5.8.1-1: Network Analytics architecture
(source: from ETSI TS 123 501 [i.60])

As shown in Figure 5.8.1-1, the 5G System architecture allows any network functions (such as PCF, NSSF) to request network analytics information from NWDAF via the Nnwdaf interface exhibited.

As specified in ETSI TS 123 503 [i.61], the PCF may collect directly slice specific network status analytic information (i.e. load level information) from NWDAF in its policy decisions. NSSF may use the load level information for slice selection.

3GPP TR 23.791 [i.59] studies the necessary data to expose to NWDAF and the necessary NWDAF outputs (i.e. statistics/prediction) in order to e.g. support (non-exhaustive list):

- Customized mobility management per UE e.g. paging enhancements and mobility pattern.
- 5G QoS enhancement e.g. 5G QoS target fulfilment verification and QoS profile for non-standardized 5QI.

- Dynamic traffic steering and splitting, UPF selection, UE traffic routing policies based on UE's service usage behaviour.

Figure 5.8.1-2 shows general framework for 5G network automation in Release 16, depicting that the NWDAF should be able to collect data from the operator OAM, AFs and 5GC network functions to contribute to consistent policies, analytics output results, and finally decision-making.

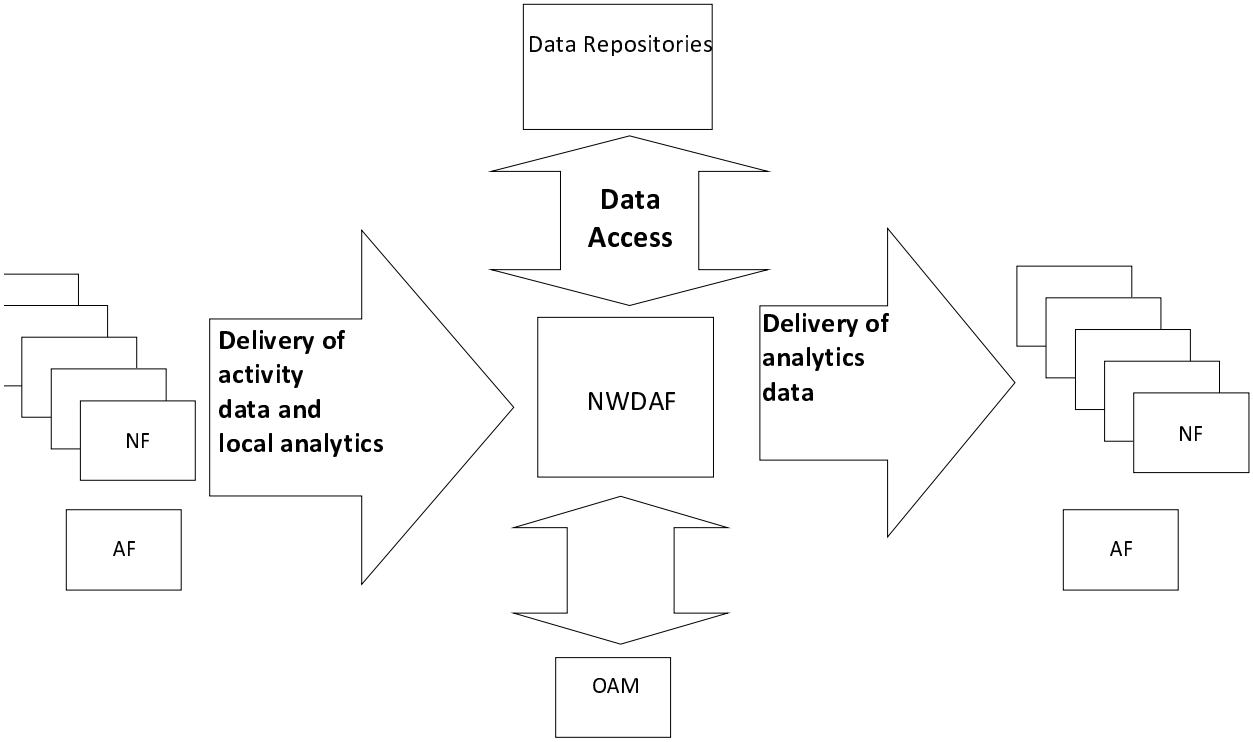


Figure 5.8.1-2: General framework for 5G network automation
(source: from 3GPP TR 23.791 [i.59])

NWDAF can interact with OAM, AF and NF in exchange of information. NWDAF can also access network data from data repositories (e.g. UDR).

Based on the data collected, the NWDAF performs data analysis and provides the analytical result to the AF, the 5GC NFs and the OAM. The NWDAF may serve use cases belonging to one or several domains, e.g. QoS, traffic steering, dimensioning, security. The input data of the NWDAF may come from multiple sources, and the resulting actions undertaken by the consuming NF or AF may concern several domains (e.g. Mobility management, Session Management, Policy management, Performance/Event management, SLA/QoS management, Application layer, Security management, NF life cycle management).

5.8.2 5G Service-Based Architecture relevant to ZSM in 3GPP SA2

The Service-Based Architecture (SBA) helps to improve the deployment agility, re-use of services, flexibility for network slicing, and automation in meeting SBA principles and concepts, in satisfying the related 5G system requirements, and in achieving Continuous Integration and Continuous Delivery (CI/CD) through modularized independent "NF services".

In 3GPP TR 23.742 [i.62], it studies and evaluates architecture enhancements on potential optimizations to the R15 SBA in order to provide higher flexibility and better modularization of the 5G System for the easier definition of different network slices and to enable better re-use of the defined services. The mechanisms to better support automation and high reliability of network function service(s) are also considered.

The following aspects are covered in the report:

- Optimizing the modularization of the system to improve its agility.

- Extending the service concept from 5GC control plane to the user plane function(s).
- Further improvements to service framework related aspects.
- Architectural support for highly reliable deployments, considering.
- Study backward and forward compatibility implications resulting from the above bullets.

The extension of NWDA and the automation requirements to the SBA in Release 16 need be further investigated by ZSM to identify the relevance to the work in ZSM, and potential cooperation and coordination may be conducted between 3GPP SA2 and ZSM in the future.

5.9 3GPP SA5

5.9.1 Performance Management relevant to ZSM in 3GPP SA5

3GPP SA5 specifies the management of performance measurements and the collection of performance measurement data for 5G mobile networks that include virtualised network functions. The administration of measurement schedules, the generation of measurement results and the transfer of these results are also specified.

The performance data can be collected in real-time and used by analytic applications (e.g. network optimization, SON, etc.) to detect the potential issues in advance, and to take appropriate actions to prevent or to mitigate the faults or performance issues.

In ETSI TS 128 521 [i.63], it specifies the Performance Management procedures for mobile networks that include virtualised network functions.

In ETSI TS 128 532 [i.82], it specifies the stage 2 and stage 3 of generic performance assurance management service for mobile network, which includes the supported operations and notifications, and the managed information.

In ETSI TS 128 550 [i.64], it specifies the management services related to performance assurance for 5G networks including network slicing. The concept, supported PM services, use cases and requirements for PM for 5G networks and network slicing are specified.

In ETSI TS 128 552 [i.65], it specifies the performance measurements and the related KPIs for 5G networks (e.g. NG-RAN and 5GC) including 5G network and E2E network slicing. The Performance Indicators are the performance data aggregated over a group of NFs, which can be derived from the performance measurements collected at the NFs that belong to the group.

In ETSI TS 128 554 [i.66], it specifies end-to-end Key Performance Indicators (KPIs) for the 5G network and network slicing. The following end to end KPI categories are or will be included:

- accessibility;
- integrity;
- utilization;
- retainability;
- availability;
- mobility.

5.9.2 Fault Management relevant to ZSM in 3GPP SA5

3GPP SA5 specifies the Fault Management (FM) of mobile networks that include virtualised network functions. The functionality of FM include fault detection, generation of alarms, clearing of alarms, alarm forwarding and filtering, storage and retrieval of alarms, correlation of alarms and events, alarm root cause analysis and fault recovery.

In ETSI TS 128 515 [i.67], ETSI TS 128 516 [i.68], ETSI TS 128 517 [i.69] and ETSI TS 128 518 [i.70], the set specifications specify the requirements, procedures, and specifications applicable to Fault Management (FM) of mobile networks that include virtualised network functions.

In ETSI TS 128 545 [i.71], it specifies use cases and requirements for fault supervision of 5G networks and network slicing.

In ETSI TS 128 532 [i.82], it specifies the stage 2 and stage 3 of generic fault supervision management service for mobile network, which includes the supported operations and notifications, and the managed information.

5.9.3 Configuration Management relevant to ZSM in 3GPP SA5

3GPP SA5 specifies the Configuration Management (CM) of virtualised network functions.

In ETSI TS 128 510 [i.72], ETSI TS 128 511 [i.73], ETSI TS 128 512 [i.74] and ETSI TS 128 513 [i.75], the set specifications specify the requirements, procedures, stage 2 and stage 3 specifications applicable to Configuration Management (CM) of virtualised network functions.

5.9.4 Network Policy Management relevant to ZSM in 3GPP SA5

3GPP SA5 specifies the policy management for mobile network based on NFV scenarios.

In ETSI TS 128 311 [i.76], it contains the architecture, requirements, use cases, procedures and definitions of interfaces for policy management. 3GPP management system would use the ETSI NFV defined related policy features/services to delegate the support of policy control for virtualised NFs such as automatic scale in/out under certain condition.

In 3GPP TR 32.871 [i.77], it studies the end-to-end network policy management for mobile network based on NFV scenarios, including the concepts and classification, use cases and requirements, policy management architecture, and potential solutions to the policy management for mobile networks based on the NFV scenarios.

In ETSI TS 123 503 [i.61], it defines the Stage 2 policy and charging control framework for the 5G System, including the following high level functions: flow based charging for network usage, policy control for session management and service data flows, management for access and mobility related policies, and management for UE access selection and PDU Session selection related policies.

5.9.5 Intent Driven Management relevant to ZSM in 3GPP SA5

3GPP SA5 studies Intent Driven Management (IDM) service for mobile network as it can help reduce the complexity of network and service management with automation mechanisms, by allowing its consumer the ability to provide desired intent for managing the 5G network and service. The IDM service provider translates the intent to appropriate network deployment information and implements it automatically.

After study phase, the work item will be initiated with the objective to document the intent driven management services of 5G networks by specifying the following aspects:

- Specify the typical management scenarios which operators could benefit from the intent driven management services in the multiple vendor environment. The scenarios should help to improve the multiple vendor operational efficiency on network management.
- Specify the intent driven management services' requirements which are derived from the scenarios above.
- Specify the intent driven management services which may include the management operations, management entities and management information.

In 3GPP TR 28.812 [i.78], it describes the levels of automation, intent driven management concept, intent driven management scenarios, and recommendation for the way forward on standardization expression of the intent in normative phase.

Intent Driven Management (IDM) is also an important automation mean considered in ZSM which can help to alleviate the complexity of network and service management. Further investigation is necessary to identify the relevance to the work in ZSM, and potential cooperation may be required between 3GPP SA5 and ZSM.

5.9.6 Self-Organization Network relevant to ZSM in 3GPP SA5

SON automation is important for operators to manage the complicated 5G networks, especially in maintaining the optimal performance efficiency. 5G SON consumes management data, including alarms, measurements, analytical KPIs, QoE, and provisioning data to analyse the network behaviour, status, and traffic pattern, based on time and locations, to predict the potential issues, and to plan a solution in advance to resolve the issues before happening. With the advances of AI and big data, 5G SON is able to process the huge number of management data collected over days, weeks, months and beyond to create self-optimization, self-configuration, and self-healing actions needed to improve network performance and efficiency.

5G SON may reuse SON features developed prior to Release 16 (e.g. automatic neighbour relation, capacity and coverage optimization, load balancing, cell outage compensation, interference control, etc.) if deemed appropriate, and will study use cases specific to 5G networks. It may cover optimization of RAN, CN, network slicing, and of the end-to-end service quality.

The objectives of the 5G SON work include:

- Study the use cases and requirements for the SON to control the 5G networks based on the analysis of both network data and management data. The following aspects of RAN and CN will be studied: Self-configuration/reconfiguration, Self-optimization, Self-healing.
- Study the use cases and requirements for SON related to network slicing.
- Study the solutions to support the above requirements.

In 3GPP TR 28.861 [i.79], it comprises the use cases, potential requirements and potential solutions of SON for mobile networks. Based on the location of the SON algorithm, SON is categorized into centralized SON, distributed SON and hybrid SON. Self-configuration/reconfiguration, self-optimization, and self-healing are also the important capabilities that need be supported by SON.

5.9.7 Management and Orchestration relevant to ZSM in 3GPP SA5

In ETSI TS 128 530 [i.80], the aspects relevant to the network management and orchestration for 3GPP networks including network slicing are specified: concept, use cases, requirements, and architecture. Two business models of network slicing are proposed: Network Slices as NOP internals, and Network Slice as a Service (NSaaS).

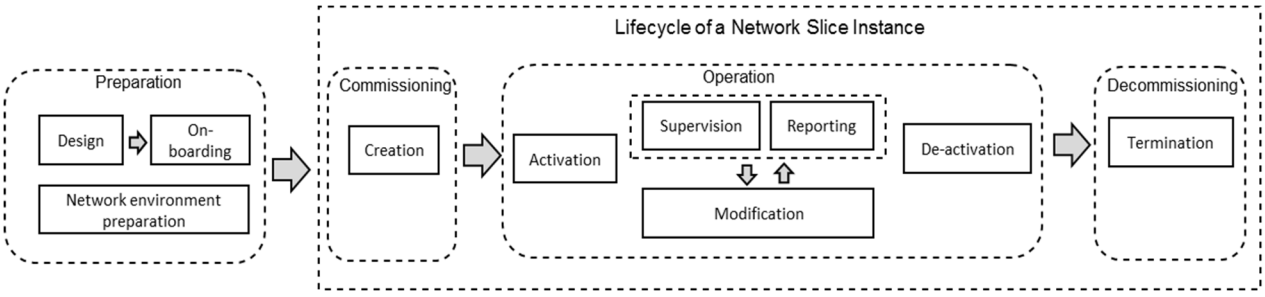


Figure 5.9.7-1: Management aspects of network slice instance
(source: from ETSI TS 128 530 [i.80])

In ETSI TS 128 531 [i.81], it specifies the use cases, requirements, and solutions to enable the provisioning of 5G networks and network slicing, including the life cycle management of network slices as well as network slice subnets.

In ETSI TS 128 532 [i.82], it specifies the stage 2 and stage 3 of generic management services for mobile network, including the generic provisioning management service, the generic fault supervision management service, and the generic performance assurance management service.

In ETSI TS 128 533 [i.83], it specifies the management services and the offered service capabilities, reference models of the management architecture framework.

In ETSI TS 128 540 [i.84], it specifies the requirements for the Network Resource Model (NRM) definition of NR, NG-RAN, 5G Core Network (5GC) and network slice.

In ETSI TS 128 541 [i.85], it specifies the Information Model and Solution Set for the Network Resource Model (NRM) definitions of NR, NG-RAN, 5G Core Network (5GC) and network slice, to fulfil the requirements identified in ETSI TS 128 540 [i.84].

In 3GPP TR 28.801 [i.86], it investigates and makes recommendations on management and orchestration for network slicing. The concepts, use cases, potential requirements and solutions are identified and included for management and orchestration of network slices. Three management functions are identified in management and orchestration of network slicing: the CSMF, the NSMF, and the NSSMF.

The Fault Supervision is also Management and Orchestration related, which is specified in ETSI TS 128 545 [i.71] in clause 5.9.2.

The Performance assurance is also Management and Orchestration related, which is specified in ETSI TS 128 550 [i.64], 5G performance measurements ETSI TS 128 552 [i.65] and 5G end to end Key Performance Indicators (KPI) ETSI TS 128 554 [i.66] in clause 5.9.1.

The PM, FM, CM, Network Policy Management, IDM, SON, Management and Orchestration work in 3GPP SA5 need be further investigated by ZSM to identify the relevance to the work in ZSM, and potential cooperation may be conducted between 3GPP SA5 and ZSM.

5.10 ONF

5.10.1 CORD Platform relevant to ZSM in ONF

The Central Office Re-architected as a Datacentre (CORD) platform [i.87] leverages SDN, NFV and Cloud technologies to build agile datacentres for the network edge where operators connect their customers to their network and deliver the best end-user experience along with innovative next-generation services. Integrating multiple open source projects, CORD delivers a cloud-native, open, programmable, agile platform for network operators to create innovative services.

The CORD Hardware Architecture is composed by Commodity Servers which interconnected by a fabric of white-box switches, switching fabric in a spine-leaf topology for optimized East-to-West traffic, and specialized access hardware for connecting subscribers (residential, mobile and/or enterprise).

CORD is currently packaged into 3 solutions for different market use cases to support emerging edge applications like IoT, Gaming, VR, etc.:

- R-CORD [i.88]: supporting residential subscribers over wireline access technologies like GPON, G.Fast, 10GPON, and DOCSIS.
- M-CORD [i.89]: a distribution supporting 5G mobile edge services complete with disaggregated and virtualised radio (RAN) and an open source Mobile Core (EPC).
- E-CORD [i.90]: enterprise services such as virtual private networks (VPNs) and application optimization (SD-WAN) over metro and wide area networks.

Residential CORD (R-CORD) [i.88] is an open source solution based on the CORD platform for delivering ultra-broadband residential services. R-CORD transforms the edge of the operator's network into an agile service delivery platform enabling the operator to deliver the best end-user experience along with innovative next-generation services. Various access technologies can be used including: GPON, G.Fast, 10GPON, and DOCSIS.

R-CORD can bring benefits for residential services, such as control subscriber access, monitor resource usage, and diagnose problems.

Mobile CORD (M-CORD) [i.89] is an open source reference solution for carriers deploying 5G mobile wireless networks. It is a cloud-native solution built on SDN, NFV and cloud technologies, and includes both virtualisation of RAN functions and a virtualised mobile core (vEPC) to enable multi-access edge applications and innovative services using a micro-services architecture. M-CORD transforms the mobile network by disaggregating and virtualizing cellular network functions as well as operator specific services.

The re-architecting of mobile infrastructure can bring benefits for 5G Networks, such as enhanced resource utilization, providing customized services and differentiated QoE to customers, agile and cost-efficient deployment leveraging commodity hardware and open source software.

Enterprise CORD (E-CORD) [i.90] builds on the CORD platform to create a cloud-native solution for delivering services to enterprise customers. Rather than deploying purpose-built equipment on the customer site or in the operator's network, E-CORD creates a nimble solution blending Cloud, SDN and NFV technologies into a cohesive solution where virtualised functions can be deployed where they make sense.

E-CORD is disruptive to cloud-based Enterprise Services with the benefits, such as Zero touch virtual networks, strong SLAs/QoS for enterprise traffic, built-in analytics, and based on commodity hardware and open source software.

NOTE: If part of the end-to-end network service can be deployed in the CORD platform, it can be integrated into or cooperate with ZSM management domain to provide support for the end-to-end network service management. But further investigation is required to check how the automation related requirements identified in ZSM can be satisfied in the CORD platform.

5.10.2 Information Modeling relevant to ZSM in ONF

5.10.2.1 General

The Open Information Models and associated open source tooling software developed in ONF help to guide/support the development of software-defined standard platforms, frameworks and interfaces used to control/manage/orchestrate Software Defined Networks.

This work can be leveraged by partner SDOs (such as MEF, OASIS-TOSCA, ITU-T, TMF and ETSI-NFV) in their information models and tool chain to facilitate industry convergence and federation to avoid needless fragmentation in the SDN/NFV/Cloud/Transport space.

5.10.2.2 CoreModel

ONF Core Information Model (CoreModel) specified in TR-512 [i.91] provides a representation of network forwarding resources from a management-control perspective. It focuses on representation of the functions/resources that have the primary purpose of supporting information forwarding (transfer and transform functions). Those resources are referred to as network forwarding resources.

The CoreModel consists of model artefacts that are intended for use by multiple applications and/or forwarding technologies.

The CoreModel is independent of:

- Specific forwarding technology, i.e. the CoreModel is forwarding technology neutral.
- Specific management-control interface protocol, i.e. the CoreModel is management-control interface protocol neutral (as described in ONF TR-513 [i.94]).

5.10.2.3 UML

ONF UML Modelling specified in TR-514 [i.92] defines a number of basic model elements (UML artefacts) to describe the structural part and a behavioural features of an information model. The structural modelling is using Attributes (Properties) contained in Classes and the behavioural modelling is using Operations contained in Interfaces. The goal of UML Modelling is to develop guidelines and tools for a harmonized modelling infrastructure that is not specific to any SDO, technology or management protocol and can then be used by all SDOs.

5.10.2.4 Papyrus

Papyrus Guideline specified in TR-515 [i.93] defines the guidelines that have to be taken into account during the creation of a protocol-neutral UML information model using the Open Source tool Papyrus. The goal of Papyrus is to develop guidelines and tools for a harmonized modelling infrastructure that is not specific to any SDO, technology or management protocol and can then be used by all SDOs.

5.10.2.5 ONF-CIM

ONF Common Information Model (ONF-CIM) specified in TR-513 [i.94] describes the things in a domain in terms of objects, their properties (represented as attributes), and their relationships that are necessary to describe the domain for the applications being developed.

The ONF-CIM is expressed in UML language which defines a number of basic model elements, called UML artefacts.

NOTE: ZSM architecture is based on model-driven approach to perform the management of services and resources through the use of information models. The protocol-neutral information modelling tools developed in ONF can be referenced by ZSM for designing the architecture and interfaces.

5.10.3 Intent based Networking

Intent NBI is a declarative paradigm/methodology for interaction between service consumers and service providers. As specified in TR-523 [i.95], the objective is to describe that paradigm, its utility and properties, and its nominal implementation structure.

Benefits brought by Intent NBI include:

- An Intent NBI request is non-prescriptive with respect to detailed provider implementation of a request.
- An Intent NBI request is independent of provider implementations and their operational policies.
- The Intent NBI paradigm is universal, in the sense that it is always possible for a consumer to express its service requirements in Intent NBI paradigm-compatible terms.
- Intent NBI may mitigate resource allocation conflicts that otherwise might arise among concurrent consumer service requests to a given provider.
- Intent NBI requests may be composable, in the sense that Intent NBI requests may represent the effective sum of multiple specific inputs.
- Intent-based systems may be more secure than prescription-based systems.

ZSM need further investigate the platforms and information models provided by ONF to identify the potential implementations, especially in supporting (part of) the E2E network and service deployment, the model-driven and open interfaces principle applied to ZSM framework.

5.11 ITU-T SG 13

5.11.1 Machine learning relevant to ZSM in ITU-T SG 13

ITU-T Study Group 13 established a new Focus Group on Machine Learning for Future Networks including 5G (FG-ML5G) at its meeting in Geneva, 6-17 November 2017. The FG-ML5G has accomplished its mission in July 2020 at the SG13 meeting, and approved ten technical specifications on use cases [i.97], architectural framework [i.98], framework for evaluating the intelligence levels [i.99], framework for data handling to enable machine learning [i.100] of future networks including IMT-2020.

As documented in FG-ML5G ToR [i.96], the machine learning methods applied in communication networks can help to improve network performance and enhance user's experience by extracting relevant information from the network data, and then leveraging the learning results for autonomic network orchestration and management as well as service provisioning. The Focus Group will provide a platform to study and advance the various machine learning approaches for future networks including 5G.

As documented in ITU-T Y.Sup55 [i.97], it describes use cases of machine learning in future networks including IMT-2020. The use cases are classified into five categories as network slice and other network service related, user plane-related, application-related, signalling or management related, and security related. For each use case, the requirements are further classified into those for data collection, data storage and processing, and application of ML output.

FG ML5G also worked on enabling technologies for AI/ML in networks like ML marketplace integration Recommendation ITU-T Y.3176 [i.101], Serving framework ML5G-O-036 [i.197], Sandbox ML5G-O-035 [i.196], ML Function Orchestrator (MLFO) ML5G-O-037 [i.198], and vertical QoE-aware network slice management ML5G-O-039 [i.200].

In addition, FG ML5G also produced an information document ML5G-O-034 [i.195] which captures the next steps and gaps from the current state of the art in integrating ML in future networks including IMT-2020. The gaps identified include:

- GAP 1: Standard set of tools and APIs for data handling:
  - Varied ML use cases in networks uses varied data sources which may have varied data formats. The "lack of standards" in this area remains a problem. ML5G recommend ITU-T to setup machine learning metadata store in ML Sandbox for the data models of the ML pipeline.
- GAP 2: Federated pooling of data and metadata:
  - Use case requirements and problems faced by different operators are similar, so the machine learning database and machine learning metadata store can be shared across ML use cases. A wider, standard mechanism is needed for operators to collaborate and solve the data/models sharing.
- GAP 3: Privacy preserving mechanisms for learning in federated networks:
  - The levels of data/models sharing can be negotiated and selected by operators. Privacy policies can be used by operators to control the data/models sharing.
- GAP 4: Automated capturing of use cases:
  - For easily automating the processing of ML intent based use cases in networks, the requirements of the use cases can be analysed and classified and clustered, then suitable models for the deployment of ML pipeline for the use case can be selected.
- GAP 5: Application of ML model metadata:
  - ML model metadata describes the characteristics of a machine learning model, which can be used in selection, training and indicating the resource requirements of the ML model.
- GAP 6: Integration of verticals and network slices:
  - There are no standard mechanisms for cross-domain ML pipeline management, so it is difficult to seamlessly apply ML pipelines across slices, operator underlay and NFVO.
- GAP 7: AI/ML trade-offs in network:
  - Propose guidance or best practices for evaluating the trade-offs on network bandwidth, CPU/GPU consumption, latency of performing the inferences while integrating AI/ML in the networks.

5.11.2 Architectural framework for machine learning in future networks

An architecture framework for integration of AI/ML in future networks including IMT-2020 [i.98] has been derived from the use cases documented in Recommendation ITU-T Y.Sup55 [i.97]. Extensions to this architecture framework have been delivered in the form of Recommendation ITU-T Y.3173 [i.99] and Recommendation ITU-T Y.3174 [i.100].

Recommendation ITU-T Y.3172 [i.98] specifies an architectural framework for Machine Learning (ML) in future networks including IMT-2020. A set of architectural requirements is presented, which in turn leads to specific architectural components needed to satisfy these requirements. This Recommendation also describes an architectural framework for the integration of such components into future networks including IMT-2020 and guidelines for applying this architectural framework in a variety of technology-specific underlying networks.

The components contained in the high-level architectural [i.98] include:

- Machine learning pipeline, a set of logical nodes, each with specific functionalities, which can be combined to form a machine learning application in a telecommunication network. Nodes of an ML pipeline may include source, collector, pre-processor, model, policy, distributor, and sink.

- Machine Learning Function Orchestrator (MLFO), a logical node with functionalities that manage and orchestrate the nodes of ML pipelines based on ML Intent and/or dynamic network conditions.
  The deliverable of ML5G-O-038 [i.199] describes an architecture and design for the MLFO based on the requirements derived from the use cases in future networks including IMT-2020.

- ML sandbox, an isolated domain which allows the hosting of separate ML pipelines to train, test and evaluate them before deploying them in a live network. For training or testing, the ML sandbox can use data generated from simulated ML underlay networks and/or live networks.
  The deliverable of ML5G-O-035 [i.196] defines the architecture of the ML Sandbox to improve the level of confidence in ML solutions before their application to the network infrastructure. It deals with the requirements, architecture, and implementation examples for ML Sandbox in future networks including IMT-2020.

The extension of architecture framework on evaluating intelligence levels can be found in Recommendation ITU-T Y.3173 [i.99].

The extension of architecture framework on data handling to enable machine learning can be found in Recommendation ITU-T Y.3174 [i.100]. It specifies a flexible approach based on data broker and base lined data models to tackle the varied data formats issue.

NOTE 1: The integration of ML pipeline with ZSM framework would enable ZSM in implementing (E2E) Domain intelligence services to generate decision, in which case ZSM can be regarded as the ML underlay networks to provide source of data and to take actions to/from ML pipeline. ZSM can also provide support to manage ML pipeline as a managed entity, especially when it crosses management domains.

NOTE 2: The machine learning methods (including interfaces, architectures, protocols, algorithms, and data formats) developed by FG-ML5G can be leveraged by ZSM to enhance the intelligence for network and service management.

5.11.3 Autonomous Networking relevant to ZSM in ITU-T SG 13

ITU-T Focus Group on Autonomous Networks (FG-AN) [i.238] was established by ITU-T SG13 at its virtual meeting, 17 December 2020. FG-AN will draft technical reports and specifications for autonomous networks, including exploratory evolution in future networks, real-time responsive experimentation, dynamic adaptation to future environments, technologies, and use cases. FG-AN will also identify relevant gaps in the standardization of autonomous networks.

Three working groups are established for FG-AN during the meeting:

- WG1: Use Cases and Requirements Analysis.

- WG2: Architecture and Core Technical enablers.

- WG3: Proof of Concepts.

As documented in FG-AN ToR [i.239], FG-AN will serve as an open platform for pre-standard study on autonomous networks enabling collaboration between experts in the ITU, other SDOs, industry, and academia. FG-AN will explore creative intelligence techniques that leverage online evolution mechanisms, enabling adaptation as a catalyst to achieve autonomous networks, and will explore and study approaches such as exploratory evolution, emergent behaviour, and real-time responsive experimentation to enable an autonomous network.

FG-AN will develop following tasks and deliverables:

- **Gap analysis:** To study existing initiatives related to autonomous networks, identify existing standards in other SDOs, and call out the additional work needed to adopt the key concepts (evolution, creativity, adaptation and online exploration, etc.) in autonomous networks.

- **Definitions glossary:** To promote the harmonization of terminologies and taxonomies for autonomous networks and the relevant eco-system needed for standardization.

- **Use case analysis:** To study and identify use cases for autonomous networks, with emphasis on the key concepts, in the context of future networks.

- **Requirements and architecture deliverable:** To study and specify possible requirements, architectures of autonomous networks.

5.12 IETF/IRTF

5.12.1 Network Management relevant to ZSM in IETF

5.12.1.1 Autonomic Networking Integrated Model and Approach (ANIMA)

The ANIMA Working Group in Operations and Management Area is developing specifications and supporting documentation for interoperable protocols, implementations and operational procedures for automated network management and control mechanism for networks that are developed, build and operated by professional personnel.

As specified in the charter [i.102] of ANIMA WG, the autonomic networking refers to the self-managing characteristics (configuration, protection, healing, and optimization) of distributed network elements, adapting to unpredictable changes while hiding intrinsic complexity from operators and users. Autonomic Networking, which often involves closed-loop control, is applicable to the complete network (functions) lifecycle (e.g. installation, commissioning, operating, etc.).

Autonomic function solves the challenges of no common infrastructure for distributed functions which leads to inefficiencies, and management and optimization of operational device configurations which are always expensive, tedious, and prone to human error. So, the general objective of autonomic function is to enable the progressive introduction of autonomic functions into operational networks, as well as reusable autonomic network infrastructure, in order to reduce the OPEX.

The autonomic functions can carry out the intentions of the network operator without the need for detailed low-level management of individual devices by providing a secure closed-loop interaction mechanism whereby network elements cooperate directly to satisfy management intent.

The initial scope of autonomic function is to develop a minimum set of specific reusable infrastructure components to support autonomic interactions between devices, and to specify the application of these components to one or two elementary use cases of general value. Future work may include a more detailed systems architecture to support the development of autonomic service agents.

The framework and components developed by ANIMA is documented in [i.110].

The components developed in the ANIMA framework constitute the Autonomic Networking Infrastructure (ANI): Autonomic Control Plane (ACP) in [i.111], Bootstrap over Secure Key Infrastructures (BRSKI) [i.112] including the concept of Vouchers [i.113], and Generic Autonomic Signalling Protocol (GRASP) [i.114] and its APIs [i.115].

The focus relevant to ZSM in ANIMA includes close-loop control of automatic networking, resource management, Intent (high level policy), tie in to ML/AI techniques, ANI OAMP (Operations, Administration, Management, and Provisioning) interfaces, Autonomic Slice Management, Autonomic SLA management/assurance.

The work on automatic networking can be leveraged by the domain control of ZSM for network functions and resources management.

5.12.1.2 Network Configuration (NETCONF)

The NETCONF Working Group [i.126] and [i.127], in Operations and Management Area is responsible for the development and maintenance of protocols such as NETCONF and RESTCONF for YANG data model-driven management (for the purposes of, for example, configuration, monitoring, telemetry, and zero-touch), their transports and encodings, defining data models necessary to support the protocols, and defining mechanisms supporting the operational deployment of systems using the protocols.

As specified in IETF RFC 6241 [i.116], the NETCONF protocol provides mechanisms to install, manipulate, and delete the configuration of network devices.

As specified in IETF RFC 8040 [i.117], the RESTCONF protocol describes an HTTP-based protocol that provides a programmatic interface for accessing data defined in YANG, using the datastore concepts defined in the NETCONF [i.116].

As specified in [i.118], it extends the NETCONF protocol defined in IETF RFC 6241 [i.116] in order to support the Network Management Datastore Architecture (NMDA) defined in IETF RFC 8342 [i.120].

As specified in [i.119], it extends the RESTCONF protocol defined in IETF RFC 8040 [i.117] in order to support the Network Management Datastore Architecture (NMDA) defined in IETF RFC 8342 [i.120].

Series of notification specifications related NETCONF are also specified in NETCONF WG [i.103], such as event notification in [i.121], notification capabilities in [i.122], notification messages in [i.123], RESTCONF notification in [i.124], notification subscription in [i.125], etc.

The Generalized Network Control Automation (GNCA) specified in [i.128] aimed to define an abstract and uniform semantics for NETCONF/YANG scripts in the form of Event-Condition-Action (ECA) containers to enable an environment allowing for manipulation of close loop network automation via configuration of abstract ECA scripts.

The work on network configuration can be leveraged by ZSM for enhancing the automation of network service management and also for the configuring the management entities in ZSM framework architecture.

5.12.1.3 Network Modeling (NETMOD)

The NETMOD Working Group [i.104] in Operations and Management Area is responsible for the YANG data modelling language, which can be used to specify network management data models that are transported over such protocols as NETCONF and RESTCONF, and guidelines for developing YANG models.

As specified in IETF RFC 7950 [i.129], the YANG data model can be applied for many aspects in network and service management, such as configuration of a syslog process [i.130], model configuration and state data manipulation [i.131], content (data and operations) carried via NETCONF [i.132], management of network interfaces [i.133], system management [i.134], SNMP configuration [i.135], event management [i.136], notifications [i.137], etc.

The YANG data model and its applications on network management can be leveraged by ZSM for enhancing the automation of network service management.

5.12.1.4 Home Networking

The Home Networking Working Group [i.108] in Internet Area focuses on the evolving networking technology within and among relatively small "residential home" networks. Some relevant trends in homing networking are addressed, such as multiple segments with different routing and security policies, restrictions on incoming connections, service discovery, automatic routing.

As specified in IETF RFC 7788 [i.138], the Home Networking Control Protocol (HNCP) is an extensible configuration protocol to the Distributed Node Consensus Protocol (DNCP), and includes a set of requirements for home network devices. HNCP enables discovery of network borders, automated configuration of addresses, name resolution, service discovery, and the use of any routing protocol that supports routing based on both the source and destination address.

As specified in IETF RFC 7368 [i.139], a general IPv6-based home networking architecture for is defined with the associated principles, considerations, and requirements, and also the need for specific protocol extensions for certain additional functionality.

As specified in [i.140], the draft describes how names are published and resolved on homenets, and how hosts are configured to use these names to discover services on homenets.

Home networking is a special kind of service environment/domain that need to be managed by ZSM if the end-to-end service be partially deployed into such environment. So the home networking specifications can be leveraged by ZSM for the management of home networking domain.

5.12.2 Operations and Management relevant to ZSM in IETF

5.12.2.1 Operations and Management Area (OPSA)

The OPSA Working Group [i.105] in Operations and Management Area serves as the forum for work items relevant to operational and management topics that are not in scope of an existing working group and do not justify the formation of a new working group.

As specified in IETF RFC 5674 [i.148], it describes how to send alarm information in syslog with the mapping of ITU perceived severities onto syslog message fields. It also includes a number of alarm-specific SD-PARAM definitions from X.733 and the IETF Alarm MIB.

As specified in IETF RFC 5675 [i.149], it defines a mapping from SNMP notifications to SYSLOG messages.

As specified in IETF RFC 5676 [i.150], it defines a mapping of SYSLOG messages to SNMP notifications.

As specified in IETF RFC 7276 [i.151], Operations, Administration, and Maintenance (OAM) is a general term that refers to a toolset for fault detection and isolation, and for performance measurement. Over the years, various OAM tools have been defined for various layers in the protocol stack. This RFC summarizes some of the OAM tools defined in the IETF in the context of IP unicast, MPLS, MPLS Transport Profile (MPLS-TP), pseudowires, and TRILL.

As specified in [i.152], the objective of this draft is to illustrate the applicability of framework for network resources categorization through use cases, then discuss the basic methodology and propose a not relatively mature framework for continued supplement and improvement.

As specified in [i.153], it defines a SD-WAN VPN service model to enable a Service Provider to deliver SD-WAN VPN services to its customers by provisioning the CE devices on behalf of the customer.

Some of the work (e.g. syslog, OAM, network resource categorization, SD-WAN VPN service model) covered in OPSA WG can be leveraged by ZSM for enhancing the end-to-end network services management.

5.12.2.2 L2VPN Service Model (L2SM)

The L2SM Working Group [i.106] in Operations and Management Area is to create a YANG data model that describes a L2VPN service (a L2VPN customer service model). The model can be used for communication between customers and network operators, and to provide input to automated control and configuration applications.

As specified in IETF RFC 8466 [i.154], a YANG data model can be used to configure a Layer 2 provider-provisioned eVPN service. It is up to a management system to take this as an input and generate specific configuration models to configure the different network elements to deliver the service.

The L2VPN service model can be leveraged by ZSM for automation of network service management.

5.12.2.3 Application-Layer Traffic Optimization (ALTO)

The ALTO Working Group [i.107] in Transport Area is to devise a request/response protocol for allowing a host to benefit from a server that is more cognizant of the network infrastructure than the host would be. The working group has developed an HTTP-based protocol to allow hosts to benefit from the network infrastructure by having access to a pair of maps: a topology map and a cost map.

ALTO is considered as a solution for data-centre networks and Content Distribution Networks (CDN) where exposing abstract topologies information of Internet Service Provider (ISP) networks to help applications maintaining or improving application performance. Serials of specifications are developed, such as ALTO Problem Statement in IETF RFC 5693 [i.155], ALTO Requirements in IETF RFC 6708 [i.156], ALTO Protocol in IETF RFC 7285 [i.157], ALTO Server Discovery in IETF RFC 7286 [i.158], and ALTO Deployment Considerations in IETF RFC 7971 [i.159], ALTO cross-domain server discovery in [i.160].The network topology information provided by ALTO can be leveraged by ZSM for optimizing the performance of the deployed network services.

5.12.3 Network Management relevant to ZSM in IRTF

5.12.3.1 Network Management Research Group (NMRG)

Network management covered by NMRG [i.109] is to explore solutions on new technologies for the management of the internet, including communication services between management systems, which may belong to different management domains, as well as customer-oriented management services.

As specified in IETF RFC 5345 [i.141], Simple Network Management Protocol (SNMP) is widely deployed for monitoring, controlling, and sometimes also configuring network elements. It describes the motivation, the measurements approaches, tools and data formats needed to carry out large-scale SNMP traffic measurements.

As specified in IETF RFC 8316 [i.142], it describes the application of active measurements mechanisms for the monitoring of SLA violations in a distributed fashion. The experimental use case given in this RFC is to inject active measurement probes into the network to maximize the likelihood of detecting service-level violations.

As specified in IETF RFC 7575 [i.143] and IETF RFC 7576 [i.144], the definitions and design goals, and general gap analysis for autonomic networking are provided. Autonomic networking mainly focuses on node-level autonomic functions with intelligence of algorithms at the node level to minimize dependency on human administrators and central management systems.

As specified in draft-clemm-nmrg-dist-intent-02 [i.145], the draft is intended to clarify the concept of "Intent" and "Intent-Based Networking", and how it relates to other concepts, such as service models, and policies. The goal is to contribute towards a common and shared understanding of terms and concepts which can then be used as foundation to guide further definition of valid research and engineering problems and their solutions. An overview of the concepts of service models, of policies and policy-based management, as well as of intent generally and intent-based management is described. The differences between them are summarized.

As specified in draft-homma-nmrg-slice-gateway-00 [i.146], the draft describes the roles and requirements for a slice gateway for handling data plane traffic, such as connecting/disconnecting and compose/decompose network slice subnets and providing network slices from end to end. The interworking between management and control elements at the management and control planes with the gateway function for controlling and orchestrating end-to-end network slices are also covered in this draft.

As specified in draft-kim-nmrg-rl-05 [i.147], the draft describes intelligent network management system to autonomously manage and monitor by using machine learning techniques. Reinforcement learning is one of the machine learning techniques that can provide autonomously management with multi-agent path-planning over a communication network.

As specified in draft-li-nmrg-intent-classification-01 [i.161], it discusses what intent means to different stakeholders, describes different ways to classify intent, and an associated taxonomy of this classification aiming at the situation that there is no common definition or model of intent. A number of behaviours that serve to further organize the purpose of intent are identified, such as persistence, granularity, abstracting intent operations, policy subjects, policy targets, and policy scope.

As specified in draft-du-anima-an-intent-05 [i.162], one of the goals of autonomic networking is to simplify the management of networks by human operators. Intent Based Networking (IBN) is a possible approach to realize this goal. With IBN, the operator indicates to the network what to do (i.e. her intent) and not how to do it. In the field of Policy Based Management (PBM), the concept of intent is called a declarative policy. This draft proposes a refinement of the intent concept initially defined in IETF RFC 7575 [i.143] for autonomic networks by providing a more complete definition, a life-cycle, some use cases and a tentative format of the ANIMA intent policy.

As specified in draft-liu-anima-intent-distribution-00 [i.163], it describes the requirements of distributing intent information in an autonomic network. Then it resolves the distribution requirements into protocol design requirements.

As specified in draft-moulchan-nmrg-network-intent-concepts-00 [i.164], it presents an overview of the concepts of network intent and provides definitions for some of the nomenclature, such as network configuration, network policy, and network intent. Some use cases are presented to illustrate the concepts introduced in this draft.

As specified in draft-bernardos-nmrg-multidomain-00 [i.165], it analyses the problem of multi-provider multi-domain orchestration, then looking into potential architectural approaches, and finally describing the solutions being developed by the European 5GEx and 5G-TRANSFORMER projects.

NOTE: Basically, the use cases, requirements and the prospective research in NMRG [i.109] can be leveraged by ZSM to avoid duplicate studies, and set a relationship with NMRG [i.109] if additional requirements are identified, such as on automatic network management, intent based orchestration/networking, multi-domain orchestration, network slicing, and network intelligence.

5.13 GSMA

5.13.1 Network Slicing Management relevant to ZSM in GSMA

The GSM Alliance (GSMA) is a telco industry association representing the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader ecosystem. A key recognized activity of GSMA is to collect information on service requirements and regulatory issues from different vertical industry associations (e.g. 5G-ACIA, 5GAA), identify potential technologies that can satisfy these requirements, and inform corresponding SDOs (e.g. 3GPP, ETSI, IETF), so that they can develop corresponding technology solutions. One of the key technologies in this regard is network slicing.

GSMA vision on network slicing was first presented in GSMA WP [i.201]. It was followed by [i.166], where GSMA provided a comprehensive overview about the service requirements on network slicing expressed by business customers from different vertical industries, including AR/VR, automotive, energy, healthcare, manufacturing (I4.0), LPWA, public safety, smart cities, etc. From the analysis conducted in [i.166], GSMA noted that service requirements on network slicing could be classified into performance, functional and control and management requirements. However, it concluded that there was no agreement on how vertical industries should express these requirements towards network operators. In this regard, GSMA agreed on the need to harmonise network slicing definition, identify network slice types with distinct characteristics and consolidate parameter and functionality requirements, from end-to-end perspective.

GSMA work on network slicing management is organized into two main workstreams.

The first workstream has the target to map service requirements from vertical industry use cases into network slice requirements. Based on the conclusions from [i.166], GSMA suggested that it was necessary to develop a solution able to offer verticals guidelines on how to issue service requirements on network slicing towards network operators, therefore addressing the existing gap between vertical and telco industries. To that end, the Generic network Slice Template (GST) has been defined and documented in GSMA PRD NG.116 [i.167]. The GST provides a universal description of a network slice, containing all the potential attributes a network slice could have. It allows the network slice provider and a network slice customer to agree on SLA for a given network slice, by means of filling GST attributes with values based on service requirements. The GSMA Networks Group (NG) is responsible for updating and maintaining GSMA PRD NG.116 GST specification.

ZSM can cooperate with GSMA NG on how to satisfy the slice management related requirements identified in the GST.

The second workstream has the target to provide a deep end-to-end network slice architecture analysis, with the mission of identifying existing gaps and informing corresponding SDOs, fostering cross-standardization collaboration to address these gaps. This activity is also led by the GSMA NG.

ZSM can cooperate with GSMA NG on how to address cross-domain network slice management related issues identified in the end-to-end slicing architecture.

5.13.2 Generic Network Slicing Template

Network slicing is one of the key feature of the 5G networks and enables to build dedicated logical networks on a shared infrastructure. The Generic Network Slice Template (GST) [i.165] specified in GSMA provides the standardized list of attributes that can characterize a type of network slice. These dedicated networks would permit the implementation of tailor-made functionality and network operation specific to the needs of each slice customer, that is, Network Slice Types (NESTs) of a GST filled with a recommended minimum set of attributes and their suitable values.

Figure 5.13.2-1: Void

The GST contains multiple attributes that can be used to characterize a network slice. According to [i.165], GST attributes can be classified into two main categories:

- Character attributes - characterize a network slice. They can be further split into:
  - performance-related attributes, which specify the Key Performance Indicators (KPIs) supported by the slice;
  - functionality-related attributes, which specify the functionality provided by the slice;

  - operation-related attributes, which specify what control and management capabilities are handed over to the vertical in order to operate the slice.

- Scalability attributes - provide information about the scalability of the network slice.

And some detailed attributes are specified for GST that can be used for network slicing instantiation, such as availability, coverage, delay tolerance, deterministic communication, downlink/uplink throughput per network slice/UE, energy efficiency, isolation level.

A Network Slice Type (NEST) describes the characteristics of a network slice by means of mapping specific service requirements to GST attributes.

NOTE: GST and NEST can be leveraged by ZSM to guarantee the Service Level Agreement (SLA) based on customers' requirements in an E2E manner.

5.14 Broadband Forum (BBF)

5.14.1 Transport Network Slice Management relevant to ZSM in BBF

The purpose of the project (SD-406 [i.168]) created by BBF is to investigate the Transport Network Slicing Management (TNSM) from end-to-end perspective supported by the BBF Multi-Service Broadband Network (MSBN) architecture. Transport network slicing is considered as a fundamental enabler to migrate the MSBN architecture from "one architecture fits all" to the logical "network per service".

The transport network slicing use cases can be organized into different types, that is, the Network Service as a Service focusing on fixed networks and the supporting 5G related 3GPP use cases, including also Fixed Mobile Convergence:

- Network Slice as a Service. It enables an on-demand customized fixed broadband network resource leasing business model on the top of a common network infrastructure. The customized logical network can be modified dynamically to suit service demands.
  Requirements that are relevant to ZSM in this use case include network performance, network control and management, flexibility and scalability, SLA/QoS management, service scaling/migration/isolation, multi-domain service deployment, etc.

- Supporting 5G related 3GPP Use Cases. From service management perspective, the identified requirements from 3GPP use cases to MSBN can be seen as a set of link requirements (e.g. topology, QoS parameters, etc.). Such link requirements are communicated to the transport network in order to support connectivity between the 3GPP RAN and/or core networks nodes that belong to the network slice instance, while the 3GPP management system configures the corresponding 3GPP nodes to use such links.

- Slicing across Fixed-Mobile Converged Networks. A Fixed-Mobile Converged (FMC) network slice is built on the top of SD-407 [i.169] by combining resources from both fixed and mobile, i.e. 3GPP, networks, with optimization of service provision and availability by offering various degrees of deterministic performance in terms of throughput, latency, resiliency, etc.

As shown in Figure 5.14.1-1, the processes and operations of Service Management and Network Slice Control supported by MSBN requires a continuous process capable to analyse the service requirements and assure the desired performance even when the conditions of the network change or the requirements from the customer perspective evolve with time.

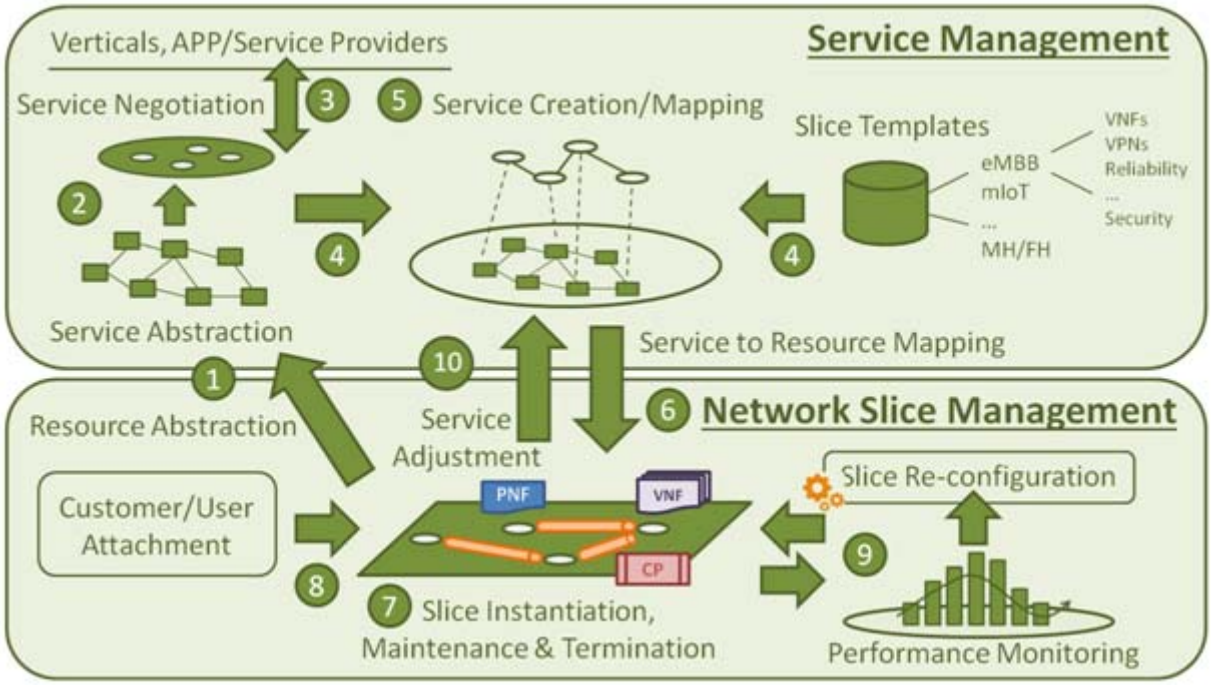


Figure 5.14.1-1: MSBN service management and network slice management processes and operations
(Copyright © The Broadband Forum. All rights reserved.)
(source: from SD-406 [i.168])

The Network Slice Management combined with the Service Management can be regarded as transport management domain which provides capabilities such as service abstraction, service negotiation, service operations, service adjustment, and service template to verticals, application/service providers and 3rd parties for end-to-end service management.

The Transport Network Slice Management (TNSM) documented in [i.168] takes care of the slice life-cycle management of the transport network Sub-Network Slice Instance (S-NSI) and provides the capability exposure of the transport network via Mobile-Transport Network Slice Interface (MTNSI) to the 3GPP mobile network, i.e. towards the network slice management function, while it also provides the mapping of the 3GPP mobile network requirements to the corresponding transport network.

The Transport Network Slice Management in BBF includes service management and network slice orchestration aspects considering the life-cycle management operations, service exposure, and interaction with mobile network and multi- administrative domain support, which can be leveraged by ZSM for end-to-end network slicing management.

5.15 OASIS

5.15.1 Service Management relevant to ZSM in OASIS

OASIS is a non-profit consortium that drives the development, convergence and adoption of open standards for the global information society, which promotes industry consensus and produces worldwide standards for security, Internet of Things, cloud computing, energy, content technologies, emergency management, and other areas.

OASIS has created many Technical Committees. Followings are the list of the technical committees that are identified to be relevant to the work in ZSM:

- Advanced Message Queuing Protocol (AMQP):
  - Defining a ubiquitous, secure, reliable and open internet protocol for handling business messaging. AMQP is a vendor-neutral and platform-agnostic protocol that offers organizations an easier, more secure approach to passing real-time data streams and business transactions, with the goal to ensure information is safely and efficiently transported between applications, among organizations, across distributed cloud computing environments, and within mobile infrastructures. For detailed information, [i.170] can be referenced.
- Cloud Application Management for Platforms (CAMP):
  - Standardizing cloud PaaS management API that cloud implementers can use to package and deploy their applications. CAMP defines interfaces for self-service provisioning, monitoring, and control. For detailed information, [i.171] can be referenced.
- Message Queuing Telemetry Transport (MQTT):
  - Providing a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium. For detailed information, [i.172] can be referenced.
- Open Data Protocol (OData):
  - Simplifying data sharing across disparate applications in enterprise, Cloud, and mobile devices. OData provides a way to break down data silos and increase the shared value of data by creating an ecosystem in which data consumers can interoperate with data producers in a way that is far more powerful than currently possible, enabling more applications to make sense of a broader set of data. [i.173] can be referenced for detailed information.
- SOA Reference Model:
  - Developing a core reference model to guide and foster the creation of specific, service-oriented architectures.
- Topology and Orchestration Specification for Cloud Applications (TOSCA):
  - Enhancing the portability and operational management of cloud and other types of applications and services across their entire lifecycle. For detailed information, [i.174] and [i.175] can be referenced.

TOSCA defines the interoperable description of services and applications hosted on the cloud and elsewhere, including their components, relationships, dependencies, requirements, and capabilities, thereby enabling portability and automated management across cloud providers regardless of underlying platform or infrastructure, thus improving reliability, and reducing cost and time-to-value.

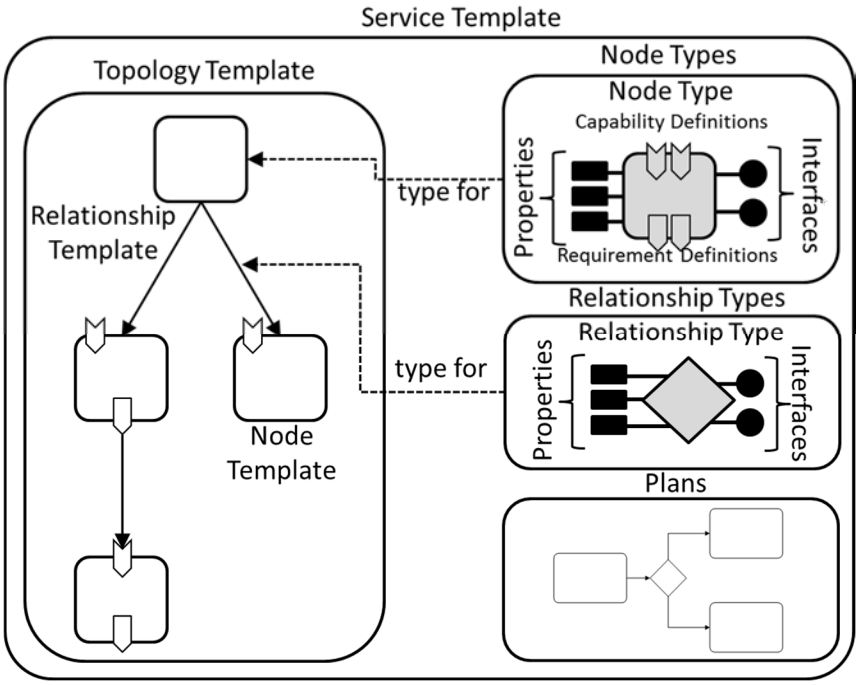


Figure 5.15.1-1: Structural Elements of a Service Template and their Relations
(Copyright © 2021 OASIS®. All Rights Reserved.)
(source: from TOSCA [i.174])

- As depicted in Figure 5.15.1-1, the meta-model can be applied for service definition on the structure of a service as well as how to manage it. A Topology Template defines the structure of a service.
- A Node Template specifies the occurrence of a Node Type as a component of a service.
- A Node Type defines the properties of such a component and the operations available to manipulate the component.
- A Relationship Template specifies the occurrence of a relationship between nodes in a Topology Template.
- Plans define the process models that are used to create and terminate a service as well as to manage a service during its whole lifetime.

The service management protocols related work in OASIS can be leveraged by ZSM to enhance the automation of network and service management in the areas, such as data service management, API implementation and network service orchestration.

5.16 DMTF

5.16.1 Introduction

DMTF (formerly known as the Distributed Management Task Force) creates open manageability standards spanning diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage as show in Figure 5.16.1-1. DMTF standards enable a more integrated and cost-effective approach to management through interoperable solutions, which can be used by industries to improve the interoperable management of information technologies.

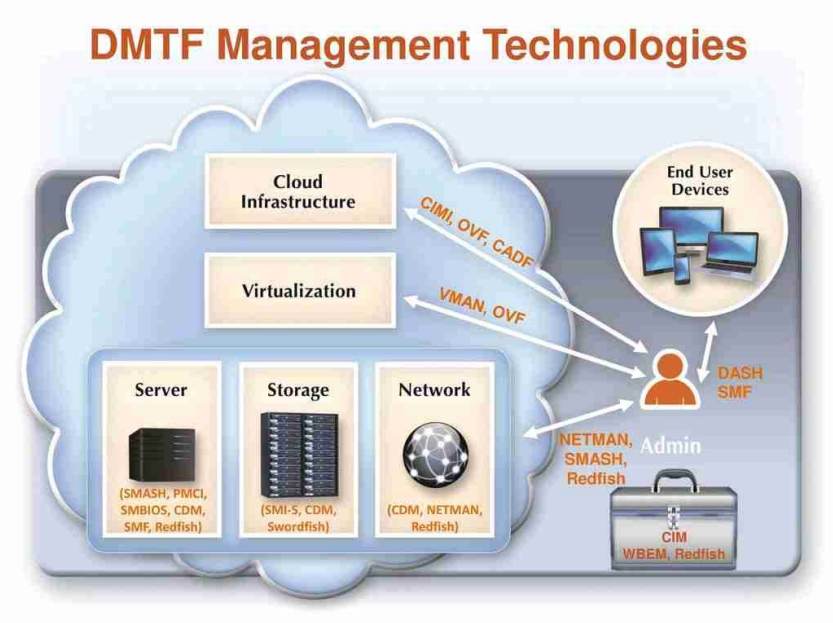


Figure 5.16.1-1: DMTF Management Technologies
(Copyright © 2021 DMTF. All rights reserved.)
(source: from https://www.dmtf.org/standards/stackmap)

DMTF standards provide common management infrastructure components for instrumentation, control and communication in a platform-independent and technology neutral way. The DMTF standards and technologies include:

- CADF - Cloud Auditing Data Federation (DSP0262 [i.232]).
- CDM - Common Diagnostic Model.
- CIMI - Cloud Infrastructure Management Interface (DSP0263 [i.230]).
- CIM - Common Information Model.
- DASH - Desktop & Mobile Architecture for System Hardware.
- MCTP - Management Component Transport Protocol.
- NETMAN - Network Management Initiative.
- NC-SI - Network Controller Sideband Interface.
- OVF - Open Virtualization Format (DSP0243 [i.231]).
- PLDM - Platform Level Data Model.
- PMCI - Platform Management Communications Infrastructure.
- REDFISH® (DSP0266 [i.229]).
- SMASH - Systems Management Architecture for Server Hardware.
- SMBIOS - System Management BIOS.
- SMF - System Management Forum.
- SMI-S - Storage Management Initiative Specification.
- SPDM - Security Protocol and Data Model.
- VMAN - Virtualization Management.
- WBEM - Web-Based Enterprise Management.

- WS-MAN - Web Services Management.

As shown in Figure 5.16.1-2, the DMTF's technologies are designed to work together to address the industry's needs and requirements for interoperable distributed management. These standards listed above provide well-defined interfaces that build upon each other, delivering end-to-end management capabilities and interoperability.

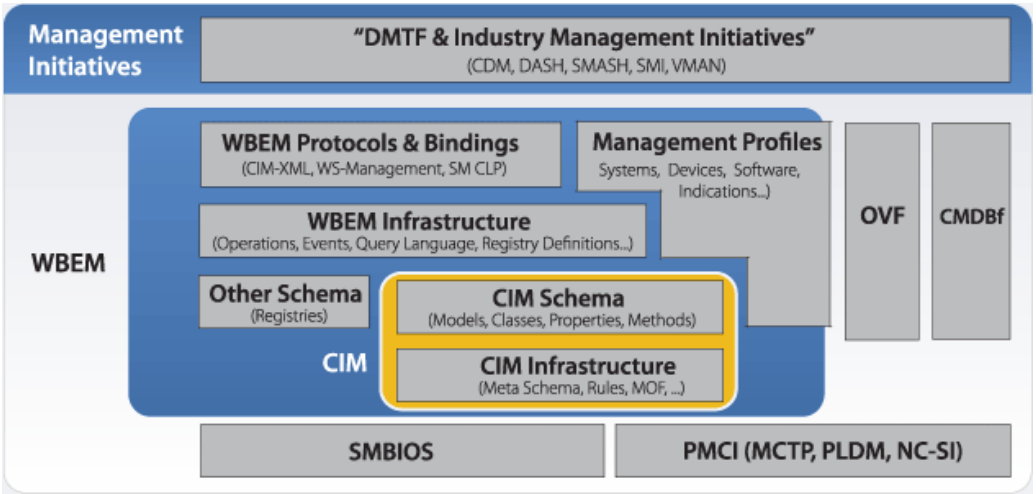


Figure 5.16.1-2: DMTF Technologies Diagram
(Copyright © 2021 DMTF. All rights reserved.)
(source: from https://www.dmtf.org/managementtechnologiesdiagram)

CIM provides the foundation of the DMTF's technologies.

- **CIM Infrastructure** specification defines CIM's "rules" and provides the details for integration with other management models.
- **CIM Schema** delivers semantically rich, object-oriented model descriptions for all managed elements, and facilitates streamlined integration and reduced costs by enabling the exchange of management information in a platform-independent and technology-neutral way.

WBEM (Web-Based Enterprise Management) built upon CIM is a set of management and Internet standard technologies developed to unify the management of distributed computing environments.

Management Profiles provide templates to describe specific management domains in CIM to help with ease of use and offer a simplified means to achieve interoperable distributed management.

Management Initiatives built upon DMTF technologies deliver functionality to specific vertical applications and industries, include important implementations.

5.16.2 Technologies

DMTF's Redfish® DSP0266 [i.229] is a standard designed to deliver simple and secure management for converged, hybrid IT and the Software Defined Data Center (SDDC) by leveraging common Internet and web services standards to expose human readable and machine capable information directly to the modern tool chain. RESTful interface semantics are used by Redfish to access a schema based data model to conduct management operations. The initial scope of Redfish targets servers.

DMTF CIMI specification DSP0263 [i.230] describes the model and protocol for management interactions between a cloud Infrastructure as a Service (IaaS) Provider and the Consumers of an IaaS service. The basic resources of IaaS (machines, storage, and networks) are modeled with the goal of providing Consumer management access to an implementation of IaaS and facilitating portability between cloud implementations that support the specification. It specifies a Representational State Transfer (REST)-style protocol using HTTP.

DMTF OVF specification DSP0243 [i.231] describes an open, secure, efficient and extensible format for the packaging and distribution of software to be run in virtual systems. The OVF package enables the authoring of portable virtual systems and the transport of virtual systems between virtualization platforms.

DMTF CADF specification DSP0262 [i.232] is an open standard that addresses the need from consumers of cloud deployments to assure that the security policies they require on their applications are as consistently managed and enforced "in the cloud" as they would be in their enterprise.

NOTE: DMTF specifications may be used by e.g. Domain Control services to configure the parameters of the resources if supported.

5.17 IEEE

Void.

5.18 ETSI ISG SAI

5.18.1 Overview

ISG SAI (Securing Artificial Intelligence) develops technical specifications that mitigate against threats arising from the deployment of AI, and threats to AI systems, from both other AIs, and from conventional sources. The underlying rationale is that autonomous mechanical and computing entities may make decisions that act against the relying parties either by design or as a result of malicious intent.

As documented in ETSI GR SAI 001 [i.205], it defines what an AI threat is and defines how it may be distinguished from any non-AI threat based on the starting point that currently there is no common understanding of what constitutes an attack on AI and how it might be created, hosted and propagated. Topics on AI and risk assessment (clause 5), threat landscape (clause 6), and AI and SAI ontology (clause 7) are studied.

As documented in ETSI GR SAI 002 [i.206], it studies the methods currently used to source data for training AI, along with a review of existing initiatives for developing data sharing protocols, then provides gap analysis on this information to scope possible requirements for standards for ensuring integrity in the shared data, information and feedback, as well as the confidentiality of these. The reason behind this study is that accessing to suitable data is often limited, which causes a need to resort to less suitable sources of data. Compromising the integrity of data has been demonstrated to be a viable attack vector against an AI system. The federated learning model is described for data exchange in ETSI GR SAI 002 [i.206] enables multiple data-owners jointly-train a shared model while local training datasets are not directly exposed to each other. Each data owner locally performs a training process on self-owned training dataset and then provides locally-computed parameter updates to a central server. The shared model is updated by the central server through aggregating parameter updates. The updated model is then distributed to all data owners. A simplified federated learning model is shown in the Figure 5.18.1-1.

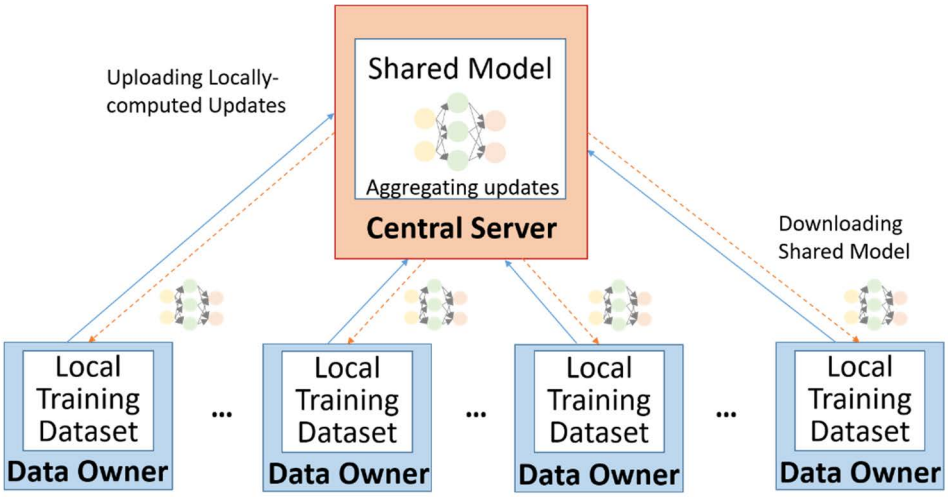


Figure 5.18.1-1: Example of federated learning model
(source: from ETSI GR SAI 002 [i.206])

As documented in ETSI GR SAI 004 [i.207], it describes the problem of securing AI-based systems and solutions, with a focus on machine learning, and the challenges relating to confidentiality, security and integrity at each stage of the machine learning lifecycle. It also describes some of the broader challenges of AI systems including bias, ethics and explainability (clause 5), a number of different attack vectors (clause 6), as well as several real-world use cases and attacks (clause 8).

As documented in ETSI GR SAI 005 [i.208], it summarizes and analyses existing and potential mitigation against security threats for AI-based systems. The goal is to have guidelines for mitigating against threats introduced by adopting AI into systems. The security capabilities, challenges, and limitations when adopting mitigation for AI-based systems in certain potential use cases are also addressed.

NOTE 1: The federated learning mentioned in ETSI GR SAI 002 [i.206] provides privacy and security features for training data exchange between multiple local data-owners and central server for machine learning. The federated learning can be leveraged by ZSM to address the data security challenges.

NOTE 2: The work in ISG SAI can be leveraged by ISG ZSM in securing the data collection and data transfer, and mitigating against threats arising from the deployment of AI.

5.19 ETSI ISG F5G

5.19.1 Overview

ISG F5G aims to document the 5th generation fixed network including:

- identifying the overall characteristics of the 5th generation fixed network;
- exploring all relevant F5G scenarios and related use cases that may include (but are not limited to) home, business and multiple vertical industries;
- performing a gap analysis to identify the necessity for both enhancements to existing technology specifications and developments of new technology specifications where required;
- studying the overall framework, outlining the complete F5G technology landscape.

Throughout the F5G work, new technologies or extensions to existing technologies will be identified through gap analysis. These topics may include, but not limited to, new ODN technologies, XG(S)-PON enhancements, Wi-Fi® 6 enhancements, control plane and user plane separation, smart energy efficiency, end-to-end full stack slicing, autonomous operation and management, Artificial Intelligence enabling, synergy of Transport and Access Networks, adaptation of Transport Network to industrial scenarios and applications, mobile network x-hauling, and convergence with 5G core network, etc. These new features need be supported by E2E network architecture, including legacy network and SDN-based networks.

As documented in ETSI GR F5G 001 [i.203], agility is one of the important technology characteristics for F5G, which includes features such as automation/orchestration, service assurance, and E2E slicing. With the E2E management, maintenance, and service provisioning, fast automatic service provisioning, real-time service ordering and online, and E2E QoS and QoE assurance can be implemented. To guarantee the quality of experience for the customer, increased intelligence and new procedures are required for the automation/orchestration systems, which include auto-healing/closed-loop, analytics - fault correlation, root cause analysis, service impact analysis, big data analytics (business data and network data), digital twin, telemetry streaming, SLA management, security management, etc.

As documented in ETSI GS F5G 005 [i.204], it studies the E2E Quality of Experience (QoE) factors in support of new services over the broadband network. High-QoE reflects the overall performance at the service level from the perspective of the end user.

NOTE: ISG F5G can cooperate with ISG ZSM in implementing the identified management relevant features, such as automation/orchestration, service assurance, network slicing, E2E QoE factors.

5.20 O-RAN Alliance

The O-RAN Alliance information can be found in https://www.o-ran.org/about.

6 Landscape of ZSM Related Open Source Communities (OSCs)

6.1 Introduction

Clause 6 identifies work done in other Open Source Communities (OSCs) in industry that may be relevant to the work in ZSM.

6.2 OSM

6.2.1 Management and Orchestration in OSM relevant to ISG ZSM

Open Source MANO (OSM) is an ETSI-hosted project to develop an open source Management and Orchestration (MANO) stack aligned with ETSI NFV Information Models. The scope of OSM project covers both design-time and run-time aspects related to service delivery for telecommunications service provider environments.

OSM orchestrates E2E Network Services (NS) and network slices across virtual domains (i.e. managed by a VIM), transport network domains, and physical and hybrid network elements. The network slice feature is aligned with 3GPP and ETSI specifications.

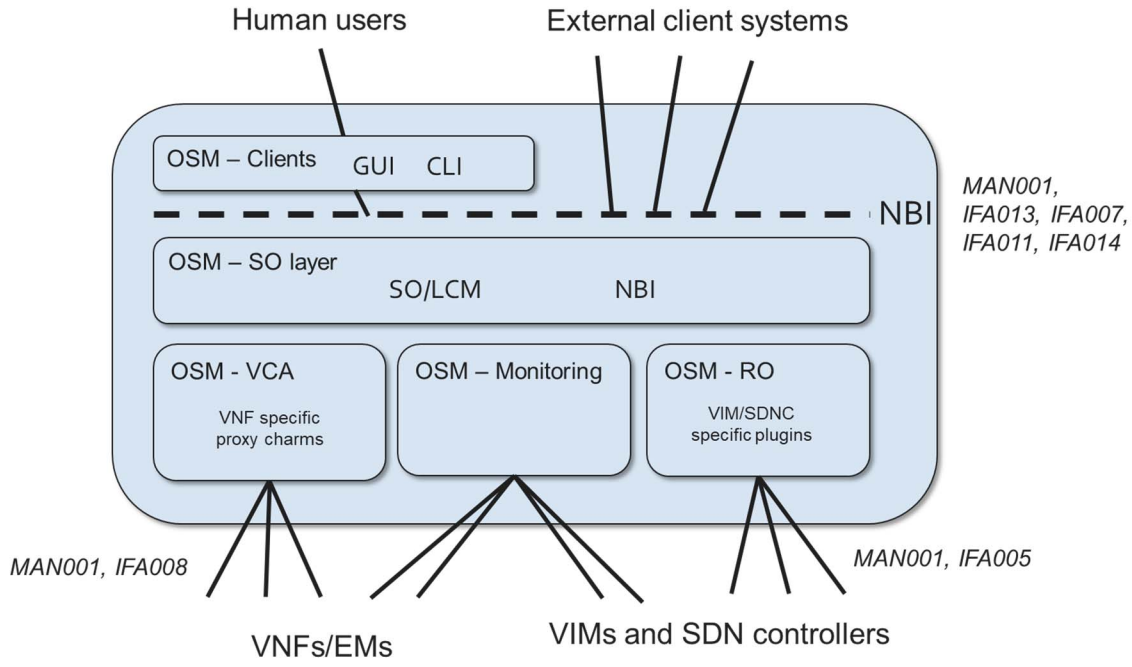


Figure 6.2.1-1: OSM Reference Architecture
(source: from OSM Release FIVE [i.176])

The OSM Reference Architecture is presented in Figure 6.2.1-1 (both run-time and design-time). The OSM components interact with other management and orchestration domains (including OSS/BSS) via well-known NFV reference points and interfaces, such as Or-Vi or Os-Ma-nfvo. OSM supports network slicing and allows different modes to control and manage the lifecycle of NSI. In the full E2E management mode, OSM takes the full control to manage the lifecycle of NSIs. In the standalone management mode, the 3rd party standalone slice manager or OSS/BBS takes the role of managing slices via the OSM exposed interfaces (e.g. ETSI GS NFV-SOL 005 [i.18] specified in ETSI NFV) whereas the OSM acts as NFVO. These two different management modes reflect aspects of the OSM capability exposure.

The support of OSM for operations across virtual domains, transport network domains, and physical and hybrid network elements is harmonized by the LCM/SO layer, as described in Figure 6.2.1-2. It not only exhibits to some extend some match with the ZSM architecture but also defines Information Model (IM) to support orchestration across the mentioned domains and automated operations over multi-layer orchestration hierarchies. With this IM, a network slice (described by network slice template in the design-time and network slice instance in the run-time) is constructed as a set of interconnected network services. This approach allows sufficient flexibility for deploying network slices.

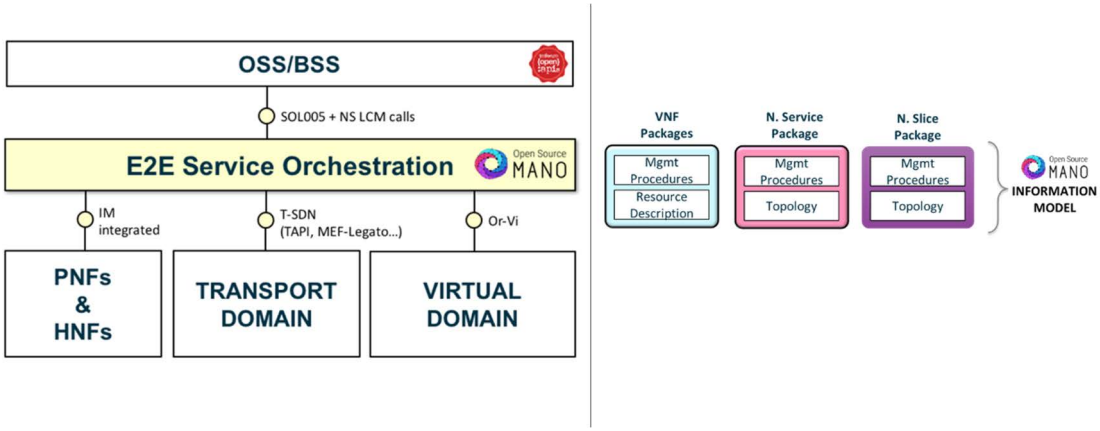


Figure 6.2.1-2: OSM operation scope across different domains and Information Model
(source: from OSM Release FIVE [i.176])

Data exposure is implemented via a common message bus (currently based in Kafka) that provides a dedicated channel for asynchronous communication between components, making simpler the integration of new pluggable modules and facilitating the centralization of common services such as common database, object storage, and metrics storage as presented in Figure 6.2.1-3.

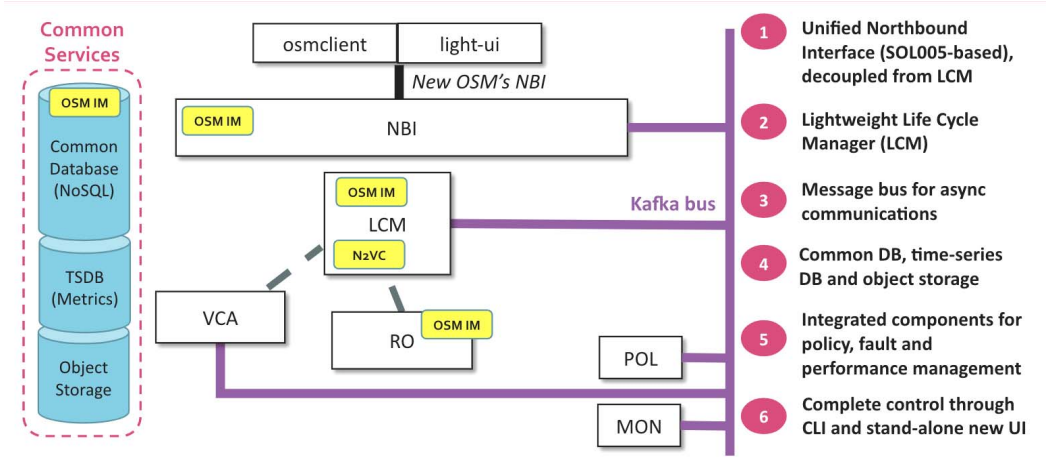


Figure 6.2.1-3: OSM Implementation Architecture
(source: from OSM Release FIVE [i.176])

6.2.2 FM and PM in OSM relevant to ISG ZSM

Alarm management is automated based on monitoring and collected data (events and metrics). Alarms can be created based on metric thresholds or associated with events relevant for the proper operations of NSs. Alarm management plays a central role in auto-scaling behaviour too. Monitoring data (metrics) is stored and correlated in a local, highly scalable and performant Time Series Database to enhance lifecycle automation based on metrics aggregation and correlation, independent of their source.

Figure 6.2.2-1 demonstrates how Fault Management is implemented.

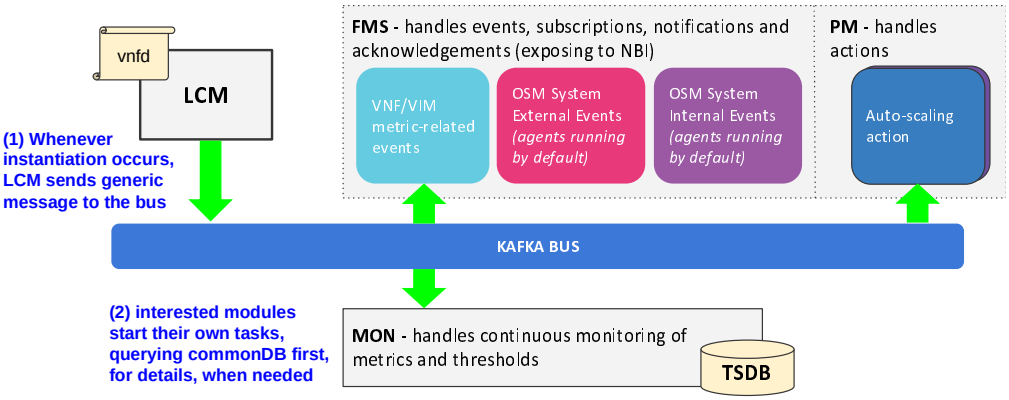


Figure 6.2.2-1: OSM Fault Management Architecture
(source: from OSM Release FIVE [i.176])

Performance management and policy management are also facilitated by monitoring and can be used to support auto-scaling. Figure 6.2.2-2 demonstrates how Performance Management is implemented.

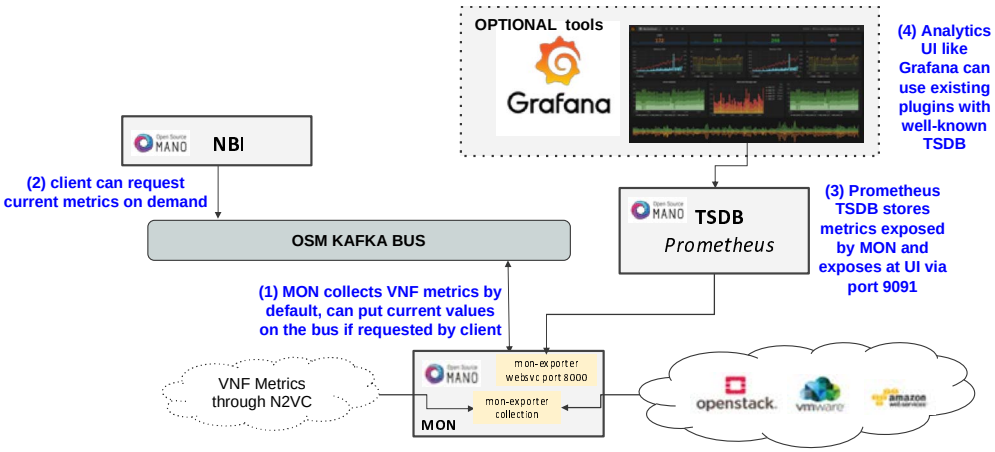


Figure 6.2.2-2: OSM Performance Management Architecture
(source: from OSM Release FIVE [i.176])

The latest version is OSM Release FIVE [i.176]. With this and previous versions, the OSM supports following features that are relevant to ZSM:

- E2E service orchestration across virtual domain, transport domain, and physical and hybrid network elements, with dynamic interconnections between DCs across heterogeneous WAN technologies.
- E2E Service Orchestration capabilities that enable and simplify the operational considerations of the various lifecycle phases involved in running a complex service based on NFV.
- A well-known Information Model (IM) that support Network Slices and Network Services (NS) composed of Network Functions (virtual, physical and hybrid). Its abstraction features reduce complexity for developers, vendors and service providers to design services.
- Dedicated and unified channel (message bus) for asynchronous communication between components, which makes OSM open and simple to integrate with new pluggable modules, facilitating the access to a coherent set of common services.
- Service Modelling to simplify, accelerate and standardize the design-time phase.
- Among other techniques, it also provides a sound support of Service Function Chaining (SFC) to simplify service composition.
- Multi-Site and multi-VIM support enables automated service delivery across multiple sites and VIMs.
- Policy-based closed-loop control with extended monitoring capabilities to assure services.

- Monitoring and data collection covers both VIM and VNF. Additionally, monitoring data (e.g. alarms) are evaluated and notified to consumers via Kafka bus.
- Auto-scaling, supported by the policy-based fault management, performance management to enable certain degree of zero-touch operation and automation.
- Policy manager coordinated with LCM orchestrator to automate the horizontal scaling decision at a fine VDU granularity.
- A unified and model-driven northbound interface to control OSM system, aligned with ETSI GS NFV-SOL 005 [i.18] (RESTful protocols specification for the Os-Ma-nfvo Reference Point).

At the initial stage, the scope of OSM covers only some aspects (present some similarities) of the ZSM architectural vision, such as (E2E) network services and network slices orchestration, performance management, fault management, and service/data capability exposure. In addition, OSM has the similar goal as ZSM by making efforts towards automating slice and service provisioning. OSM will be extended to implement its goal with the inspiration of the current ZSM work.

6.2.3 Closed loop automation in OSM relevant to ISG ZSM

Closed loop automation is a built-in capability for zero-touch service assurance in large production deployments. In OSM, service assurance requires the execution of three closed loops: one main closed loop (primary closed loop) and two assistant closed loops (secondary closed loops). Figure 6.2.3-1 represents the functional view of these closed loops running within the OSM framework, together with the interactions between them (closed loop coordination).

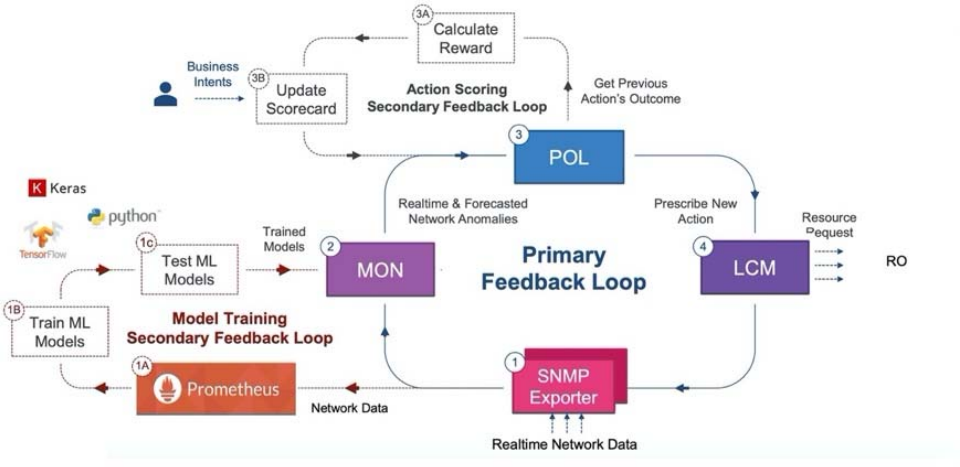


Figure 6.2.3-1: Closed loop automation in OSM.
(source: from OSM Release FIVE [i.176])

- The primary closed loop carries out data-driven resource management activities over a target managed entity (e.g. network slice, network service, VNF, etc.). It consists of four stages: Collection (stage 1), responsible for collecting and pre-processing data from individual VNFs. The collection stage is realized by the SNMP exporters.

NOTE 1: OSM has introduced the collection of VNF indicators via Prometheus exporters, in a way that allows different "exporter components" that perform the collection to be plugged-in dynamically into the system on a per-VNF basis and feed OSM's Prometheus time-series database with real-time VNF-level monitoring information. OSM makes the use of SNMP for exporters, considering its vast popularity in commercial VNFs.

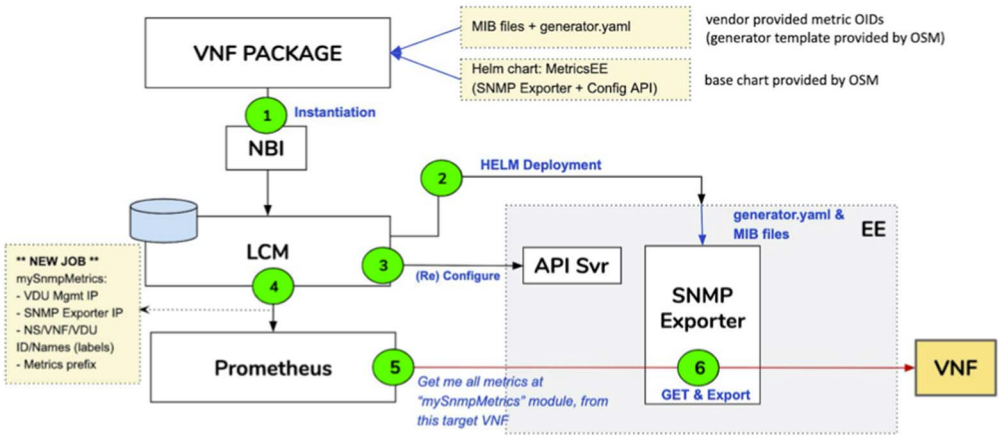


Figure 6.2.3-2: Use of SNMP exporters for VNF level monitoring in OSM
(source: from OSM Release FIVE [i.176])

NOTE 2: Figure 6.2.3-2 shows the possibility of modelling an SNMP exporter as part of the VNF package through a Helm Chart, so it can be instantiated by OSM and have metrics predefined by the VNF package builder automatically collected.

- Analytics (stage 2), responsible for deriving insights from available data, including collected data as well as historical data. The analytics stage is realized by the MON module.

- Decision (stage 3), responsible for deciding which actions are required to be taken in face of issues detected in the analytics stage. The decision stage is realized by the POL module.

- Actuation (stage 4), responsible for translating prescribed actions into specific resource lifecycle commands (e.g. scaling operation) to be enforced on the target managed entity. The actuation stage is realized by the LCM module.

NOTE 3: The enforcement of commands on the target managed entity is done by the RO.

- The primary closed loop is aligned with the closed loop concept in ZSM framework, as described in ETSI GS ZSM 009-1 [i.202]. As shown in Figure 6.2.3-1, this closed loop interacts with two other secondary loops: Model training secondary closed loop, which provides ML assisted predictions on network status (e.g. congestion, etc.) based on historical data. The interactions between this closed loop and the primary closed loop occurs in both directions. On the one hand, the output from the test ML models stage of the secondary closed loop (stage 1c) provides input to the analytics stage of the primary closed loop (stage 2). On the other hand, the output from the collection stage of the primary closed loop (stage 1) provides input to the store collected data stage of the secondary closed loop (stage 1a).

NOTE 4: Interactions between both closed loops correspond to E2 reference point, as defined in ETSI GS ZSM 009-1 [i.202].

- Action scoring secondary closed loop, which provides predictions on how good a decision would be, based on historical actions outcomes. The goodness of an action over the target managed entity is computed using reward-based approaches. The interactions between this closed loop and the primary closed loop occurs in both directions. On the one hand, the output from the update scorecard stage of the secondary closed loop (stage 3b) provides input to the decision stage of the primary closed loop (stage 3). On the other hand, the output from the decision stage of the primary closed loop (stage 3) provides input to the calculate reward stage of the secondary closed loop (stage 3a).

NOTE 5: Interactions between both closed loops correspond to E3 reference point, as defined in ETSI GS ZSM 009-1 [i.202].

OSM upcoming releases will continue working on improving interactions between closed loops, aligned with ZSM progress on closed loop coordination.

6.3 OPNFV

6.3.1 OPNFV Platform relevant to ISG ZSM

Open Platform for NFV (OPNFV) is a Linux Foundation project which facilitates the development and evolution of NFV components across various open source ecosystems. Through system level integration, deployment and testing, OPNFV creates a reference NFV platform to accelerate the transformation of enterprise and service provider networks. As an open source project, OPNFV is uniquely positioned to bring together the work of standards bodies, open source communities, service providers and commercial suppliers to deliver a de facto NFV platform for the industry.

OPNFV focuses on building NFV Infrastructure (NFVI) and Virtualised Infrastructure Management (VIM) by integrating components from upstream projects such as OpenDaylight, OVN, OpenStack, Kubernetes, Ceph Storage, KVM, Open vSwitch, Linux, DPDK, FD.io and ODP.

OPNFV Hunter 8.1 [i.178] is the current release, which progresses the state of NFV around continuous delivery, cloud native network functions (CNFs), testing, carrier-grade features and upstream project integration. The release also includes new service assurance and monitoring features.

As shows in the OPNFV Platform architectural of Gambia [i.177] left side of the diagram highlights upstream components along with the community lab infrastructure, where users can test the platform in different environments and on different hardware. The right side of the diagram shows representative capabilities in the areas of integration, testing, and adding new features to services and applications.

6.3.2 Integration and Test relevant to ISG ZSM

As a common NFVI platform, OPNFV brings together upstream components across compute, storage and network virtualisation in order to create an end-to-end platform. Activities within OPNFV focus on integration of components, end-to-end stack testing and automated build and deployment of the integrated environment. Continuous integration and automated testing of the platform for key NFV use cases is key to ensure that the platform meets NFV industry needs.

OPNFV devotes development resources towards integration and testing tools. DevOps CI/CD (Continuous Integration and Continuous Deployment) methodologies are the backbone of OPNFV. Scenarios are built and deployed in an automated fashion to Pharos labs [i.179] across the globe on multiple hardware platforms. This level of built-in testing and automation enables network provisioning, speed, and technical diversity.

The OPNFV test projects continue to pack new features and offer CSPs with an easy way to build an internal CI pipeline that can in-turn accelerate their operation journey:

- Functest used for functional testing, includes support for OpenStack Rocky [i.180] and k8s [i.188], parallelization of multiple test case execution resulting in faster runs, and the ability to execute Functest on constrained platforms, e.g. Raspberry PI.
- Yardstick, used for performance testing, includes additional support for k8s testing, easy-to-use reports, and expanded support for test tools, e.g. TRex, PktGen, and IxNextGen.
- Bottlenecks, used for stress and longevity testing, has added AI-based historical test results analysis to predict failures in subsequent test runs. Bottlenecks enhancements also include monitoring while testing is in progress.
- VSPerf, used for virtual switch performance characterization, incorporated new test cases and test tools to support causation analysis, and visibility into live metrics during test runs. The release also supports analysis automation and expanded test collection metrics including OVS DPDK core mapping and interrupt latencies and logging during test runs.
- NFVBench, used for NFVI data plane performance testing, includes support for VXLAN-based OpenStack deployments, upgrade to TRex [i.189], along with bug fixes.
- SampleVNF, that provides open source VNF approximations, includes PROX traffic generator performance optimization and latency reduction to enable better NFVI characterization.

NOTE: The features provided by OPNFV platform for virtualised resources management can be leveraged and consumed by Domain control to provide services to other functional components in the domain orchestration services group, for example to change the state or configuration of a resource entity managed in the OPNFV platform.

6.4 OpenStack

6.4.1 Overview

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacentre, all managed through a dashboard that gives administrators control while empowering their users to provision resources through a web interface.

The Mission of OpenStack is to produce a ubiquitous Open Source Cloud Computing platform that is easy to use, simple to implement, interoperable between deployments, works well at all scales, and meets the needs of users and operators of both public and private clouds.

The latest version of Open Stack is Rocky [i.180] released in August 2018. Driven by use cases like AI, machine learning, NFV and edge computing, Rocky addresses the new demands and enhanced upgrade features for infrastructure, such as on bare metal clouds, fast forward upgrades, and hardware accelerators.

6.4.2 Infrastructure Resource Management relevant to ISG ZSM

As shows in the latest OpenStack Architecture [i.180], it includes new features, such as Bare Metal, Containers (Magnum project), Edge/Internet of Things (Octavia project), High Availability (Masakari project) and High-Performance Computing (Cyborg project).

Following list takes out some projects in OpenStack which develop services [i.181] that are relevant to ZSM, especially for the management of network functions and resources:

- Nova project provides Compute Service for OpenStack. It provides massively-scalable, on-demand, self-service access to compute resources, including bare metal, virtual machines, and containers.
- Zun project provides Containers Service for OpenStack. It supports for launching and managing containers backed by different container technologies.
- QinLing project provides Functions Service for OpenStack. It provides a platform to support serverless functions (like AWS Lambda).
- Swift project provides Object Store Service for OpenStack. It provides a highly available, distributed, eventually consistent object/blob store, which can be used to store lots of data efficiently, safely, and cheaply.
- Cinder project provides Block Storage service for OpenStack. It virtualises the management of block storage devices and provides end users with a self-service API to request and consume those resources without requiring any knowledge of where their storage is actually deployed or on what type of device.
- Neutron project provides Networking Service for OpenStack. It delivers Network-Connectivity-as-a-Service in virtual compute environments.
- Keystone project provides Identify Service for OpenStack. It provides Identity API for client authentication, service discovery, and distributed multi-tenant authorization. It supports LDAP, OAuth, OpenID Connect, SAML and SQL.
- Glance project provides Image Service for OpenStack. It provides virtual machine images discovering, registering, and retrieving via a RESTful API.
- Heat project provides Orchestration Service. It orchestrate the infrastructure resources for a cloud application based on templates.

- Mistral project provides Workflow Service for OpenStack. It takes care of state management, correct execution order, parallelism, synchronization and high availability for business processes consisting of multiple distinct interconnected steps that need to be executed in a particular order in a distributed environment.
- Blazar project provides Resource Reservation Service for OpenStack. It enables users to reserve a specific type/amount of resources for a specific time period and it leases these resources to users based on their reservations.
- Aodh project provides Alarming Service for OpenStack. Its goal is to enable the ability to trigger actions based on defined rules against sample or event data collected by Ceilometer.
- Magnum project provides Container Orchestration Engine Provisioning Service for OpenStack. It makes container orchestration engines such as Docker Swarm, Kubernetes, and Apache Mesos available as first class resources in OpenStack.
- Sahara project provides Big Data Processing Framework Provisioning Service for OpenStack. It provides users with a simple means to provision data processing frameworks (such as Hadoop, Spark and Storm) on OpenStack. This is accomplished by specifying configuration parameters such as the framework version, cluster topology, node hardware details and more.
- Trove project provides Database as a Service Provisioning Service for OpenStack. It provides relational and non-relational database engines.
- CeiloMeter project provides Metering and Data Collection Service for OpenStack. Its goal is to efficiently collect, normalize and transform data across all current OpenStack core components.
- PANKO project provides Event, Metadata Indexing Service for OpenStack. It is designed to provide a metadata indexing, event storage service which enables users to capture the state information of OpenStack resources at a given time.
- Monasca project provides Monitoring Service for OpenStack. It provides monitoring-as-a-service solution integrated with OpenStack.
- Watcher project provides Optimization Service for OpenStack. It provides a flexible and scalable resource optimization service.
- Vitrage project provides Root Cause Analysis Service for OpenStack. It is used to organize, analyse and visualize OpenStack alarms and events, yield insights regarding the root cause of problems and deduce their existence before they are directly detected.
- Congress project provides Governance Service for OpenStack. It provides policy as a service across any collection of cloud services in order to offer governance and compliance for dynamic infrastructures.
- Rally provides Benchmark service for OpenStack. It is a benchmarking and performance analysis tool for OpenStack that can be used to automate measuring and profiling focused on how new code changes affect OpenStack performance, detect scaling and performance issues, and investigate how different deployment architectures and hardware affect OpenStack performance. It can be used as a basic tool for an OpenStack CI/CD system that would continuously improve its SLA, performance and stability.
- Tricircle provides Networking Automation for Multi-Region Deployments Service for OpenStack. It provides networking automation across Neutron in multi-region OpenStack deployments. Use cases include application high availability, dual ISPs for internet link redundancy, east-west traffic isolation, cross Nuetron L2 network for NFV, and cloud capacity expansion.

As specified in [i.181], OpenStack also provides APIs in supporting the services developed by the above projects.

NOTE: The infrastructure resources and services management in OpenStack need be further investigated by ZSM to identify the relevance to the work in ZSM, especially the infrastructure resources and services provisioning for supporting the service deployment in the management domain.

6.5 ONAP

6.5.1 ONAP Architecture relevant to ISG ZSM

ONAP (Open Network Automation Platform) is an open source software platform that delivers capabilities for the design, creation, orchestration, monitoring, and lifecycle management of physical and virtual network functions.

ONAP Architecture provides the common functions (e.g. data collection, control loops, meta-data recipe creation, policy/recipe distribution, etc.) necessary to create a service or operational capability. The ONAP platform includes: ONAP design-time framework which provides a comprehensive development environment with tools, techniques, and repositories for defining and describing resources, services, and products, including policy design and implementation, as well as an SDK with tools for VNF supplier packaging and validation; and an ONAP run-time environment which executes the rules and policies distributed by the design and creation environment, as well as the Controllers that manage physical and virtual networks.

The high-level view of ONAP Release 3 overall architecture [i.182] depicts microservices-based platform components.

The functionality description of ONAP component relevant to ZSM are listed as follows:

- **Application Controller (APP-C):** receives commands from ONAP components, such as MSO, DCAE, or the Portal, and uses these commands to manage the life cycle of Services, Resources (virtual applications and Virtual Network Functions), and their components.
- **SDN Controller (SDN-C):** a Network Controller, instantiates a Virtual Network Function by carrying out its network configuration workflow and reporting the resulting status (to both AAI and MSO. Examples of Network Controllers include those for Transport Virtual Network Functions, infrastructure networking (for instance, leaf, spine, and virtual switches), and Wide-Area-Networks (WANs).
- **Virtual Function Controller (VF-C):** leverages ETSI NFV MANO architecture and information model as a reference, and implements full life cycle management and FCAPS of VNF and NS.
- The Data Collection, Analytics, and Events (DCAE) subsystem, in conjunction with other ONAP components, gathers performance, usage, and configuration data from the managed environment. This data is then fed to various analytic applications, and if anomalies or significant events are detected, the results trigger appropriate actions, such as publishing to other ONAP components such as Policy, MSO, or Controllers.
- **Master Service Orchestrator (MSO):** manages orchestration at the top level and facilitates additional orchestration that takes place within underlying controllers. It also marshals data between the various controllers so that the process steps and components required for execution of a task or service are available when needed. The MSO's primary function is the automation of end-to-end service instance provisioning activities. MSO is responsible for the instantiation and release, and subsequent migration and relocation of VNFs in support of overall end-to-end service instantiation, operations and management. MSO executes well-defined processes to complete its objectives and is typically triggered by the receipt of service requests generated by other ONAP components or by Order Lifecycle Management in the BSS layer.
- **Policy:** provides a logically centralized environment for the creation and management of policies, including conditional rules. This provides the capability to create and validate policies/rules, identify overlaps, resolve conflicts, and derive additional policies as needed. Policies are used to control, influence, and help ensure compliance with goals. Policies can support infrastructure, products and services, operation automation, and security. Users, including network and service designers, operations engineers, and security experts, can easily create, change, and manage policy rules from the POLICY Manager in the ONAP Portal.

The functional architecture [i.180] highlights the role of a few key components:

1) External API provides northbound interoperability for the ONAP Platform and Multi-VIM/Cloud provides cloud interoperability for the ONAP workloads. ONAP northbound API continues to align better with TMForum (around ServiceOrder) and MEF APIs (around Legato and Interlude APIs) to simplify integration with OSS/BSS.

2) ONAP Operations Manager (OOM) is responsible for orchestrating the end-to-end lifecycle management and monitoring of ONAP components, and provides the ability to manage cloud-native installation and deployments to Kubernetes-managed cloud environments. It is integrated with the micro-services Bus, which provides service registration/discovery and support for internal and external APIs and key SDKs.

3) ONAP Common Services manages complex and optimized topologies. Multi-Site State Coordination (MUSIC) allows ONAP to scale to multi-site environments to support global scale infrastructure requirements. The ONAP Optimization Framework (OOF) provides a declarative, policy-driven approach for creating and running optimization applications like Homing/Placement, and Change Management Scheduling Optimization.

4) Information Model and framework utilities continue to evolve to harmonize the topology, workflow, and policy models from a number of SDOs including ETSI NFV MANO, TM Forum SID, ONF Core, OASIS TOSCA, IETF, and MEF.

5) Design time environment for on-boarding services and resources into ONAP and designing required services.

6.5.2 CLAMP

ONAP CLAMP (Control Loop Automation Management Platform) [i.190] is a platform for designing and managing control loops. It is used to visualize a control loop, configure it with specific parameters for a particular network service, then deploying and un-deploying it. The user can also update the deployed loop with new parameters during runtime, as well as suspending and restarting it.

As shown in Figure 6.5.2-1, closed loop control is provided by cooperation among a number of design-time and run-time ONAP elements. The design-time aspects of CLAMP, Policy and DCAE (Data Collection, Analytics and Events) supports the creation of the loops. The run-time loop starts with data collectors from DCAE. DCAE also supports PNDA (Platform for Network Data Analytics) analytics capabilities. CLAMP is used to monitor the loops themselves.

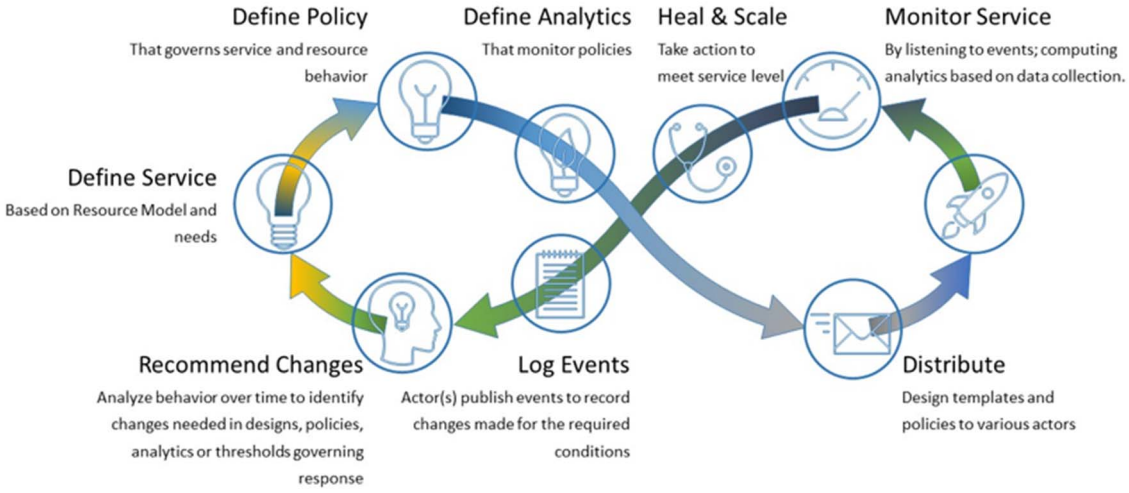


Figure 6.5.2-1 ONAP Closed Control Loop Automation
(Copyright © 2021 The Linux Foundation®. All rights reserved.)
(source: from ONAP CLAMP [i.190])

CLAMP interacts with other systems to deploy and execute the control loop. For example, it extracts the control loop blueprint and Policy Model from CSAR (Cloud Service Archive) distributed by SDC / DCAE-DS. It requests from DCAE the instantiation of micro-services to manage the control loop flow. Furthermore, it creates and updates multiple policies (for DCAE mS configuration and actual Control Operations) in the Policy Engine that define the closed loop flow.

At a higher level, CLAMP is about supporting and managing the broad operational life cycle of VNFs/VMs and ultimately ONAP components itself. It will offer the ability to design, test, deploy and update control loop automation - both closed and open.

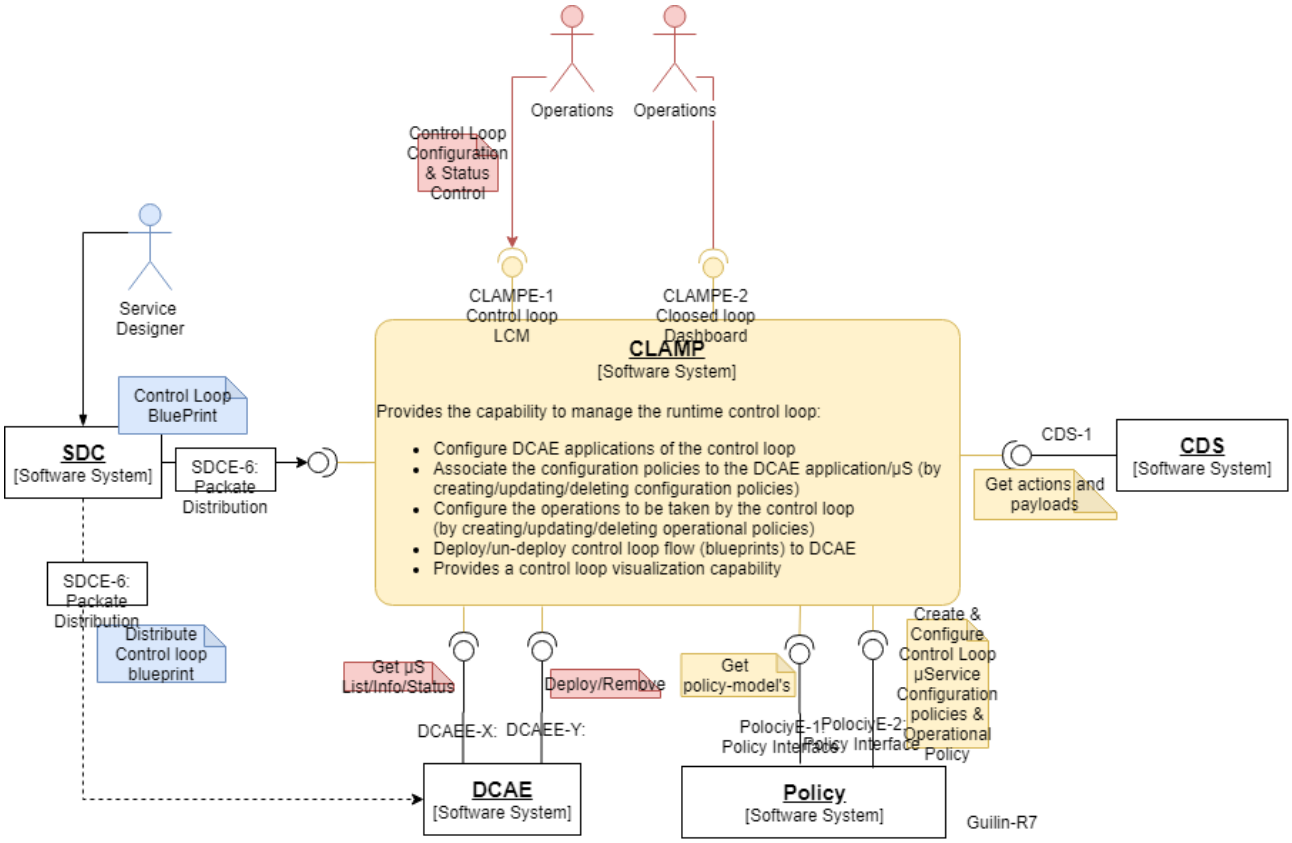


Figure 6.5.2-2 CLAMP Interfaces
(Copyright © 2021 The Linux Foundation®. All rights reserved.)
(source: from ONAP CLAMP [i.190])

CLAMP offers the internal APIs [i.190] for the management of closed loops on health check, dictionary, policies and its lifecycle. As shown in Figure 6.5.2-2, CLAMP also consumes the API's exposed by the following ONAP components [i.190] for the management of closed loop workflows:

- SDC: REST based interface exposed by the SDC, Distribution of service to DCAE.
- DCAE: REST based interface exposed by DCAE, Common Controller Framework, DCAE micro-services on-boarded (TCA, Stringmatch, Holmes (optional)).
- Policy: REST based interface, Policy engine target both XACML and Drools PDP, Policy Engine trigger operations to App-C/VF-C/SDN-C.
- CDS: REST based interface, to retrieve list of operations/actions with their corresponding payload at runtime for Operational Policies where the field 'actor' is 'CDS'.

NOTE: ZSM need further check the mechanisms and interfaces (being) developed by ONAP CLAMP can be leveraged by ZSM for its closed loop management.

6.5.3 Edge Automation

The deployment locations of edge clouds are located at close proximity to end users, typically within the access networks or at the boundary of access networks. In some deployments, they can be within the customer premises (e.g. home; enterprise; factory floor; vehicles including trains, planes, and private cars). The core thrusts of edge clouds for applications are low latency, high bandwidth, and trusted computing and storage. Various edge cloud architectures have already emerged from different communities (such as Akraino, MEC, Kubernetes, Starling, OPNFV Edge, Edge Pharos, etc.) and potentially can be plugged into the ONAP architecture for service orchestration. The group analyzes the orchestration requirements of services over various edge clouds and how these requirements impact ONAP components in terms of data collection, processing, policy management, resource management, control loop models, security, as well as application & network function deployment and control.

The Edge Automation work in ONAP is to identify architectural gaps in ONAP in satisfying edge requirements and drive those requirements in various ONAP projects and deep engagement with edge related external open source initiatives to drive the above work. Based on the analysis on edge applications (real-time or near real-time) and edge infrastructure (size of edge), the edge automation ([i.191] and [i.192]) has different requirements on distributed location, performance awareness, resource isolation, capacity constraints, security, cloud diversity (private and public cloud), configuration diversity (such as 5G factory automation, 5G general mobility services), etc., which requires ONAP to provide following capabilities:

- Scalability:
  - Ability to address large number of distributed Edge Clouds with varying capacity and very large number of end points with configuration diversity.
- Security & regulations:
  - Infrastructure verifications, securing secrets/keys, keep Data local, GDPR.
- Constrained environment:
  - Platform-awareness, Data reduction across WAN, Lesser utilization of resources.
- Performance/isolation-aware workload placement & mobility:
  - Workload placement & mobility across deployment/operation w/ closed loop control and several constraints - latency, isolation, HW profiles, etc.
- Service Assurance (SA):
  - Fault detection, root cause discovery, faster closed loop control, keep metering data local.
- Zero Touch Provisioning (ZTP):
  - Faster bring up of Edge Clouds, Easy upgrades.
- Edge APP provisioning:
  - Traffic Redirection, Providing contextual information, slice aware.

The following decomposed functions with the mapping projects provided by ONAP can implement the edge automation workflow:

- Multi-Cloud Support (Multi-VIM to support distributed cloud infrastructure capability discovery).
- Logging (-).
- IP Address Management (SDN-C).
- Inventory (A&AI to support standardized distributed cloud infrastructure object hierarchy & capability Database).
- Initial Placement (OOF to execute distributed cloud infrastructure placement policies for optimized service/VNF placement across cloud regions).
- Infra/App Monitoring events (-).
- Infra Closed Loop Analytics (Multi-VIM, DCAE).
- Closed Loop Policy (Policy).
- Closed Loop Controller (APP-C).
- App Closed Loop Analytics (DCAE).

NOTE: The identified requirements, gaps, and functions for ONAP to support edge automation need to be also considered by ZSM if edge automation falls into the scope of ZSM in the near future.

6.5.4 DCAE

The primary functions of the DCAE [i.193] subsystem are to:

- Collect, ingest, transform and store data as necessary for analysis.
- Provide a framework for development of analytics.

These functions enable closed-loop responses by various ONAP components to events or other conditions in the network.

DCAE provides the ability to detect anomalous conditions in the network. Such conditions, might be, for example, fault conditions that need healing or capacity conditions that require resource scaling. DCAE gathers performance, usage, and configuration data about the managed environment, such as about virtual network functions and their underlying infrastructure. This data is then distributed to various analytic micro-services, and if anomalies or significant events are detected, the results trigger appropriate actions. In addition, the micro-services might persist the data (or some transformations of the data) in the storage lake. In addition to supporting closed-loop control, DCAE also makes the data and events available for higher-level correlation by business and operations activities, including Business Support Systems (BSS) and Operational Support Systems (OSS).

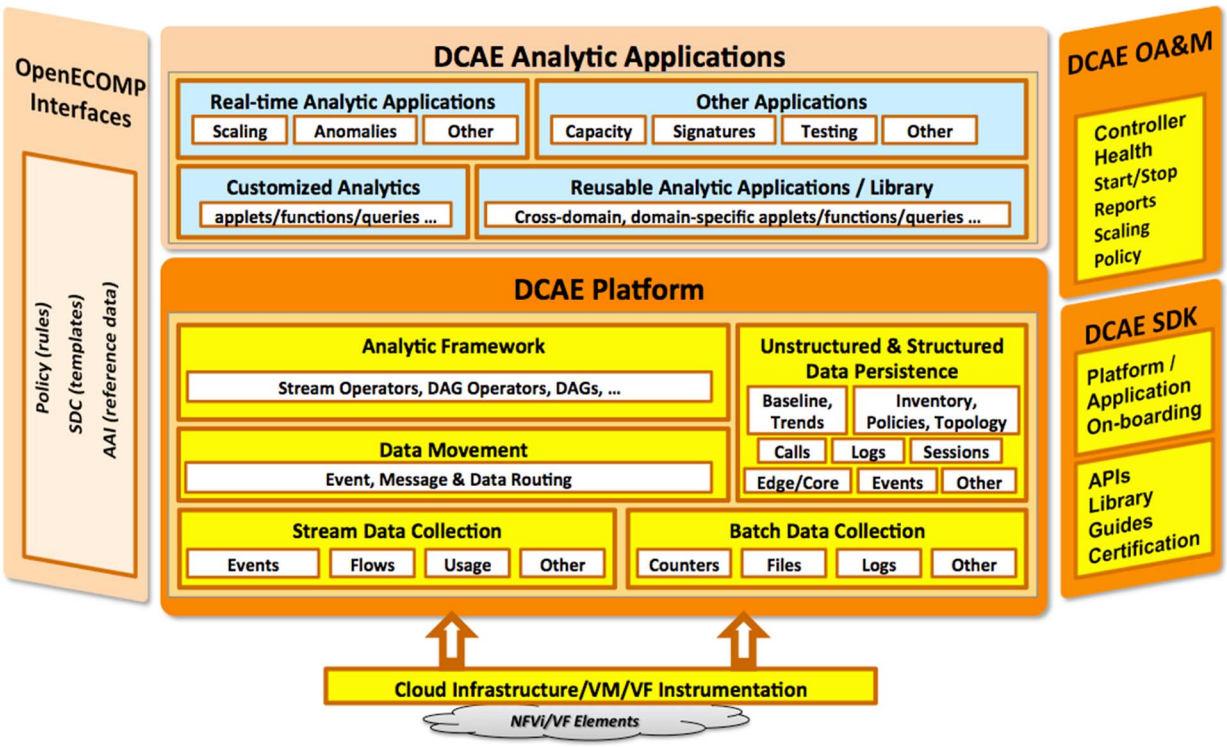


Figure 6.5.4-1: DCAE Platform high-level architecture
(Copyright © 2021 The Linux Foundation®. All rights reserved.)
(source: from ONAP DCAE [i.193])

As shown in Figure 6.5.4-1, the DCAE Platform consists of several functional components:

- Collection Framework:
  - The collection layer provides the various data collectors that are needed to collect the instrumentation that is available from the cloud infrastructure.
- Data Movement:
  - This component (known as DMaaP) facilitates the movement of messages and data between various publishers and interested subscribers that may reside at different sites.

- Storage Lake:
  - The storage lake uses big-data storage technologies such as in-memory repositories and support for raw, structured, unstructured and semi-structured data to accommodate a broad scope of requirements such as large volume, velocity, and variety.
- Analytic Framework:
  - The Analytic Framework enables agile development of analytic applications which process data from multiple streams and sources. The framework can process both real-time streams of data and data collected through traditional batch methods. Analytic applications are managed by the DCAE controller.
- Analytic Applications:
  - The types of applications that can be built on top of DCAE include analytics, fault/event correlation, performance surveillance and visualization, capacity planning, testing and troubleshooting, security, etc.

The APIs [i.194] provided and consumed by DCAE to and from other systems are specified and depicted in Figure 6.5.4-2.

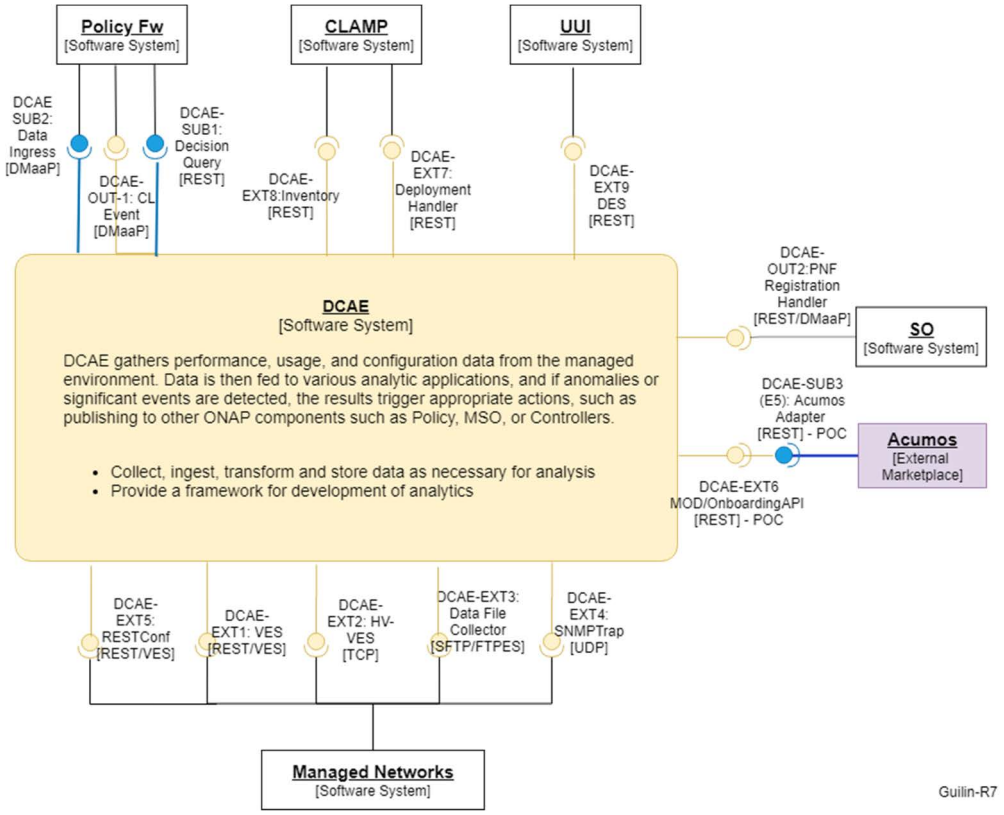


Figure 6.5.4-2: DCAE Platform high-level architecture
(Copyright © 2021 The Linux Foundation®. All rights reserved.)
(source: from ONAP DCAE APIs [i.194])

NOTE: ZSM needs to further check whether the mechanisms and interfaces (being) developed by ONAP DCAE can be leveraged by ZSM for its closed loop management.

6.6 Openslice

6.6.1 Introduction

Openslice is an open-source community that was created as a result of the work in 5G Verticals INNovation Infrastructure (5G-VINNI) project [i.235]. 5G-VINNI is an European Commission financed project that builds up a large-scale, end-to-end facility providing advanced 5G capabilities that can be accessed and used by vertical industries for use case trialing. The mission of 5G-VINNI is to provide a realistic 5G test and experimentation environment that is open to verticals and which supports rapid and agile testing of real-world use cases. To that end, 5G-VINNI facility leverages the use of Network Slice as Service (NSaaS) model, as captured in ETSI GS ZSM 003 [i.246]. This means that facility provides every vertical with an isolated service experimentation platform, deployed in the form of a slice. Each vertical will then use the provided slice to set up one or more use cases, assessing their KPIs under different load conditions through the execution of test campaigns.

6.6.2 Openslice Architecture relevant to ISG ZSM

Openslice community has defined an open-source Operations Support System (OSS) solution providing E2E Service Management functionality, covering lifecycle management processes related to service on-boarding, service fulfilment and service assurance. These processes are aligned with the work done in ETSI GS ZSM 008 [i.245].

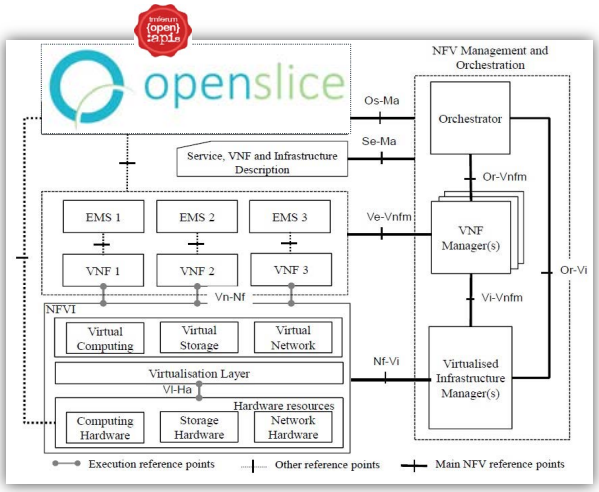


Figure 6.6.2-1: On the relationship of Openslice and ETSI NFV MANO.
(Copyright © 2019-2020 Openslice Project. All rights reserved.)
(source: from Openslice website [i.236])

Openslice provides a NSaaS enabling framework, covering both customer-facing and resource-facing service management activities, and bridging gaps between them (going from a service order to an operative network slice). In terms of customer-facing service management, Openslice defines a user-friendly web portal that allows managing the interactions with the vertical customers (e.g. customer authentication, authorization), capturing their service orders, and keeping them informed about the status of requested network slice instances. For resource-facing service management activities, based on provisioning necessary resources for the requested slice instances, Openslice interacts with the necessary ZSM management domains. For example, to deploy (and later operate) the virtualized resources of the network slice, the Openslice communicates with the NFV MANO. As captured in Figurer 6.6.2-1, in the interaction with NFV MANO, Openslice plays the role of archetypal OSS/BSS, consuming NFVO exposed capabilities through ETSI GS NFV-SOL 005 [i.18].

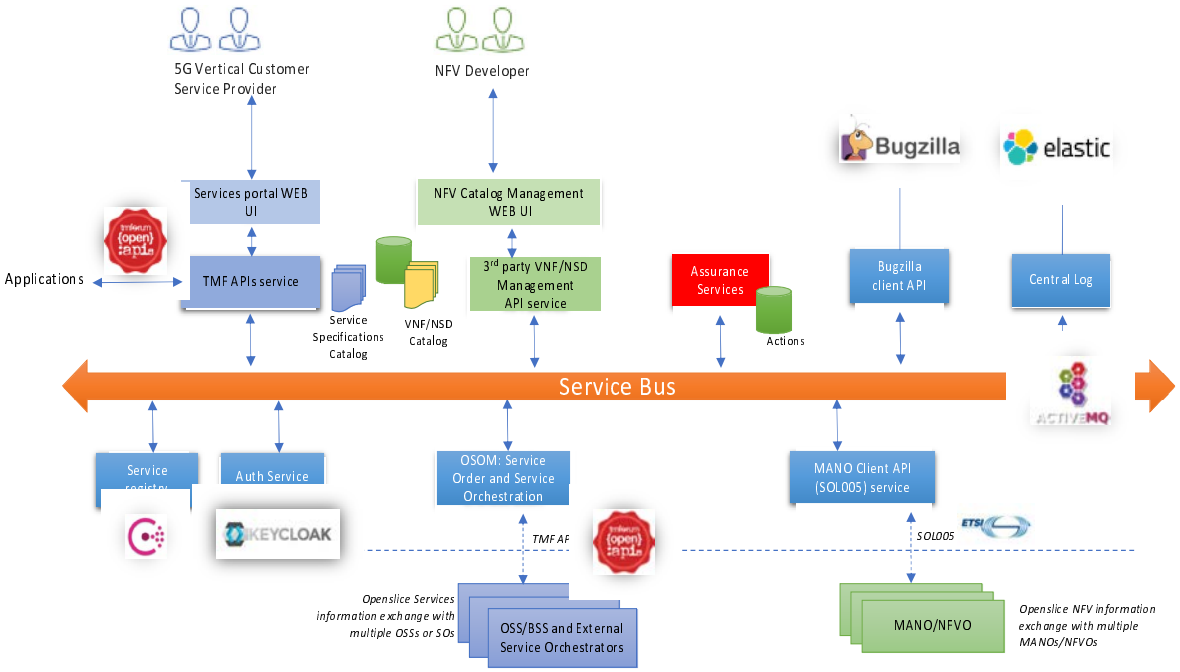


Figure 6.6.2-2: Openslice architecture
(Copyright © 2019-2020 Openslice Project. All rights reserved.)
(source: from Openslice website[i.236])

Figure 6.6.2-2 illustrates the architectural framework of Openslice. As seen, Openslice follows a microservice architecture, with a set of loosely coupled modules producing/consuming data and management services through an ActiveMQ service bus. Table 6.6.2-1 provides a summary of the main microservices building up Openslice.

Table 6.6.2-1: Openslice services

µService	Description
Auth	Keycloack server to authenticate/authorize vertical customers using OAuth 2.0 schemes.
Service registry	One-stop solution for typical procedures in microservice architectures, including service (self) registration, discovery, key-value store and load balancing. It is implemented using Consul.
Bugzilla client API	Offers interface to Bugzilla, which is a ticketing tool that allows issue tracking (fault alarms, service orders) and reporting via tickets.
Central Logging	Logs all distributed actions into an Elasticsearch cluster.
TM Forum APIs	Offers TM Forum's OpenAPIs to allow external consumption of service specification related capabilities. These open APIs include Service Catalog API (TMF633) [i.50], Service Ordering Management API (TMF641) [i.51] and Service Inventory Management APIs (TMF638) [i.54]. See note 1.
MANO client APIs	Offers ETSI GS NFV-SOL 005 [i.18] API services (e.g. NSD/VNFD on-boarding, network service instantiation/termination requests, etc.).
3rd party VNFD/NSDs Mgmt APIs	Offers APIs for NSD/VNFD management (e.g. on-boarding, updating). These APIs allow NFV developers to bring their own network services in a common marketplace. These network services will be used for the composition of network slices, which then be latter offered to vertical customers as a service.
Openslice Service Orchestrator and order Management	Referred to as OSOM, captures service ordering requests triggered by vertical customers and propagates them to external systems, including legacy OSS/BSS or other Service Orchestrators.
NOTE: These TM Forum APIs, which are the ones depicted in Figure 6.6.2-1, are for external consumption. Additionally, Openslice also has built-in TM Forum APIs for internal consumption, which are not captured in Figure 6.6.2-1, and which include among others: Resource Catalog Management API (TMF634) [i.240], Service Activation and Configuration API (TMF640) [i.53], Alarm Management API (TMF642) [i.242] or Service Test Management API (TMF653) [i.243].	

For more details on individual Openslice modules, see the Openslice official documentation in [i.236].

6.6.3 Service specification in OpenSlice relevant to ISG ZSM

Openslice supports two types of clients: vertical customers and NFV developers. On the one side, *vertical customers* are digital service providers that issue service orders following NSaaS, requesting the allocation of dedicated network slices. They use the allocated network slices to deploy one or more use cases. On the other side, *NFV developers* are network function providers that design VNFDs/NSDs. Once certified, these descriptors are onboarded to the NFV catalog. Figure 6.6.3-1 shows the two types of clients, and their interaction with the Openslice services.

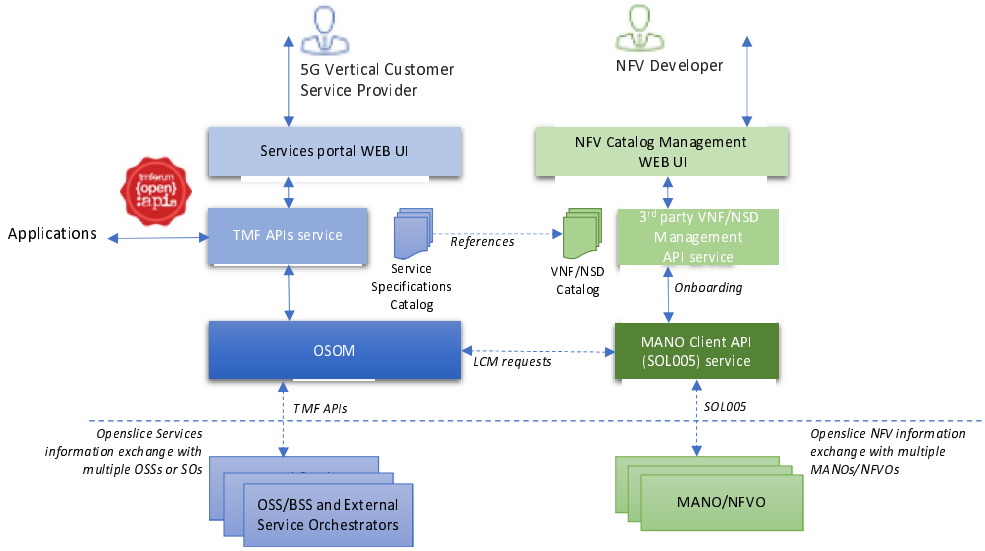


Figure 6.6.3-1: Openslice customers
(Copyright © 2019-2020 Openslice Project. All rights reserved.)
(source: from Openslice website [i.236])

As captured in Figure 6.6.3-1, to translate a service order into a network slice instance there needs to exist references/mapping between network slice components and VNFDs/NSDs. To address this, Openslice defines a service specification framework aligned with the TM Forum SID framework, based on the definition of Customer-Facing Service (CFS) and Resource-Facing Service (RFS) specifications. Figure 6.6.3-2 illustrates how this service specification can be done for a network slice example.

The right-hand side of the Figure shows the internal composition of this slice, which consists of two network slice subnets, each modelled as a separate NSD:

- **Network Slice Subnet A (NSS-A),** deployed according to NSD_F. The NSD_F is composed of four VNFs, including two Load Balancers (LB-1 and LB-2), one Web Server and one backend API brokering service.
- **Network Slice Subnet B (NSS-B),** deployed according to NSD_{SRV}. The NSD_{SRV}, consisting of three VNFs, includes one Load Balancer (LB-3), one repository catalogue and one catalogue DB.

The left-side depicts the corresponding service specification, including CFS and RFS specifications.

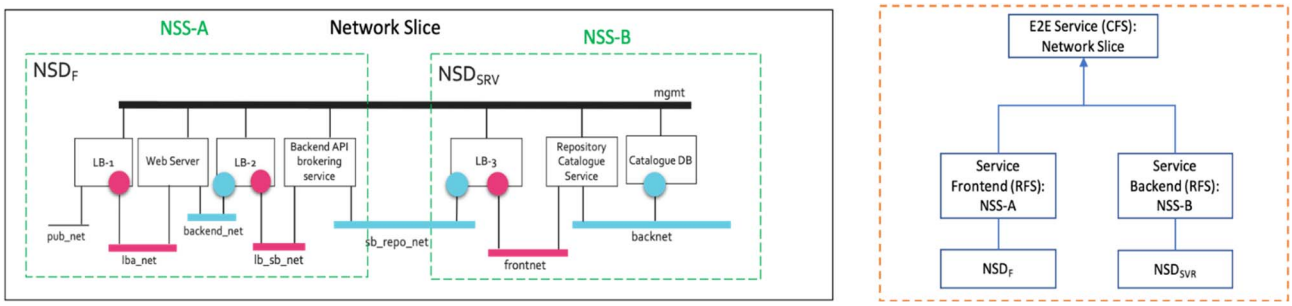


Figure 6.6.3-2: An example of service specification in Openslice
(source: from ZSM PoC#2 showcase [i.237])

6.6.4 Assurance framework in OpenSlice relevant to ISG ZSM

Openslice defines a framework that allows operators to keep track of the state of running network slice instances, ensuring they behave as expected by comparing the collected performance metrics and fault alarms against pre-defined policies. A more detailed of this framework, originally presented in Figure 6.6.2-2, is depicted in Figure 6.6.4-1. As seen this framework is governed by a service assurance planner, which is in charge of bridging performance management and fault management activities together with policy management processes. The logic of the service assurance planner can be programmatically defined for individual running services, with the injection and execution of service-specific tests. The specification of a given test is done through a test descriptor, which is stored in corresponding repository and can be managed through the TMF653 [i.243]. Examples of fields present in a test descriptor include KPI definition, the measurements methodology and the workflows for data collection and aggregation.

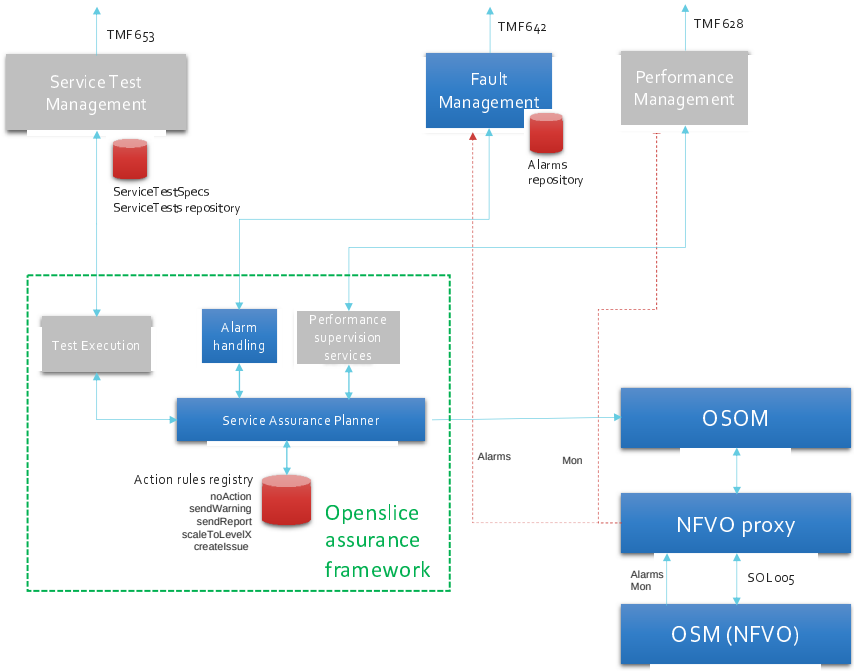


Figure 6.6.4-1: Openslice assurance framework
(source: from ZSM PoC#2 showcase [i.237])

For the policy management, there exists a registry which hosts a set of action rules. These policies define the possible corrective actions to be executed on a running instance. Figure 6.6.4-2 shows the action rule information model, and provides an example applied to the scenario captured in Figure 6.6.3-2. In this example, the rule states the following: when there a critical tagged threshold value is crossed on NSS-A, the NSS-B needs to be resized to the scale level number 4.

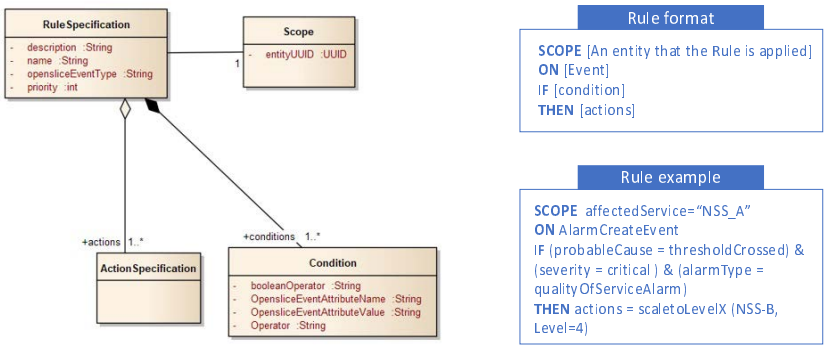


Figure 6.6.4-2: Action rules in Openslice
(source: from ZSM PoC#2 showcase [i.237])

6.6.5 Multi-stakeholder ecosystem in OpenSlice relevant to ISG ZSM

In Openslice, the TMF Open APIs for external consumption (i.e. TMF633 [i.50], TMF638 [i.54] and TMF641 [i.51]) are not only used to provide the North-Bound Interface for the vertical customers, but also the East-/West-Bound Interface with external partner organization. Indeed, with these APIs Openslice can implement the communication with systems from other administrative domains at the Service Orchestration layer, thereby fulfilling the INTERLUDE (SOF:SOF) interface requirements defined in the MEF Lifecycle Service Orchestration (LSO) framework. In order to specify and register which organizations take part in this communication, Party Management API (TMF632 [i.252]) is also used.

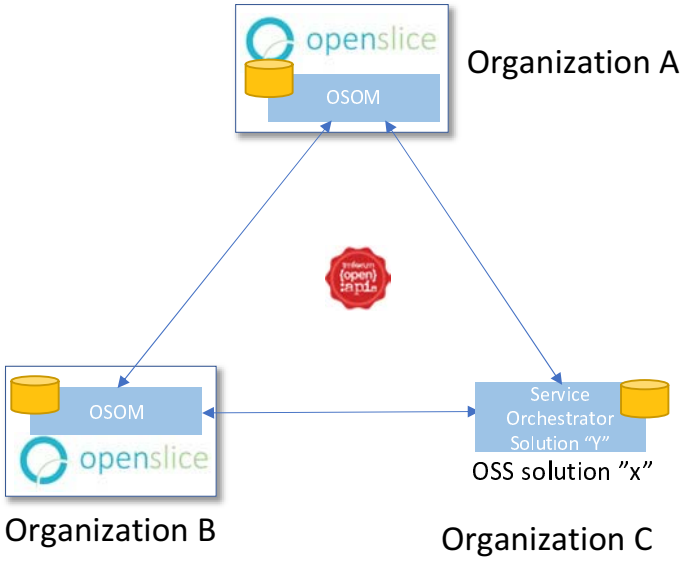


Figure 6.6.5-1: Multi-stakeholder ecosystem in Openslice
(Copyright © 2019-2020 Openslice Project. All rights reserved.)
(source: from ZSM PoC#2 showcase [i.237])

The East-/West-Bound Interface communication allow different organizations to exchange request-response/notify-subscribe messages and information for the following:

i) import service specifications;

ii) issue service orders; and

iii) use the service inventory to query the status of the service ordered to an external partner organization.

Figure 6.6.5-1 shows how Openslice can be used in such scenarios. Note that an Openslice instance can communicate with other Openslice instance, or with other service orchestration solutions (e.g. ONAP or vendor-specific solution).

7 Conclusions and Recommendations

7.1 Conclusions

The activities in the investigated SDOs in clause 5 and OSCs in clause 6 can be referenced by or contribute to ZSM in achieving the automated E2E networks and services management at different aspects, such as use cases and requirements, architecture design, service capabilities, models and service implementations, and network slicing management.

CON#1: The use cases and requirements identified in some organizations (such as NFV, MEC, ENI, 3GPP SA2/SA5, ONF, ITU-T SG13, IETF, BBF, OpenStack) are relevant to the automation of end-to-end network service management to some extent, such as service category, service performance/fault collection, SLA management, multi-domain orchestration, infrastructure resource management, data analytics, assurance, resiliency, elasticity, service continuity, service optimization, policies and constraints, testing, predictive maintenance, Network Management and Orchestration.

CON#2: The architecture frameworks specified in some organizations (such as NFV, MEC, MEF, 3GPP SA2/SA5, ONF, BBF, OSM, OPNFV, OpenStack, ONAP) can provide different options as management domains for ZSM to manage specific or part of the end-to-end network and service, or provide infrastructure resources for network services managed in the management domain.

CON#3: The service capabilities or management functions specified in some organizations (such as NFV, MEC, 3GPP SA2/SA5, ONAP, OpenStack) for service orchestration, data collection, resource control, etc. may be referenced or leveraged by the management domains including e2e service management domain of ZSM for the automation of end-to-end network service management.

CON#4: The models (such as templates, operations, information elements) and the service implementations developed in some organizations (such as NFV, MEC, ONAP, 3GPP SA5, OpenStack, ONF, OPNFV, TMF, MEF, OASIS, OSM) for service orchestration, data collection, resource control, etc. may be referenced or leveraged by ZSM for its future work in next stages.

CON#5: Supporting network slicing management (such as slice resource allocation, slice lifecycle management, slice performance/fault collection, slice template) at some aspects in some organizations (such as NFV, MEC, ENI, 3GPP SA2/SA5, GSMA, BBF, OSM, OPNFV, ONAP, Openslice, TMF) can be referenced or leveraged by ZSM for the automation of e2e network slicing management. The managed slice in these organizations can be combined at the E2E service management domain level to create end-to-end network slice.

Based on the activities in the existing and new organizations, some additional aspects related to ZSM phase II are identified that can contribute to ZSM in achieving the automated E2E networks and services management, such as closed loop automation, autonomous networks, AI/ML, CI/CD, interfaces/APIs, information models and data models.

CON#6: Closed Loop Automation (CLA) or some aspects of it is worked on in some organizations, such as reference architecture and AI CLADRA in TM Forum, CL SLS assurance in 3GPP SA5, CL architecture in ISG ENI, CL requirements/usages for Autonomic Networks in IETF, scoped within FG-AN in ITU-T SG13, CLA management platform in ONAP, CLA WG and data collection in OPNFV.

CON#7: Autonomous Networks (AN) or some aspects of it is worked on in some organizations, such as AN technical/reference architecture, AN levels evaluation, and intent modelling/LCM/interfaces in TM Forum, AN levels and intent-driven management services in 3GPP SA5, autonomous management in MANO in ISG NFV, intent policy in ISG ENI, anima WG in IETF, FG-AN in ITU-T SG13, automation platform and Intent-based network (PoC) in ONAP.

CON#8: The integration of AI/ML in network and service automation process is studied on by some organizations, such as AI maturity, AI governance, AIOps, and AI CLADRA in TM Forum, NWDAF in 3GPP SA5, AI mechanisms and AI categories in ISG ENI, ML5G in ITU-T SG13, DCAE, acumos-DCAE integration, and Holms in ONAP, fault localization in OPNFV.

CON#9: The work on CI/CD in some organizations includes but not limited to DevOps in TM Forum, study on CI/CD support in 3GPP SA5, CI/CD & DevOps in ISG NFV, CI/CD in ONAP, and Octopus project in OPNFV.

CON#10: The work on interfaces/APIs in some organizations includes Open APIs in TM Forum (such as TMF640 [i.53] for service activation and configuration, TMF633 [i.50] for service catalogue, TMF638 [i.54] for service inventory management, TMF641 [i.51] for service ordering), management services in 3GPP SA5 (such as 3GPP TS 28.532 [i.82] for generic management services), series of NFV-SOL APIs in ISG NFV, ExtAPI project in ONAP).

CON#11: The work on IM/DM in some organizations includes AI model, Intent modelling in TM Forum, network resource model in 3GPP SA5, protocols and data models in ISG NFV, IM/DM in ONAOP, and model-driven NFV in OPNFV.

7.2 Recommendations

Based on the activities in the investigated organizations and the scope of ZSM in achieving the automation of E2E networks and services management, some recommendations are summarized and proposed for further consideration.

REC#1: Use Cases and Requirements.
ZSM needs to further check some of the key use cases and the derived requirements in the organizations identified in the present document that may be a useful complement to the automation of end-to-end network service management. Potential cooperation and coordination can be conducted with the relevant organizations, and potential gaps and additional automation requirements can be provided as input by these organizations to ZSM to extend its future work.

REC#2: Architecture framework.
The architecture design principles and best practise in some other organizations such as 3GPP SA5 can be referenced by ZSM for its architecture extension and evolution.

REC#3: E2E Management Domain.
The service management across multiple technology/administrative domains is also covered in organizations such as NFV, MEF, OSM, and BBF. ZSM needs to further check if the work in these organizations can be leveraged by E2E management domain for the E2E network and service management.

REC#4: Management Domain.
The administration domain focused on by organizations such as NFV, MEC, 3GPP, OPNFV, and OSM can be regarded as a kind of management domain as specified in ZSM architecture framework, which can contribute to managing part of E2E network and service.

REC#5: Integration Fabric.
The integration fabric provides means for the integration, discovery and consumption of services, which are also covered in the Management and Orchestration functions (such as NFVO in NFV). The functions that are relevant to integration fabric can be taken out from Management and Orchestration functions and as service capabilities for interaction fabric.

REC#6: Data Services.
ZSM need further check if the data services developed in some organizations (such as data store in IETF, open data protocol in OASIS, data exposure in OSM, DCAE in ONAP) can be referenced for data integration, data storage, and data processing in ZSM.

REC#7: Infrastructure resource provisioning.
The infrastructure resource management is developed in some organizations (such as VIM in NFV, OPNFV, and OSM, Network management in IETF, OPNFV, and OpenStack). ZSM needs to further check if their resource can be managed by domain control of the management domain.

REC#8: Orchestration.
The orchestration is developed in some organizations (such as NFVO in NFV, Edge Orchestrator in MEC, LSO in MEF, Network Management and Orchestration in 3GPP SA5, Autonomic Networking in IETF) for their own purpose. ZSM needs to further check if their work can be leveraged for the automation of end-to-end network service management at domain or end-to-end level.

REC#9: Intelligence/Analytics.
The intelligence/analytics is developed in some organizations (such as ENI, ML in ITU-T, DCAE in ONAP, and NWDAF in 3GPP SA2). ZSM needs to further check if their work can be leveraged for the automation of end-to-end network service management. Potential cooperation can be conducted with these organizations.

REC#10: Data Collection.
The data collection is developed in some organizations (e.g. NFV, 3GPP SA5, OSM, OPNFV and OpenStack, DCAE in ONAP) on performance, fault, configuration, log, etc. ZSM needs to further check if their work can be leveraged in supporting closed loop network automation, based on intelligence/analytics. Potential cooperation can be conducted with these organizations for the automation of end-to-end network service management.

REC#11: Network Slicing.
The Network Slicing management is developed in some organizations (such as NFV, 3GPP SA2/SA5, BBF, GSMA, OSM, Openslice, and ONAP). ZSM need further check their work can be leveraged and potential cooperation can be conducted for the automation of end-to-end network slicing management. These managed slices in these organizations may be combined at the E2E service management domain level to create E2E network slice.

REC#12: Means of Automation.
The means of automations are worked on in some organizations (such as Intent Driven Management, 5G SON, Policy management in NFV and 3GPP SA5, Intent based Networking in ONF and IRTF). ZSM needs to further check their if work can be leveraged and potential cooperation can be conducted for the automation of end-to-end network service management.

REC#13: Service Templates.
The Service templates developed in some organizations (such as VNFD and NS templates in NFV, Generic Slice Template (GST) in GSMA, slice templates in BBF, service/Topology Template in OASIS, network slice template in OSM, Heat Orchestration Template (HOT) in OPENSTACK) focus on the automation of deployment and management of service or service components. ZSM needs to further check if their work can be referenced and leveraged, and potential cooperation can be conducted for the automation of end-to-end network service management.

Based on the activities in the existing and new identified organizations, some additional recommendations related to ZSM phase II are summarized and proposed for further consideration.

REC#14: Closed Loop Automation.
As specified in CON#6, the architectures, technologies, best practices and guidelines worked on by some other organizations for CLA can be checked by ZSM to identify the solutions and advanced topics that can be utilized for the automation of e2e network and service management. Further analysis can be performed in ETSI GS ZSM 009-2[i.247] and ETSI GR ZSM 009-3 [i.248].

REC#15: Autonomous Networks.
As specified in CON#7, the AN architecture, AN levels, intent-driven management studied by some organizations can be further checked by ZSM to identify what can be utilized to enhance the autonomous network and service management, such as intent models, intent capabilities, intent-based interfaces. Further analysis can be performed in ETSI GR ZSM 011 [i.249].

REC#16: AI/ML.
As specified in CON#8, the AI governance, AIOps, AI mechanisms, AI categories, ML serving framework, ML function orchestrator, AI/ML use cases, the best practises and guidelines worked on by some other organizations can be further checked by ZSM to identify what can be utilized by ZSM for providing support for the automation of network and service management. Further analysis can be performed in ETSI GS ZSM 012[i.250].

REC#17: CI/CD.
As specified in CON#9, some aspects/practices such as CI/CD pipeline, automated testing, version control, monitoring, metrics, and joint agile delivery (JAD) need to be further checked if they can be applied in accordance with ZSM context. Further analysis can be performed in ETSI GR ZSM 013 [i.251].

REC#18: Interfaces/APIs.
As specified in CON#10, one needs to further check if the management services specified in some organizations (such as open APIs in TM Forum, management services in 3GPP SA5, protocols in ISG NFV, and ExtAPI in ONAP) can be utilized/referenced by ZSM in achieving the e2e network and service management. Further analysis can be performed in ETSI GS ZSM 008 [i.245] and ZSM stage 3.

REC#19: IM/DM.
As specified in CON#11, the IM/DM worked on in some organizations can be further checked to identify if they can be utilized/referenced by ZSM for managing the lifecycle of e2e service, closed loops. Further analysis can be performed in ETSI GR ZSM 009-3 ([i.248]), ETSI GR ZSM 011 [i.249], ETSI GR ZSM 013 [i.251], and ZSM stage 3.

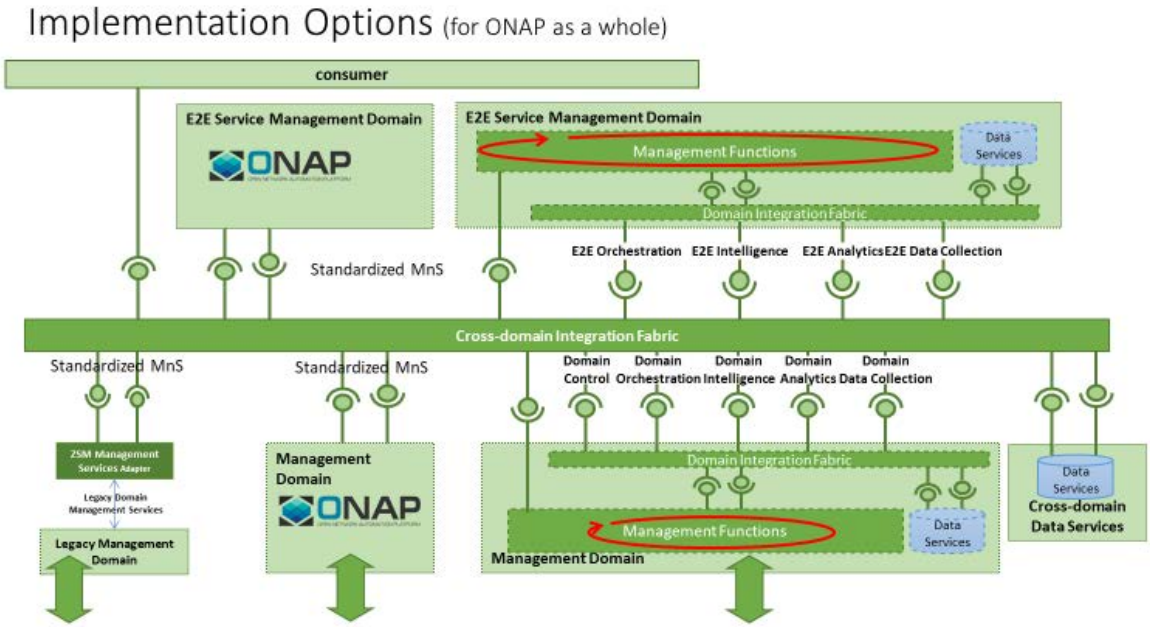
Annex A:
ONAP in ZSM Architecture

The following is a proposal on how ONAP fits with the ZSM architecture:

1) Illustrating how ONAP based implementation (as a whole) would fit into ZSM.

2) Illustrating how ONAP components would fit into the ZSM architecture and how components map within ZSM.

This is far from an exhaustive list of possible combinations.



NOTE: The term "Standardized MnS" in the diagrams refer to an ETSI ZSM standardized MnS.

Figure A.1: Illustration of multiple deployment options

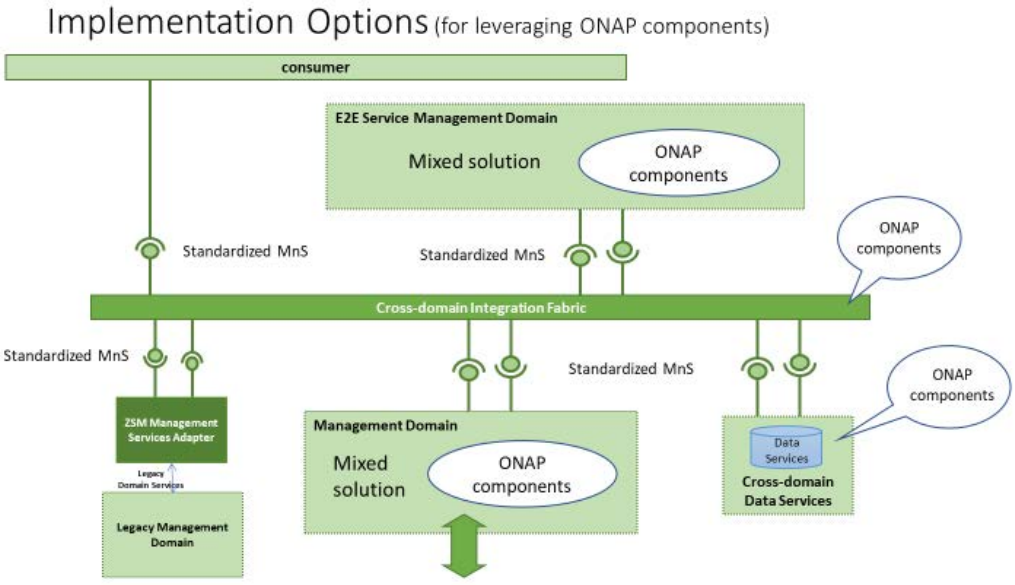


Figure A.2: ONAP components used in implementations

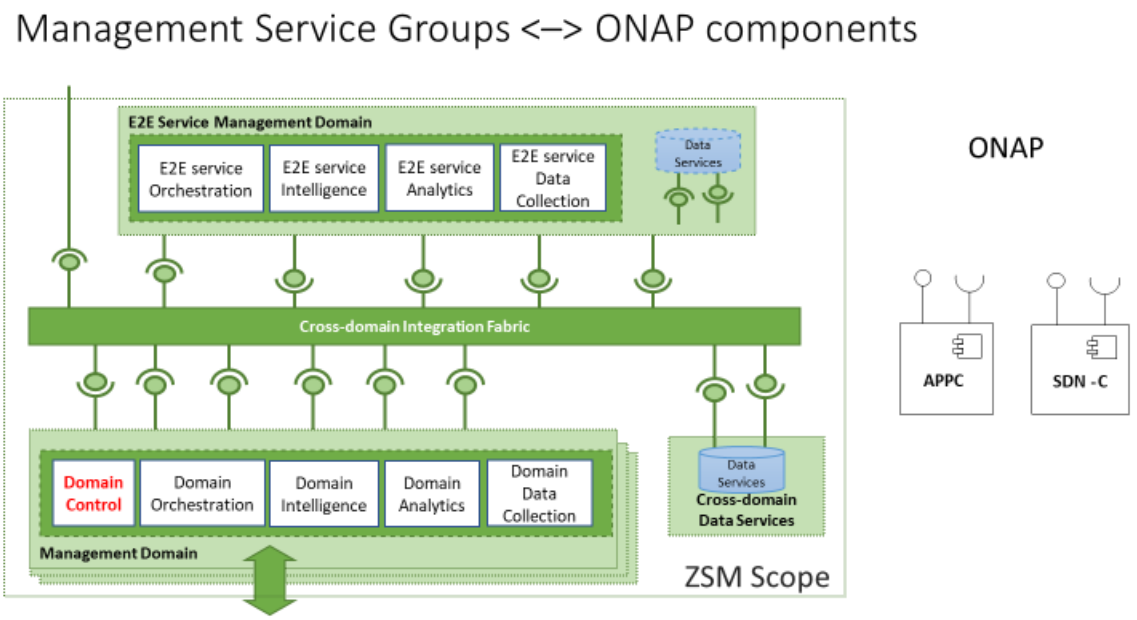


Figure A.3: ONAP components for Domain Control

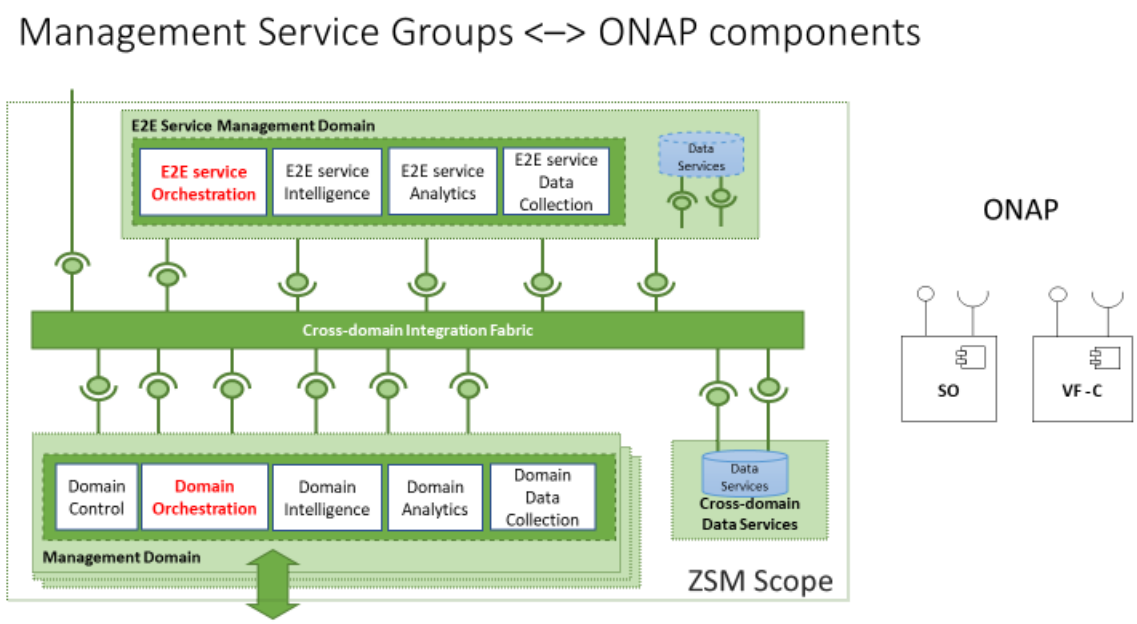


Figure A.4: ONAP components for Domain Orchestration

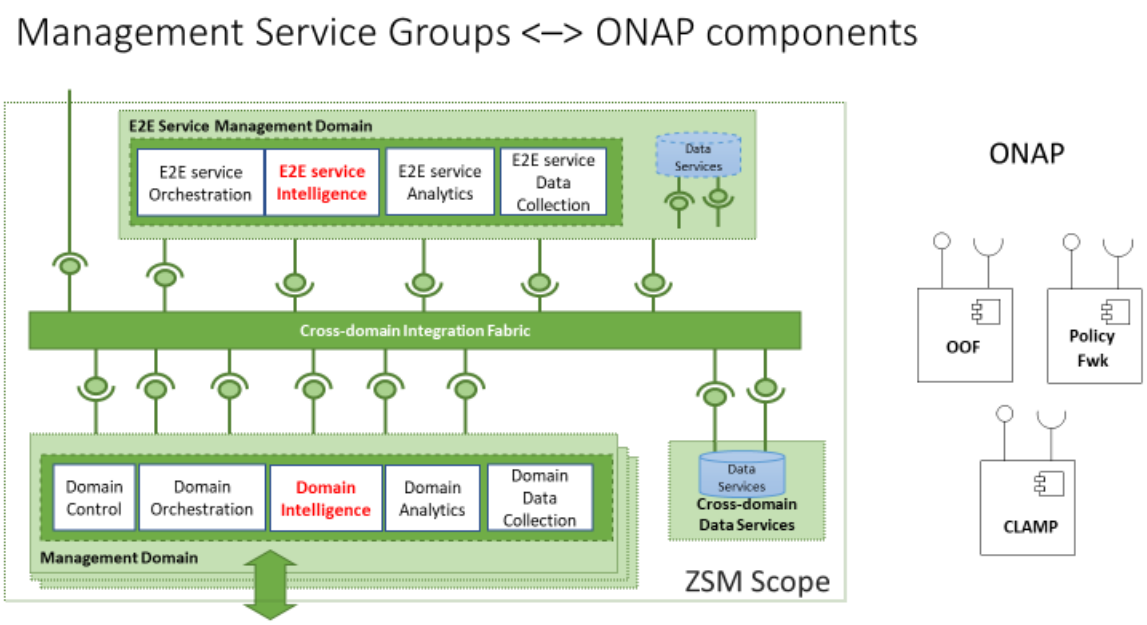


Figure A.5: ONAP components for Domain Intelligence

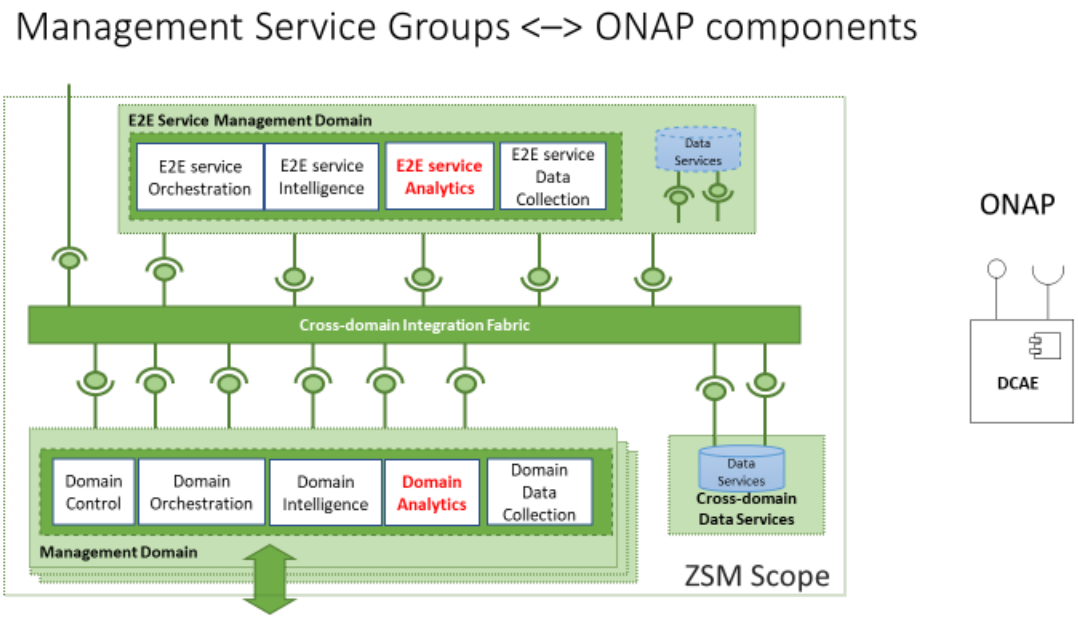


Figure A.6: ONAP components for Domain Analytics

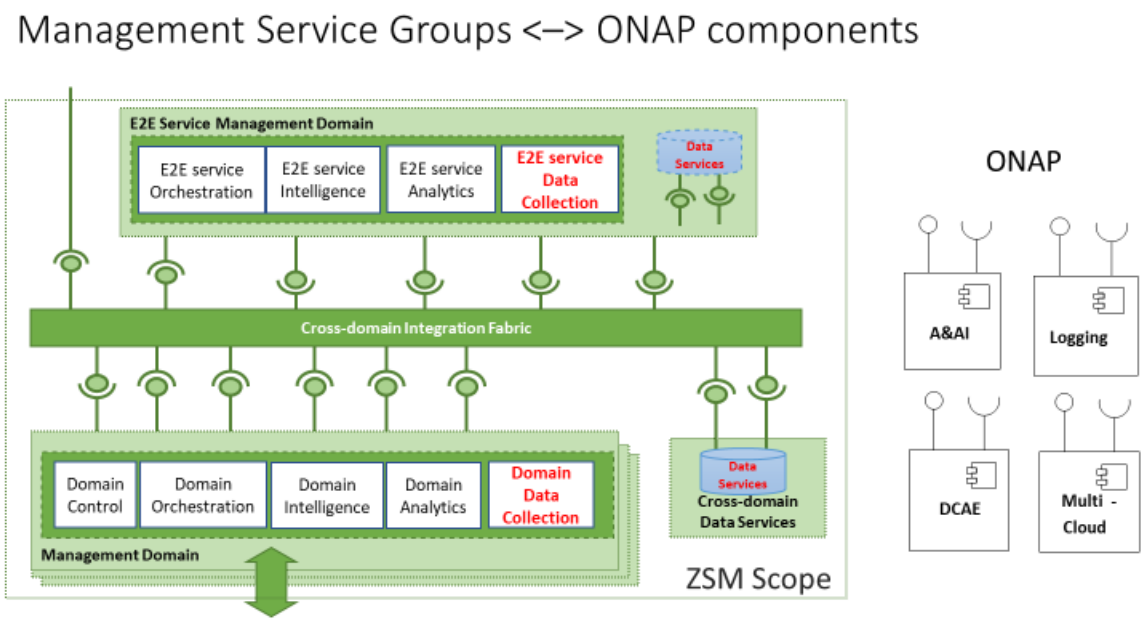


Figure A.7: ONAP components for Domain Data Collection

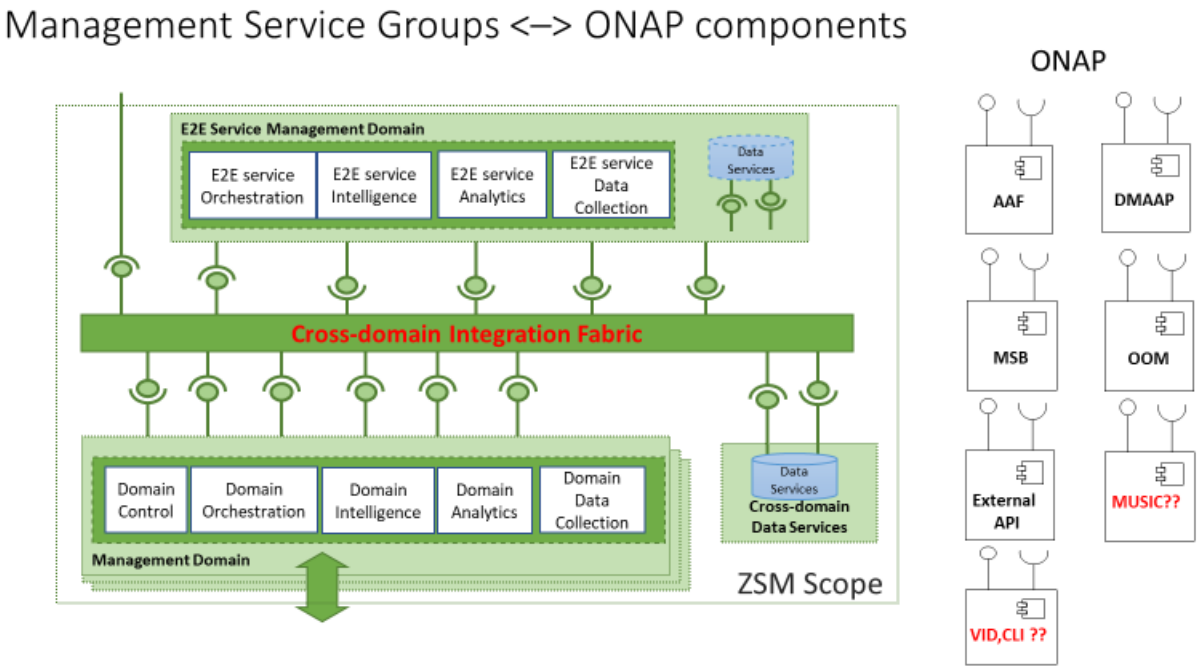


Figure A.8: ONAP components for the Cross-domain Integration Fabric

Annex B:
OSM in ZSM Architecture

OSM framework fits with the scope and design principles of ZSM reference architecture [i.187]. As illustrated in Figure B.1, OSM can be mapped to a ZSM Management Domain which:

1) exposes management capabilities to the rest of ZSM Management Domains, including individual Management Domains and the E2E Service Management Domain. The referred Management Domains, represented as OSS/BSS on the right side of Figure B.1, consume the management capabilities that OSM makes externally available through the OSM's NBI. This NBI provides a superset of ETSI NFV-SOL 005 [i.18] APIs together with the ability to handle network slices from a resource management viewpoint (i.e. the ability to handle network slice instances as a concatenation of network slice subnet instances, each deployed as an exclusive or shared network service). Since ETSI GS NFV-SOL 005 [i.18] APIs are not currently compliant with service-based principles, it is needed for the cross-domain integration fabric to make necessary adaptation to the OSM's NBI provided RESTful APIs, so they can be consumed by other ZSM Management Domains.

2) interacts with domain managed infrastructure resources through the OSM's SBI. This SBI includes plugins towards virtual and transport domains (e.g. VIM, WIM and SDN-C plugins) as well as configuration interfaces towards individual physical (and hybrid) network functions.

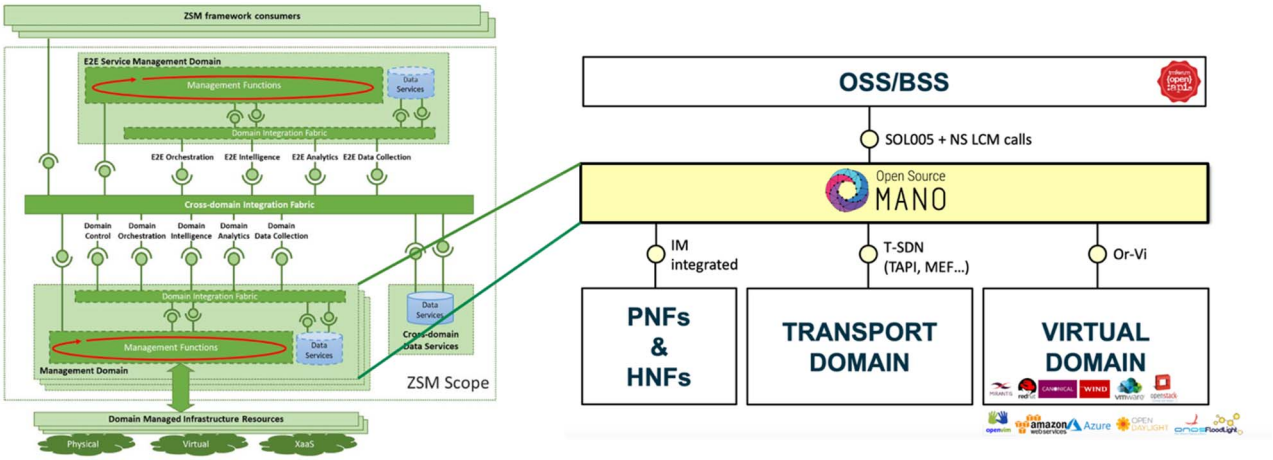


Figure B.1: OSM as a Management Domain in ZSM reference architecture

The latest version of OSM framework is OSM Release EIGHT. Figure B.2 illustrates the components building up the OSM software architecture. The different components are designed according to the architecture principles of modularity (ZSM principle 01) and resiliency (ZSM principle 07), and are based on model-driven approach, with open interfaces (ZSM principle 04). As shown in the figure, individual components interact with each other through a Kafka bus, which provides integration fabric functionality to allow extensibility (ZSM principle 02) and scalability (ZSM principle 03) in OSM architecture.

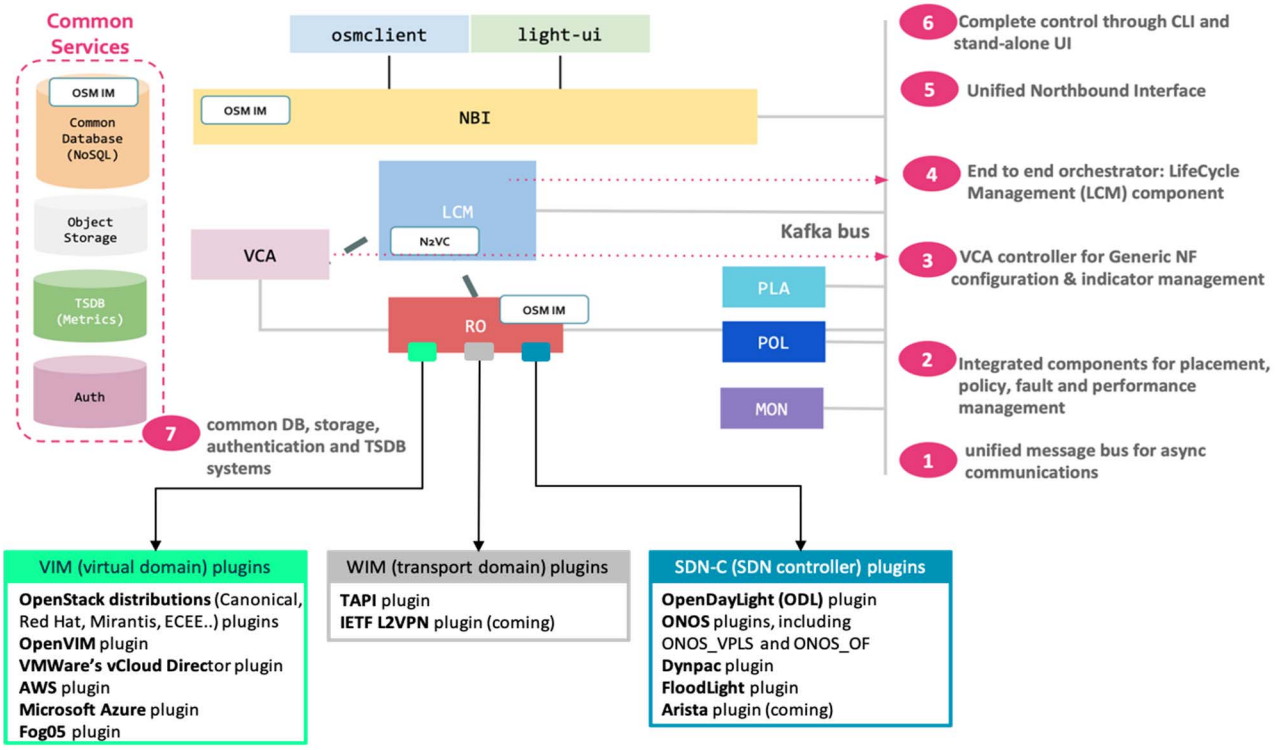


Figure B.2: OSM Release EIGHT architecture

Figure B.3 shows the potential mapping of OSM components with the ZSM grouping of management services specified in ETSI GS ZSM 002 [i.187].

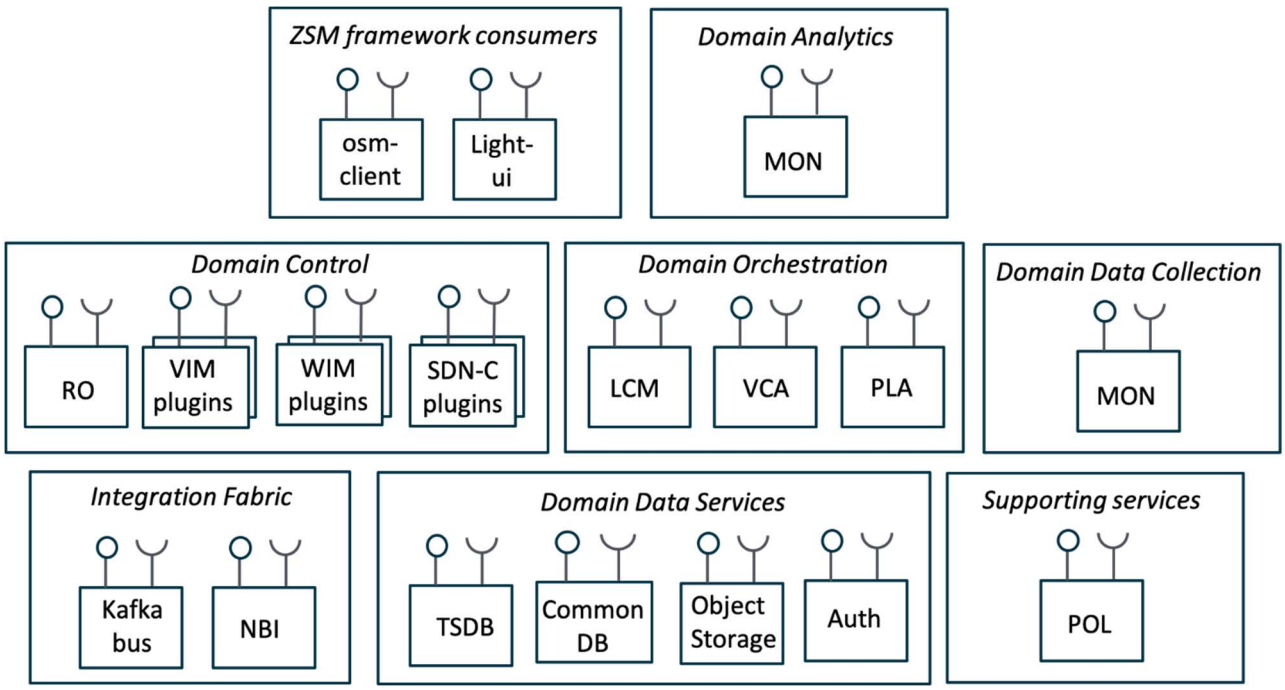


Figure B.3: On mapping OSM components with ZSM management service groups

Annex C:
Openslice in ZSM Architecture

Openslice fits with the scope and design principles of ZSM reference architecture [i.187]. As illustrated in Figure C.1, Openslice can be mapped to the E2E Service Management Domain which:

1) exposes management capabilities to their clients, namely the vertical customers and the NFV developers, both playing the role of ZSM framework consumer. Facing the *vertical customers*, Openslice provides service specification related capabilities through the use of three TM Forum open APIs, including Service Catalog API (TMF633 [i.50]), Service Ordering Management API (TMF641 [i.51]) and Service Inventory Management API (TMF638 [i.54]). Facing the *NFV developers*, Openslice provides 3rd party VNFD/NSD management (e.g. on-boarding, updating) APIs.

2) Interacts with the NFV cloud management domain (MANO) through the use of ETSI GS NFV-SOL 005 [i.18].

3) Interacts with any other ZSM management domains through the use of TMF633 [i.50]/638 [i.54]/641 [i.51]. If a ZSM management domain belongs to a different administrative domain, then Party Management API (TMF632 [i.252]) is also used.

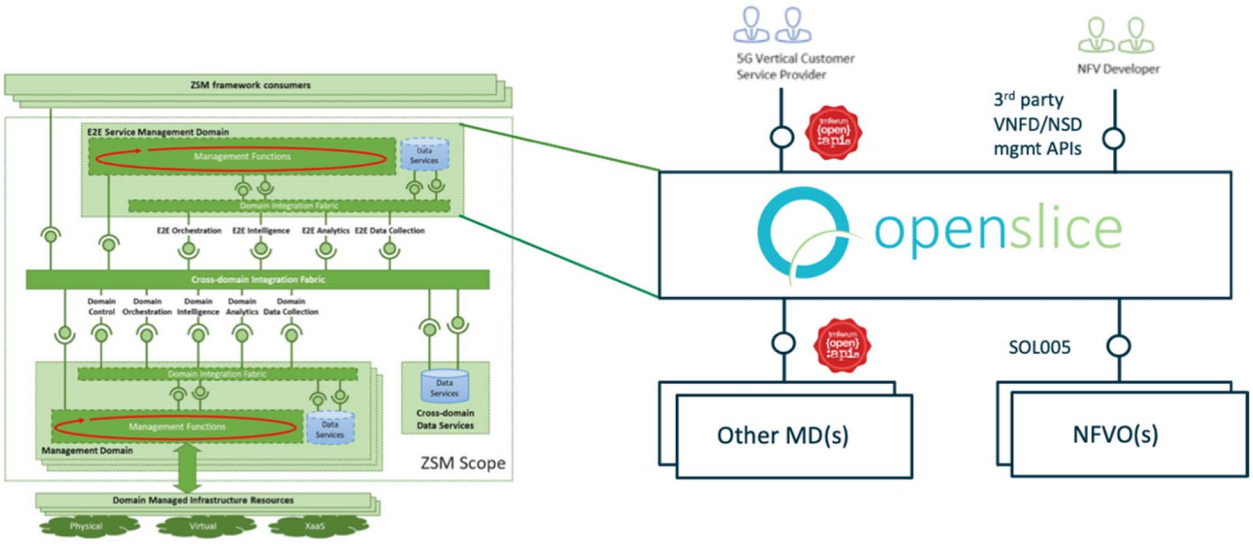


Figure C.1: Openslice as a E2E Service Management Domain in ZSM reference architecture

Figure C.2 illustrates the components building up the Openslice architecture. The different components are designed according to the architecture principles of modularity (ZSM principle 01) and resiliency (ZSM principle 07), and are based on model-driven approach, with open interfaces (ZSM principle 04). As shown in the figure, individual components interact with each other through a ActiveMQ service bus, which provides integration fabric functionality to allow extensibility (ZSM principle 02) and scalability (ZSM principle 03) in Openslice architecture.

NOTE 1: Figure C.2 corresponds to the "Figure 6.B" which was previously captured in clause 6.

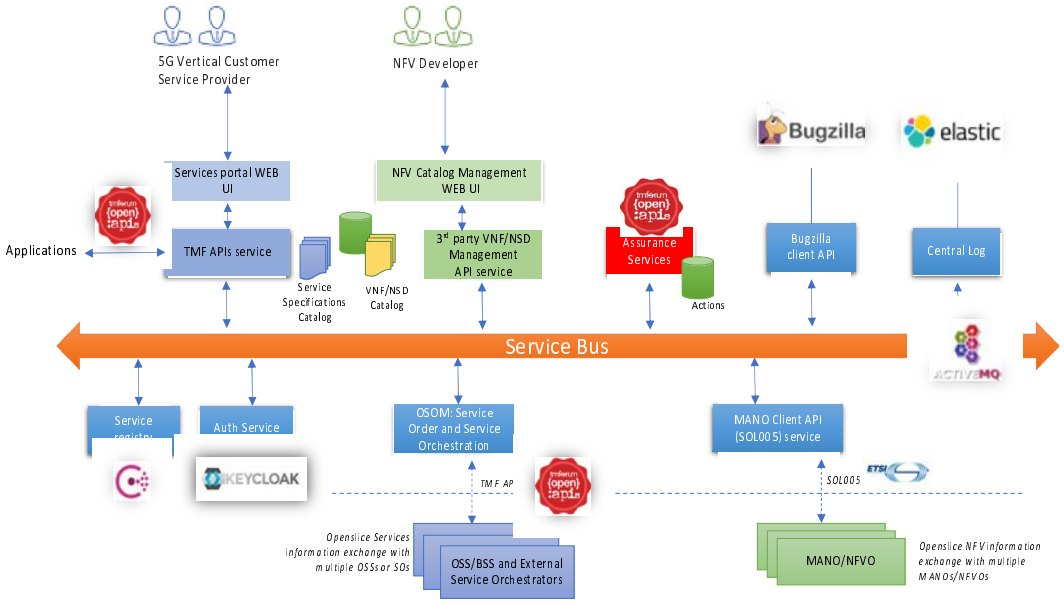


Figure C.2: Openslice architecture

Figure C.3 shows the potential mapping of Openslice services with the ZSM grouping of management services specified in ETSI GS ZSM 002 [i.187]. Apart from the TMF open APIs that Openslice makes available for external consumption, namely TMF633 [i.50]/638 [i.54]/641 [i.51]/632 [i.252], there exist other TMF open APIs which are needed for Openslice internal operation. This includes Resource Catalog Management API (TMF634 [i.240]), Activation and Configuration API (TMF640 [i.53]), Alarm Management API (TMF642 [i.242]), Performance Management API (TMF628 [i.253]) and Service Test Management API (TMF653 [i.243]).

NOTE 2: TMF642 [i.242]/628 [i.253]/653 [i.243] are part of the Openslice assurance framework, which also includes policies (actions).

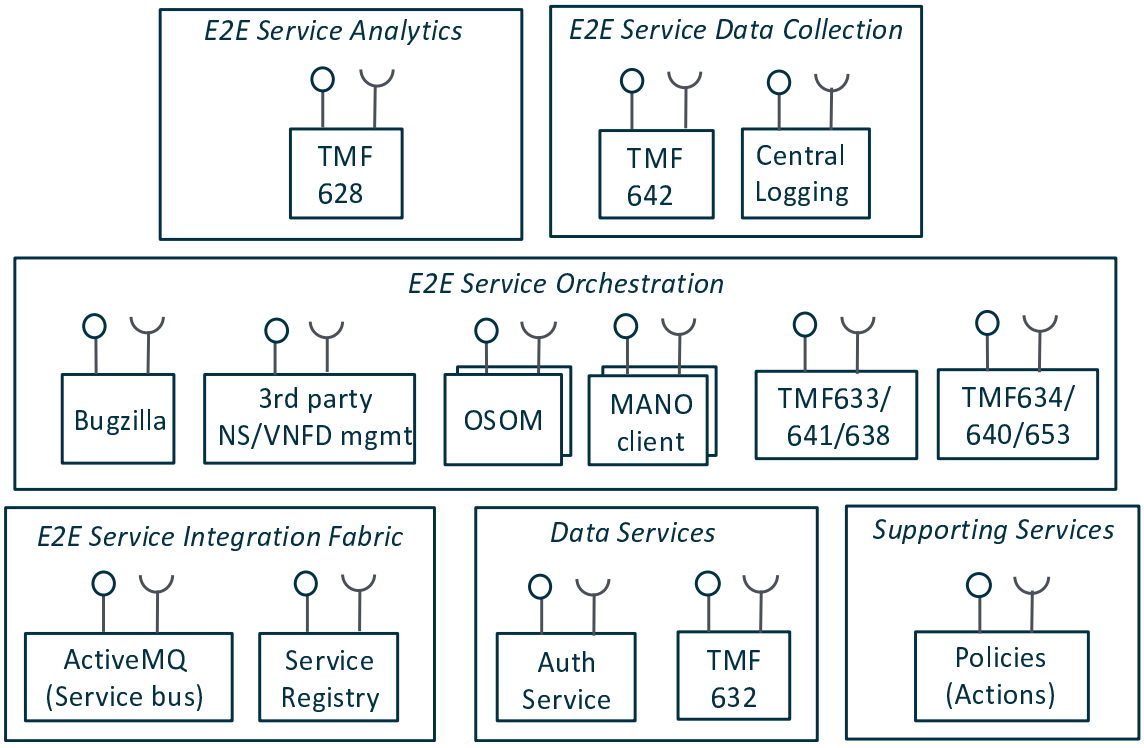


Figure C.3: On mapping Openslice services with ZSM service groups

Annex D:
Change History

Date	Version	Information about changes
21 May 2020	1.2.0	Incorporated contributions: - ZSM(20)000167_ZSM004_update_scope_and_skeleton.zip
25 August 2020	1.3.0	Incorporated contributions: - ZSM(20)000306_ZSM004_Add_Edge_Automation_progress_to_6_5_ONAP - ZSM(20)000307_ZSM004_Add_CLAMP_progress_to_6_5_ONAP - ZSM(20)000308_ZSM004_Add_DCAE_progress_to_6_5_ONAP - ZSM(20)000309_ZSM004_Add_ORAN_progress_to_5_20 - ZSM(20)000320r3_ZSM004_OSM_in_ZSM_architecture - ZSM(20)000321_ZSM004_Update_on_GSMA_description - ZSM(20)000326r1_ZSM004_Closed_Loop_Automation_in_OSM_relevant_to_ISG_ZSM
12 December 2020	1.4.0	Incorporated contributions: - ZSM(20)000441r1_ZSM004_Add_ISG_F5G_relevant_progress_to_5_19 - ZSM(20)000495_ZSM004_Add_ISG_SAI_relevant_progress_to_5_18
2 March 2021	1.5.0	Incorporated contributions: - ZSM(21)000019r1_ZSM004_Add_TMF_Autonomous_Networks_to_5_6_4 - ZSM(21)000064r1_ZSM004_Add_TMF_AIOps_relevant_progress_to_5_6_5
24 March 2021	1.5.1	Incorporated contributions: - ZSM(21)000112_ZSM004_Resolve_Copyright_Issues_in_5_6_TM_Forum
31 March 2021	1.6.0	Incorporated contributions: - ZSM(21)000135_ZSM004_Remove_Copyright_Notes_for_References_in_5_6_TM_Forum - ZSM(21)000114r2_ZSM004_Add_TMF_AI_Governance_relevant_progress_to_5_6_7
30 April 2021	1.7.0	Incorporated contributions: - ZSM(21)000156_ZSM004_Add_DMTF_progress_5_16
20 May 2021	1.8.0	Incorporated contributions: - ZSM(21)000162r1_ZSM004_Add_Openslice_to_Section_6
7 June 2021	1.8.1	Incorporated contributions: - ZSM(21)000163r1_ZSM004_Openslice_in_ZSM_architecture
23 June 2021	1.9.0	Incorporated contributions: - ZSM(20)000442r3_ZSM004_Update_the_progress_of_ML5G_in_ITU-T_SG_13 - ZSM(21)000209r1_ZSM004_Add_the_progress_of_FG-AN_in_ITU-T_SG_13
1 July 2021	1.9.1	Incorporated contributions: - ZSM(21)000224r1_ZSM004_Update_section_7_Conclusions_and_Recommendations
27 July 2021	1.9.2	Incorporated contributions: - ZSM(21)000126r3_ZSM004_remove_O-RAN_related_description - ZSM(21)000237r1_ZSM004_Editorial_Changes_to_6_6_Openslice - ZSM(21)000244r1_ZSM004_Editorial_Changes_to_Latest_Draft_v191
3 August 2021	1.9.3	Created as final draft for approval. - ZSM(21)000275r1_ZSM004_Add_in_5_4_2_2

History

Document history		
V1.1.1	March 2020	Publication
V2.1.1	January 2022	Publication