ETSI GR NFV-IFA 041 V4.1.1 (2021-08)

Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Report on enabling autonomous management in NFV-MANO

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) 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
DGR/NFV-IFA041

Keywords
autonomic networking, management, MANO, NFV

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) Network Functions Virtualisation (NFV).

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 evaluates possible enhancement to the framework of NFV-MANO to improve its automation capabilities and introduce autonomous management mechanisms. High-level use cases, functional key issue analysis and architectural options of newly introduced autonomous management functions and evaluation with impacts on NFV-MANO architectural framework are described resulting in recommendations for the normative 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 GR NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] 3GPP TR 28.812: "Telecommunication management; Study on scenarios for Intent driven management services for mobile networks".

[i.3] 3GPP TR 28.809: "Management and Orchestration; Study on enhancement of Management Data Analytics (MDA)".

[i.4] 3GPP TR 28.810: "Study on concepts, requirements and solutions for levels of autonomous network".

[i.5] 3GPP TR 28.861: "Study on the Self-Organizing Networks (SON) for 5G networks".

[i.6] 3GPP TR 28.890: "Study on integration of Open Network Automation Platform(ONAP) and 3GPP management for 5G networks".

[i.7] ETSI GS ZSM 001: "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios".

[i.8] ETSI GS ZSM 003: "Zero-touch network and Service Management (ZSM); End-to-end management and orchestration of network slicing".

[i.9] ETSI GS ZSM 008: "Zero-touch network and Service Management (ZSM); Cross-domain E2E service lifecycle management".

[i.10] ETSI GS ZSM 009-1: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 1: Enablers".

[i.11] 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.12] ETSI GR ZSM 009-3: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 3: Advanced topics".

[i.13] ETSI ETSI TS 128 550: "5G; Management and orchestration; Performance assurance (3GPP TS 28.550)".

[i.14] ETSI GS NFV-IFA 040: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Requirements for service interfaces and object model for OS container management and orchestration specification".

[i.15] ETSI GR NFV-IFA 023: "Network Functions Virtualisation (NFV); Management and Orchestration; Report on Policy Management in Mano; Release 3".

[i.16] ETSI GS NFV-IFA 027: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Performance Measurements Specification".

[i.17] ETSI GS NFV-IFA 005: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vi reference point - Interface and Information Model Specification".

[i.18] ETSI GS NFV-IFA 006: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Vi-Vnfm reference point - Interface and Information Model Specification".

[i.19] ETSI GS NFV-IFA 007: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Or-Vnfm reference point - Interface and Information Model Specification".

[i.20] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Os-Ma-nfvo reference point - Interface and Information Model Specification".

[i.21] TM Forum Exploratory report IG1193: "Cross-Industry Autonomous Networks - Vision and Roadmap".

[i.22] ETSI GS ENI 001: "Experiential Networked Intelligence (ENI); ENI use cases".

[i.23] ETSI GS ENI 002: "Experiential Networked Intelligence (ENI); ENI requirements".

[i.24] ETSI GR ENI 003: "Experiential Networked Intelligence (ENI); Context-Aware Policy Management Gap Analysis".

[i.25] ETSI GS ENI 005: "Experiential Networked Intelligence (ENI); System Architecture".

[i.26] ETSI GS ENI 011: "Experiential Networked Intelligence (ENI); Mapping between ENI architecture and operational systems".

[i.27] ITU-T Deliverable FG NET-2030 Sub-G2: "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis".

[i.28] ITU-T Technical Report FG-NET2030-Sub-G1: "Representative use cases and key network requirements for Network 2030".

[i.29] ITU-T Technical Report: "Network 2030 - Gap Analysis of Network 2030 New Services, Capabilities and Use cases".

[i.30] ITU-T Technical Report: "Network 2030 - Additional Representative Use Cases and Key Network Requirements for Network 2030".

[i.31] ITU-T Technical Specification: "Network 2030 Architecture Framework".

[i.32] ITU-T Technical Report: "Network 2030 - Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day", 13 January 2020.

[i.33] Recommendation ITU-T Y.3177: "Architectural framework of artificial intelligence-based network automation for resource and fault management in future networks including IMT-2020".

[i.34] ITU-T Draft Recommendation Y.IBN-reqts: "Scenarios and requirements of Intent-Based Network for network evolution".

[i.35] ETSI GR NFV-IFA 029: "Network Functions Virtualisation (NFV) Release 3; Architecture; Report on the Enhancements of the NFV architecture towards "Cloud-native" and "PaaS"".

[i.36] ETSI GS NFV-IFA 008: "Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Ve-Vnfm reference point - Interface and Information Model Specification".

[i.37] ETSI GR NFV-EVE 017: "Network Functions Virtualisation (NFV); Management and Orchestration; Report on the support of real-time/ultra-low latency aspects in NFV related to service and network handling".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR NFV 003 [i.1] and the following apply:

intent: formal specification of all expectations including requirements, goals, and constraints given to a system

intent driven action: action or set of actions, derived from the translation of an Intent, which provide abstract and simplified network and operation information according to the objectives of the intent

NOTE: The definition of Intent Expression, Intent Driven Object and Intent Driven Action are based on 3GPP TR 28.812 [i.2], clauses 4.1.3 and 6.3.

intent driven object: management object whose information (models, properties and/or artifacts) is capable to capture the requirements of the intent

intent expression: representation of an intent, which captures the consumer requirements, objectives and related details

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR NFV 003 [i.1] and the following apply:

AI	Artificial Intelligence
AN	Autonomous Networks
CLA	Closed-Loop Automation
DCAE	Data Collection, Analytics and Events
E2E	End to End
ENI	Experiential Networked Intelligence
FB	Functional Block
GKE	Google® Kubernetes® Engine
HPA	Horizontal Pod Autoscaler
IBN	Intent-Based Network
IM	Intent Management
ION	Intelligent Operation Network
MDA	Management Data Analytics
MDA-C	MDA-Composite
MDA-N	MDA-Nested
MDs	Management Domains
ML	Machine Learning
NFVO-C	NFVO-Composite
NFVO-N	NFVO-Nested
NOP	Network Operator
ONAP	Open Network Automation Platform
PAP	Policy Administration Point
PF	Policy Function
RAN	Radio Access Network

SBMA	Services Based Management Architecture
SON	Self-Organizing Networks
VPA	Vertical Pod Autoscaler
ZSM	Zero-touch network and Service Management

4 Background and Overview

4.1 Introduction

The NFV industry is experiencing a transformation towards cloud-native. It is anticipated that virtualised network functions will be increasingly designed according to cloud-native principles. This profound change brings a higher demand of automation to the management and orchestration of NFV (NFV-MANO), to satisfy unprecedented operational agility and efficiency.

Although NFV-MANO has already been equipped with fundamental automation mechanisms (e.g. policy based management), it is still necessary to study feasible improvements on the existing NFV-MANO functionality with respect to automation. The study in the present document focuses on the intrinsic requirements of automation from NFV-MANO via use case study, and learns the practices of automation mechanisms from other SDOs like 3GPP SA5, ETSI ISG ZSM, ETSI ISG ENI, TM Forum, ITU-T, to investigate whether those automation mechanisms can be adapted to NFV-MANO during the NFV evolution to cloud-native. It aims at assessing how autonomous management techniques could be leveraged to provide a higher level of automation in NFV-MANO.

4.2 Current automation mechanisms in NFV-MANO

Currently NFV-MANO specifies the following automation mechanisms: rule based auto-scaling and auto-healing.

These two kinds of rules are determined as policies in the VNFD, which provide the description of scale or heal actions to be executed when a condition involving monitoring parameters or VNF indicators is satisfied. The enforcement of auto-scale rule or auto-heal rule occurs in the VNFM and the NFVO automatically.

4.3 Automation related work in standardization

4.3.1 3GPP SA5

This clause provides an overview of automation related work in 3GPP SA5.

NOTE: The following text is according to the scope of the work in 3GPP SA5.

- Study on intent driven management services for mobile networks.

3GPP TR 28.812 [i.2] aims to describe 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. The relation with other automation mechanisms is also addressed in this study. Refer to 3GPP TR 28.812 [i.2] for more details of this study.

- Study on enhancement of Management Data Analytics Services.

3GPP TR 28.809 [i.3] aims to study the enhancements of MDA (Management Data Analytics). The MDA use cases and the corresponding potential requirements are identified and documented, and their possible solutions with analytics input and output (report) are developed and evaluated. The study also captures the MDA functionality and service framework, MDA process, MDA role in management loop and management aspects of MDA, including cross-domain analytics. Moreover, recommendations are provided for the normative specifications work in full alignment with 3GPP SA5 5G Services Based Management Architecture (SBMA). Refer to 3GPP TR 28.809 [i.3] for more details of this study.

- Study on concept, requirements and solutions for levels of autonomous network.

3GPP TR 28.810 [i.4] aims to describe the background, concept, definition and classification of network autonomy levels, typical scenarios for managing network and service which need autonomous support, the potential requirement and solutions and recommendation for the way forward in normative work. Refer to 3GPP TR 28.810 [i.4] for more details of this study.

- Study on the Self-Organizing Networks (SON) for 5G networks.

3GPP TR 28.861 [i.5] aims to describe management use cases, potential requirements and potential solutions of SON for 5G mobile networks. Refer to 3GPP TR 28.861 [i.5] for more details of this study.

- Study on integration of Open Network Automation Platform(ONAP) and 3GPP management for 5G networks.

3GPP TR 28.890 [i.6] investigates compatibility of the ONAP management platform architecture and functionality with that of the 5G service-based management architecture. The scope of the study includes the following aspects. Refer to 3GPP TR 28.890 [i.6] for more details of this study.

- Analysis and comparison of 3GPP and ONAP configuration management mechanisms.
- Analysis of how ONAP configuration management mechanisms can be supported in 3GPP.
- Analysis and comparison of 3GPP and ONAP alarm management and performance management mechanisms, concentrating on DCAE (Data Collection, Analytics and Events) / Collection Framework event stream and batch data collection on the ONAP side.
- Study how notify mechanisms are handled by ONAP DCAE and 3GPP management services.
- Study if any gaps exist between the semantics and format of data collected by DCAE and the semantics and format of data produced by both alarm supervision and performance management services.
- Analysis of ONAP/3GPP protocol compatibility.

4.3.2 ETSI ISG ZSM

Generally, ETSI ISG ZSM is an SDO responsible for specifying automated standardization solutions for management and orchestration system. This clause enumerates representative work in ETSI ISG ZSM.

NOTE: The following text is according to the scope of the work in ETSI ISG ZSM.

- Requirements based on documented scenarios

ETSI GS ZSM 001 [i.7] specifies requirements on the zero-touch E2E (End-to-End) network and service management. Scenarios are documented and used to derive the requirements. The requirements in ETSI GS ZSM 001 [i.7] will also be considered for the work on the topics Zero-touch network and Service Management (ZSM) reference architecture, ZSM end to end management and orchestration of network slicing, and ZSM Inter management domain lifecycle management. Refer to ETSI GS ZSM 001 [i.7] for more details of this specification.

- End to end management and orchestration of network slicing

ETSI GS ZSM 003 [i.8] aims to investigate the available standards and open source outputs relevant to support the requirements and solutions for the zero-touch, inclusive of 100 % automation, management and orchestration of end to end network slicing. Taking into account identified gaps, specify the end to end zero-touch management solutions and management interfaces to support the recognized use cases and requirements in alignment with the agreed zero touch end-to-end network and service management architecture. The available standards and open source outputs will be used and referred where appropriate in the end to end zero-touch management solution. Refer to ETSI GS ZSM 003 [i.8] for more details of this specification.

- Inter management domain lifecycle management

ETSI GS ZSM 008 [i.9] aims to investigate the automation functions of managing end to end services across Management Domains (MDs). It will specify communication patterns and information flows used in interactions between service producer and service consumer as well as the functional requirements, interfaces and operations in support of automated cross-domain lifecycle management in the ZSM framework. This work item will define what the lifecycle operations of E2E services mean, which may include e.g. instantiation, scaling, update/upgrade, healing and termination. It will describe the interactions between E2E service management domain and management domains including nested MDs. Furthermore, it describes procedures and models to enable the automation of lifecycle management. In addition, automation of LCM including the relations to necessary CM, FM, PM and closed loop functionalities will be specified. Refer to ETSI GS ZSM 008 [i.9] for more details of this specification.

- Closed-loop automation

This work includes two specifications and one report in the following aspects:

ETSI GS ZSM 009-1 [i.10] aims to describe how to enable closed-loop automation based on the ZSM architectural framework. It specifies how to automatically deploy and configure closed loops involving both the E2E service management domain and the management domains. Closed loops running within the managed entities are out-of-scope. The specification will include:

i) means for coordination, delegation, escalation, etc. between closed loops;

ii) the use of policies, rules, intents and/or other forms of inputs to steer their behaviour; and

iii) interactions between closed loops and external entities. The deliverable will specify stage-2 generic enablers and flexible procedures for closed-loop automation. Refer to ETSI GS ZSM 009-1 [i.10] for more details of this specification.

ETSI GS ZSM 009-2 [i.11] aims to specify solutions of particular E2E service and network automation use cases, based primarily on the generic enablers and architectural elements for closed loops. The solution specifies how the E2E management loop interacts with ZSM consumers with specifics for the selected use cases. The work item makes recommendations on the preferred option if multiple solutions are available. Refer to ETSI GS ZSM 009-2 [i.11] for more details of this specification.

The study in ETSI GR ZSM 009-3 [i.12] aims to investigate advanced topics related to closed-loop operations such as learning and cognitive capabilities (e.g. based on different degrees of use and integration of artificial intelligence technologies), ways to set and evaluate levels of oversight, autonomy, and operational confidence on the behaviour of the closed loops. The study will document problem statements and technical challenges, derive potential requirements, capture and evaluate potential solution options, and provide recommendations for further standardization activities. Refer to ETSI GR ZSM 009-3 [i.12] for more details of this study.

4.3.3 ETSI ISG ENI

ETSI ISG ENI focuses on improving the operator experience, adding closed-loop artificial intelligence mechanisms based on context-aware, metadata-driven policies to more quickly recognize and incorporate new and changed knowledge, and hence make actionable decisions. This clause enumerates representative work in ETSI ISG ENI.

NOTE: The following text is according to the scope of the work in ETSI ISG ENI.

- ENI use cases

ETSI GS ENI 001 [i.22] specifies a collection of use cases from a variety of stakeholders, where the use of an Experiential Networked Intelligence (ENI) system can be applied to the fixed network, the mobile network, or both, to enhance the operator experience through the use of network intelligence. It identifies and describes use cases and scenarios and gives the baseline on how the studies in ENI can be applied as solutions of some identified use cases in accordance with the ENI Reference Architecture. It also provides guidelines in terms of how to use ENI system in the network and for third parties, including the use of ENI systems in intent based networks. Refer to ETSI GS ENI 001 [i.22] for more details of this specification.

- ENI requirements

ETSI GS ENI 002 [i.23] captures the requirements of how intelligence is applied to the network and applications in different scenarios to improve experience of service provision and network operation. Also, how intelligence enables dynamic autonomous behaviour and adaptive policy driven operation in a changing context. The ENI requirements are based on the ENI use case document and identified requirements from other SDOs. These requirements will form the base for the architecture design work. Refer to ETSI GS ENI 002 [i.23] for more details of this specification.

- Context-aware policy management gap analysis

ETSI GR ENI 003 [i.24] analyses the work done in various SDOs and open source consortia on policy-based modelling. This information will be used to develop a specification for a context-aware, policy-based management model and architecture for enhancing the operator experience through the use of network intelligence. Refer to ETSI GR ENI 003 [i.24] for more details of the present document.

- ENI system architecture

ETSI GS ENI 005 [i.25] specifies the functional architecture of an ENI System, which 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:

- defining the functionality and behaviour of a system that satisfy the ENI requirements as specified in ETSI GS ENI 002 [i.23];
- defining a functional architecture, in terms of Functional Blocks, that addresses the goals specified by the ENI use cases as specified in ETSI GS ENI 001 [i.22];
- defining Reference Points used by the above Functional Blocks for all communication with systems and entities that are external to the ENI System;
- proposing a progression plan towards full support of the proposed ENI System and intermediary level of compliance (e.g. support of some architecture components or a subset of the Reference Points).

Refer to ETSI GS ENI 005 [i.25] for more details of this specification.

- Mapping between ENI architecture and operational systems.

ETSI GS ENI 011 [i.26] specifies the following bullets ordered based on its priority:

- The mapping of functional blocks in the ENI architecture and functionalities of the operational systems (e.g. NWDAF, 5GC and NFV MANO).
- How different intelligent entities of ENI and the operational system cooperate and work in parallel on assigned tasks.
- How to automatically optimize the use of multiple AI models to provide a joint decision.
- Different metrics, such as performance, accuracy, and reliability, per capability, to ensure that recommendations and/or commands provided, can be done along with other pertinent tasks (e.g. data analysis) with respect to these metrics.

Refer to ETSI GS ENI 011 [i.26] for more details of this specification.

4.3.4 TM Forum

The Autonomous Networks project resulted in several deliverables among which the IG1193 [i.21] exploratory report. The resulting proposal consists in a framework which outlines the Closed-Loop Automation (CLA) concept applied within management domains classified under 3 layers, as well as across the layers to support the user service fulfilment. This is useful from an NFV perspective to understand the broader management picture where it fits in. NFV would position itself as one of the constituent management domains at the Network Resource layer, where it consequently would run its own CLA, as well as it would interact with the CLAs that cross boundaries of one management layer.

4.3.5 ITU-T

4.3.5.1 Focus Group on Technologies for Network 2030

The ITU-T Focus Group on Technologies for Network 2030 (FG NET-2030) was established by ITU-T Study Group 13 in July 2018 and concluded its activity on July 2020. This Focus Group, as a platform to study and advance networking technologies, investigated the future network architecture, use cases, and capabilities of the networks for the year 2030 and beyond.

The automation related deliverables of ITU-T FG NET-2030 are as follows:

- ITU-T Deliverable FG NET-2030 Sub-G2 "New Services and Capabilities for Network 2030: Description, Technical Gap and Performance Target Analysis" [i.27] describes new services and capabilities for Network 2030. For other aspects and capabilities of future networking services, management with further automation and closing of control loops for network 2030 is discussed, and technologies such as Intent-Based Networking is also analysed. Refer to ITU-T Deliverable FG NET-2030 Sub-G2 [i.27] for more details.

- ITU-T Technical Report "Network 2030 - Gap Analysis of Network 2030 New Services, Capabilities and Use cases" [i.29] analyses the gaps in current network and communication technologies with respect to the Network 2030 services, capabilities, and representative use cases. Gaps in intelligent operation network is analysed. Intelligent Operation Network (ION) is a fully automated and intelligent closed-loop control framework to monitor network health while supporting flexible and complex network functions. Artificial intelligence aware networking refers to connectivity and placement aspects of AI components (data, models, knowledge) for the deployment of intelligent services along the cloud-to-things continuum. Refer to ITU-T Technical Report [i.29] for more details.

- ITU-T Technical Report "Network 2030 - Additional Representative Use Cases and Key Network Requirements for Network 2030" [i.30] is an update of use cases and network requirements for Network 2030, follows the first ITU-T Technical Report FG-NET2030-Sub-G1 [i.28]. This report covers five additional use cases: huge scientific data applications, application-aware data burst forwarding, emergency and disaster rescue, socialized Internet of things, and connectivity and sharing of pervasively distributed AI data, models and knowledge. This report also analyses the use case according to 5 abstract network dimensions, including bandwidth, time, security, AI and many nets. Refer to ITU-T Technical Report [i.30] for more details.

- ITU-T Technical Specification "Network 2030 Architecture Framework" [i.31] describes architectural principles and overall architecture for Network 2030, and the details of access/edge architecture, routing and addressing, data path security, quality of service, burst switching, network slicing, Multi-access Edge Computing federation, and network management for Network 2030. The Network 2030 management architecture, management requirements, management functional areas, the intent management framework, the autonomic characteristics, the AI/ML role in management and orchestration for Network 2030 are analysed. Refer to ITU-T Technical Specification [i.31] for more details.

- ITU-T Technical Report "Network 2030 - Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January 2020" [i.32] provides a description of demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day. An intent-based system was also demonstrated. Refer to ITU-T Technical Report [i.32] for more details.

Normative work resulting from the outcome of this Focus Group is being developed in ITU-T Study Group 13.

4.3.5.2 Focus Group on Autonomous Networks

ITU-T Focus Group on Autonomous Networks (FG-AN) was established by ITU-T Study Group 13 in December 2020, to serve as an open collaboration platform to research and study necessary pre-standardization works on the topic of autonomous networks. Its lifetime is set for one year from the first meeting but extensible if necessary. Its target is to study the meaning and characteristics of autonomous networks, study and propose technical enablers for evolution in autonomous networks, provide guidelines to enable higher levels of autonomy through real-time responsive experimentation, and specify architectures for adaptation in future networks to enable autonomy.

4.3.5.3 Recommendation ITU-T Y.3177

Recommendation ITU-T Y.3177 [i.33] specifies the architectural framework of Artificial Intelligence (AI)-based network automation for resource management and fault management in future networks including IMT-2020 (5G). This Recommendation provides high-level architecture of network automation for resource management and fault management with AI/ML, describes the resource management with AI/ML to achieve the agile control of network resources and the fault management with AI/ML to achieve the automation of network operations. Refer to Recommendation ITU-T Y.3177 [i.33] for more details.

4.3.5.4 ITU-T Y.IBN-reqts

ITU-T Draft Recommendation Y.IBN-reqts "Scenarios and requirements of Intent-Based Network for network evolution" [i.34] aims to study scenarios and requirements of Intent-Based Network for network evolution. This Recommendation was established by ITU-T Study Group 13 on Aug 2020, and planned to be completed in 2022 Q4. Its target is to study scenarios and workflow, capability requirements, general framework and model architecture of Intent-Based Network. Refer to ITU-T Draft Recommendation Y.IBN-reqts [i.34] for more details.

4.4 Closed loops automation applied to NFV framework

The zero-touch automation goal is to remove the need of human execution of manual tasks in the network operation and in the creation and delivery of services. The concept of the Closed-Loop Automation (CLA) was introduced as an approach employed towards reaching the zero-touch automation objectives.

In ETSI GS ZSM 009-1 [i.10], the CLA is depicted as: "a type of control mechanism that uses feedback signals to monitor and regulate itself with the objective of achieving a specific goal. Closed-loop automation (CLA) is the combination of automated processes with a closed feedback loop that aim at removing human interaction from the operation of a system.

Even though the ultimate objective of the CLA is zero human intervention, the autonomous systems still need to allow some specific interactions with the human workforce. In autonomous systems, human intervention is needed if a policy failed, for example. In cognitive systems, the system can, reactively or pro-actively, create a new policy simply based on its policy learning mechanisms, which is useful when a human intervention is not possible at a specific time e.g. during policy failure.

For certain tasks such as performing data science work to improve the models used for automating the operations, or for changing the business goals, or rejecting an action, the human operator might still be expected to interact with the autonomous system. To allow such interaction, the autonomous system will typically expose interfaces to allow the human operator to express expectations, such as the autonomous system's goals, requirements and constraints as well as to receive information (feedback) on status of the system and managed entities.

The Intent is the information object used on such interface and is thus essential in a highly autonomous, zero-touch system. The information exchanged between components used within a CLA can also benefit from using Intents as their information objects, hence simplify their interactions within a CLA.

In the management domain, the CLA is typically realized by chaining different management services, such as orchestration, management data analytics, intents and policies, knowledge base management, etc. The CLA outcome is to make a system autonomous, capable to continuously monitor its behaviour and performance, evaluate and take any necessary actions when the goals are not fulfilled.

For the NFV domain, the CLA follows the following main functional, and often circular, steps: monitoring and management data collection (as input), execution of actions as a result of CLA (output), and any number of analysis and decision-making steps as needed in between. The CLA logic and processes can involve any element of the NFV architectural framework, as well as the orchestration and management layers above NFV-MANO, or combinations of both.

This CLA concept in the NFVO domain is depicted in Figure 4.4-1.

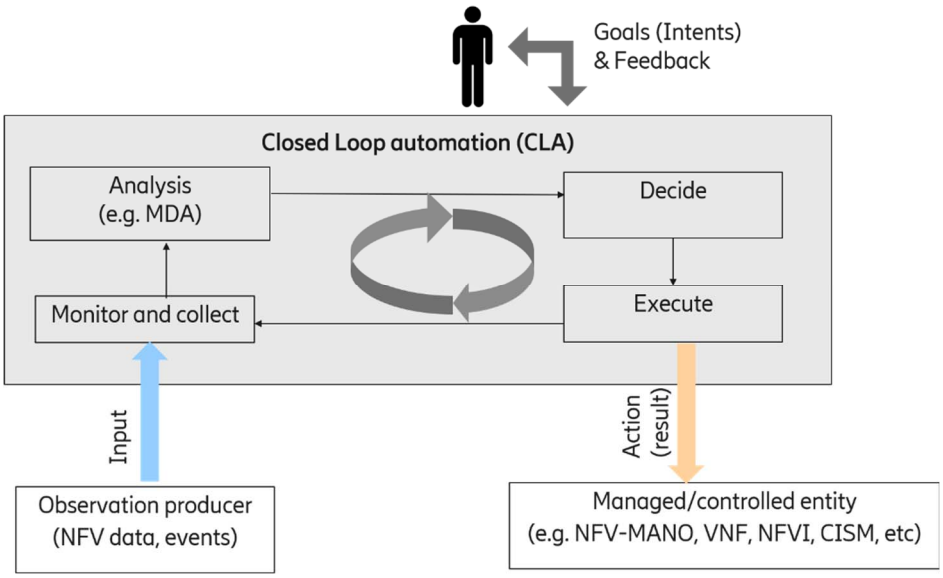

Figure 4.4-1: High-level overview of steps in an NFV closed loop

5 Use cases

5.1 Introduction

This clause enumerates the use cases for supporting autonomous management in NFV-MANO. Use cases in this clause are grouped into categories, to avoid potentially unlimited development of use cases with regards to broad connotation of automation. Some principles can also be applied for deriving use cases, such as less complexity of system operations, fast response to changes, reliable closed-loop decision making of the management domain and ease of interaction with consumers. The following categories of use cases are determined:

- Intent based network service management
- Management Data Analytics assisted management
- Autonomous container infrastructure management

The relationship of use case study principles and their derived use cases is depicted in Table 5.1-1.

Table 5.1-1: Principles and use cases relationship

Use case study principles	Use cases
Less complexity of system operations	Intent based NS management Autonomous container infrastructure management
Fast responses to changes	MDA assisted management Autonomous container infrastructure management
Reliable closed-loop decision making	Intent based NS management MDA assisted management
Ease of interaction with consumers	Intent based NS management MDA assisted management

5.2 Intent based network service management

5.2.1 Overview

Intent is a desire to reach a certain state/position for a specific entity, includes consumer expectations and goals e.g. for a service assurance or network deployment task (see 3GPP TR 28.812 [i.2], clause 3.1). It is expressed in a declarative way, without indicating how the system should realize it. An intelligent system is able to understand the intent of the consumer and translate it automatically into a concrete prescription of actions in the network.

Intent Management (IM) can be regarded as a role fulfilled by a set of logical functions that can be integrated in the NFV-MANO architecture, and does not necessarily mean any new functional block than the existing NFV-MANO functional blocks.

NFV-MANO can apply intent based management for simplifying the interaction between the OSS/BSS and NFV-MANO. The details of managing a Network Service (NS) are hidden in the NFV management domain, and not visible to the OSS/BSS. The OSS/BSS manages the intent and transmits it to NFV-MANO for the translation and fulfilment of the intent.

The following use cases on intent based NS management are included as input for analysis, but are not exhaustive:

- Intent based network service instantiation
- Intent based network service scaling
- Intent based network service termination

5.2.2 Intent based network service instantiation

5.2.2.1 Use case description

This use case describes a process of fulfilling an intent by initiating NS instantiation in NFV-MANO. Unlike the policy related to NS instantiation, the intent determined by the consumer of NFV-MANO functionality does not directly contain any request of NS instantiation, but addresses a high-level desire (customer-friendly and machine readable) which will be further interpreted to the concrete operations of NS instantiation executed by NFV-MANO.

A concrete example of the intent is the high-level functionality defined in the Network Service Descriptor (NSD) together with intended expected characteristics. The consumer of NFV-MANO functionality such as the OSS/BSS might not be aware of all the details of an NS as defined in NSD. It might only know the functionality delivered by the NS and it might want to deploy this NS for a certain performance, i.e. of a certain dimension determined by performance metrics. Moreover, the NSD typically can only cover a subset of all possible valid deployment options for an NS. Hence, it is also possible that the intended dimension cannot be satisfied with any of the deployment flavours already defined in the NSD. Accordingly, the consumer (OSS/BSS) requests the instantiation of an NS specifying intended dimensions of performance metrics rather than the deployment flavour.

This use case is described in a logical view, in which an actor and role "Intent Management" is introduced.

5.2.2.2 Actors and roles

Table 5.2.2.2-1 describes the use case actors and roles.

Table 5.2.2.2-1: Actors and roles for intent based NS instantiation

#	Role	Description
1	OSS/BSS	Determines an intent identifying NS functionality with certain dimensions of performance metrics and transfers it to NFV-MANO for fulfilment.
2	Intent Management	Interprets the intent and maps it to NS instantiation operations, generates an NS deployment flavour for the NSD that can satisfy the requested dimensions, transfers the NS instantiation operations to be executed by NFV-MANO and verifies that the intent is fulfilled by the execution of the NS instantiation operations.
3	NFV-MANO	Executes the NS instantiation operations using the generated NS deployment flavour to fulfil the intent.

5.2.2.3 Pre-conditions

Table 5.2.2.3-1 describes the use case pre-conditions.

Table 5.2.2.3-1: Pre-conditions for intent based NS instantiation

#	Pre-condition	Additional description
1	An NSD of the desired NS functionality has been on-boarded.	The NSD does not include a deployment flavour which could be used to satisfy the requested dimensions of the NS functionality.
2	The OSS/BSS accesses the NSD for fetching the NS functionality and determines an intent to be fulfilled.	The OSS/BSS expresses its intent as the required functionality which can be delivered by the NSD, together with the required dimensions specified as high-level performance metrics in association with the functionality delivered at the service access points, rather than identifying or generating a deployment flavour for the functionality.

5.2.2.4 Post-conditions

Table 5.2.2.4-1 describes the use case post-conditions.

Table 5.2.2.4-1: Post-conditions for intent based NS instantiation

#	Post-condition	Additional description
1	The intent identifying the NS functionality with certain dimensions is fulfilled.	This result expresses expectations, such as the autonomous system's NS related goals, requirements and constraints as well as to receive information.

5.2.2.5 Flow description

Table 5.2.2.5-1 describes the use case flow for intent based NS instantiation.

Table 5.2.2.5-1: Flow for intent based NS instantiation

#	Actor/Role	Action/Description
Begins when	OSS/BSS	The intent identifying the NS functionality with certain dimensions of performance metrics is available in the OSS/BSS.
Step 1	OSS/BSS -> NFV-MANO	The OSS/BSS transfers the intent to NFV-MANO for fulfilment.
Step 2	Intent Management	The Intent Management of NFV-MANO interprets the intent and maps it to instantiation operations of one or multiple NSs to be executed by NFV-MANO. Based on the NS functionality information of the NSD and the requested dimensions of the intent, the Intent Management selects the suitable VNF deployment flavours and generates an appropriate NS deployment flavour for the NS to be instantiated. The Intent Management of NFV-MANO may further include the generated NS deployment flavour in the NSD.
Step 3	NFV-MANO	NFV-MANO instantiates the NSs determined in step 2, including the instantiation of the constituent VNFs of the NSs with the selected VNF deployment flavours and the instantiation of the VLs of the needed dimensions.
Step 4	Intent Management	The Intent Management of NFV-MANO verifies that the intent is fulfilled by the availability of NS instance(s) satisfying the requested dimensions.
Step 5	NFV-MANO -> OSS/BSS	NFV-MANO returns the result of intent transfer to the OSS/BSS.
Ends when	OSS/BSS	The intent requested by the OSS/BSS is fulfilled.

5.2.3 Intent based network service scaling

5.2.3.1 Use case description

This use case describes a process of fulfilling an intent by initiating NS scaling in NFV-MANO. Similar to use case "intent based network service instantiation" in clause 5.2.2, a logical entity of "Intent Management" is introduced to represent an actor and role in the use case description. An intent is determined by the OSS/BSS and sent to NFV-MANO for fulfilment.

5.2.3.2 Actors and roles

The actors and roles the OSS/BSS, the Intent Management and NFV-MANO in clause 5.2.2 use case apply for this use case.

5.2.3.3 Pre-conditions

The pre-conditions in clause 5.2.2 use case apply for this use case, and the intent for initiating NS scaling operations may be different. An example of the intent applied in this use case may be, the OSS/BSS requests for an instantiated NS functionality with updated dimensions specified in association with the functionality delivered at the service access points.

5.2.3.4 Post-conditions

The post-conditions in clause 5.2.2 use case apply for this use case.

5.2.3.5 Flow description

The flow description in clause 5.2.2 use case applies for this use case, except that the NS LCM operations interpreted by the Intent Management of NFV-MANO is replaced by NS scaling. It is the logic of Intent Management to identify the semantics of different intents and interprets the intents to different NS LCM operations (e.g. NS instantiation, NS scaling) to be executed by NFV-MANO for fulfilling the intents.

5.2.4 Intent based network service termination

5.2.4.1 Use case description

This use case describes a process of fulfilling an intent by initiating NS termination operations in NFV-MANO.

5.2.4.2 Actors and roles

This use case is described in a logical view, in which an actor and role "Intent Management" is introduced. The actors and roles the OSS/BSS, the Intent Management and NFV-MANO in clause 5.2.2 use case apply for this use case.

5.2.4.3 Pre-conditions

Table 5.2.4.3-1 describes the use case pre-conditions.

Table 5.2.4.3-1: Pre-conditions for intent based NS termination

#	Pre-condition	Additional description
1	The OSS/BSS determines an intent to complete the usage of a deployed functionality.	

5.2.4.4 Post-conditions

Table 5.2.4.4-1 describes the use case post-conditions.

Table 5.2.4.4-1: Post-conditions for intent based NS termination

#	Post-condition	Additional description
1	The intent of completing the usage of deployed functionality is fulfilled.	

5.2.4.5 Flow description

Table 5.2.4.5-1: Flow for intent based NS termination

#	Actor/Role	Action/Description
Begins when	OSS/BSS	The intent of completing the usage of deployed functionality is available in the OSS/BSS.
Step 1	OSS/BSS -> NFV-MANO	The OSS/BSS transfers the intent to NFV-MANO for fulfilment.
Step 2	Intent Management	The Intent Management of NFV-MANO interprets the intent and maps it to termination operations of one or multiple NS instances to be executed by NFV-MANO, which fulfil the intent.
Step 3	NFV-MANO	NFV-MANO terminate the NS instances determined in step 2.
Step 4	Intent Management	The Intent Management of NFV-MANO verifies that the intent is fulfilled.
Step 5	NFV-MANO -> OSS/BSS	NFV-MANO returns the result of intent transfer to the OSS/BSS.
Ends when	OSS/BSS	The intent requested by the OSS/BSS is fulfilled.

5.3 Management Data Analytics assisted management

5.3.1 Overview

Management Data Analytics (MDA) is initially specified in ETSI TS 128 550 [i.13], which refers to management services using management analytical data in network and service management. The raw performance data of network functions can be analysed, together with other management data (e.g. alarm information, configuration data), and formed into one or more management analytical data for network functions, sub-networks, or network slice/sub-network slice instances. The MDA provides a capability of processing and analysing the raw data related to network and service events and status to provide analytics report to enable the necessary actions for network and service operations.

The MDA, in conjunction with Artificial Intelligence (AI) and Machine Learning (ML) techniques (as parts of internal implementation of the MDA), brings intelligence and automation to the network service management & orchestration. In the management domain of NFV-MANO, the closed-loop decision making capability of the management and orchestration can be improved by communication with the MDA function, which results in reduced on-demand management operations initiated by the OSS/BSS, and increased self-detection and/or self-recovery operations in the management domain.

The MDA provides two types of processing: the ML model training and the data analysis.

The following use cases on MDA assisted management are included as input for analysis, but are not exhaustive:

- Network service alarm incident analysis
- Network service health analysis
- Network service resource utilization analysis
- Cross administrative domain management data analytics
- Cross management domain NFV-MANO data analytics consumed by OSS/BSS

NOTE: ML model training is not explicitly described in clause 5 use cases, and use case in 3GPP TR 28.809 [i.3], clause 6.10.1.1 can be referenced.

5.3.2 Network service alarm incident analysis

5.3.2.1 Use case description

This use case describes the analysis of network service alarm incidents with assistance of the MDA function in NFV-MANO. With regards to complex topological relationship among the constituent components (i.e. the VNF, PNF and/or nested NS) of a network service, a series of alarms occurred in NFV-MANO may have the same root cause and be correlated with each other. Alarms can be propagated over multiple layers (the VIM, VNFM or NFVO) of a management domain if one source fault occurs. In addition, the same root cause may give rise to the performance deterioration of the NS as well.

To reduce the operations and maintenance complexity caused by a huge number of alarms, the alarms and deteriorated performance measurements should be analysed. Some AI/ML models and algorithms implemented by the MDA can be used to group or filter correlated alarms and indicate the root cause. The analytics report is finally returned to the consumer functional entities in NFV-MANO indicating the root cause of the alarms and deteriorated performance measurements.

5.3.2.2 Actors and roles

Table 5.3.2.2-1 describes the use case actors and roles.

Table 5.3.2.2-1: Actors and roles for network service alarm incident analysis

#	Role	Description
1	NFVO	Responsible for NS PM/FM, collect alarms and performance measurements in the management domain.
2	MDA	Perform root cause analysis for collected alarms and deteriorated performance measurements.

5.3.2.3 Pre-conditions

Table 5.3.2.3-1 describes the use case pre-conditions.

Table 5.3.2.3-1: Pre-conditions for network service alarm incident analysis

#	Pre-condition	Additional description
1	The MDA is equipped with AI/ML models and algorithms for root cause analysis of a NFV-MANO system. Historical alarms, performance measurements and NS topology data can be used as foreknowledge of the MDA.	
2	The NFVO collects alarms and performance measurements of the VNFs and/or nested NSs belonging to an NS from the underlying functional entities (e.g. the VNFM, the VIM).	

5.3.2.4 Post-conditions

Table 5.3.2.4-1 describes the use case post-conditions.

Table 5.3.2.4-1: Post-conditions for network service alarm incident analysis

#	Post-condition	Additional description
1	The report of NS alarm root cause analysis is returned to the NFVO.	

5.3.2.5 Flow description

Table 5.3.2.5-1 describes the use case flow for network service alarm incident analysis.

Table 5.3.2.5-1: Flow for network service alarm incident analysis

#	Actor/Role	Action/Description
Begins when	NFVO	The alarms and performance measurements related to an NS and its constituent components/infrastructure resources are available in the NFVO.
Step 1	NFVO -> MDA	The NFVO sends the alarms and performance measurements indicating a deterioration to the MDA for analysis of the root cause. See note.
Step 2	MDA	The MDA uses its internal AI/ML models and algorithms for analysing the input alarms and deteriorated performance measurements, and derives an analytics report including the root alarm or root cause of the NS fault.
Step 3	MDA -> NFVO	The MDA returns the analytics report to the NFVO.
Ends when	NFVO	The NFVO acknowledges the root cause of the NS alarm incidents, and can group the alarms, performance measurements with the root cause correspondingly.
NOTE: This process does not prevent the NFVO from immediately reporting any alarms to the OSS/BSS. The NFVO can further report the analytics report including the root alarm or root cause of the NS fault to the OSS/BSS after the MDA returns the result to the NFVO.		

5.3.3 Network service health analysis

5.3.3.1 Use case description

This use case describes the analysis of NS health with assistance of the MDA function to NFV-MANO. NS health is a high-level metrics of the NS runtime status, which reflects whether the NS runs normally or not during one period of its lifecycle. The MDA can collect NS health analysis required information in advance, or collect those information per request of NS health analysis from the NFVO. Based on the NS health analytics report of the MDA, the NFVO may further initiate lifecycle operations (e.g. NS scaling or healing) of an unhealthy NS to bring it back to its normal state.

5.3.3.2 Actors and roles

Table 5.3.3.2-1 describes the use case actors and roles.

Table 5.3.3.2-1: Actors and roles for network service health analysis

#	Role	Description
1	NFVO	Consumer who initiates a request for health analysis of a certain NS.
2	MDA	Producer who performs the operations for NS health analysis and returns the analysis output to the NFVO.

5.3.3.3 Pre-conditions

Table 5.3.3.3-1 describes the use case pre-conditions.

Table 5.3.3.3-1: Pre-conditions for network service health analysis

#	Pre-condition	Additional description
1	The MDA is equipped with AI/ML models and algorithms for NS health analysis. Historical alarms, performance measurements and NS topology data can be used as foreknowledge of the MDA.	

5.3.3.4 Post-conditions

Table 5.3.3.4-1 describes the use case post-conditions.

Table 5.3.3.4-1: Post-conditions for network service health analysis

#	Post-condition	Additional description
1	The report of NS health analysis is returned to the NFVO.	

5.3.3.5 Flow description

Table 5.3.3.5-1 describes the use case flow for network service health analysis.

Table 5.3.3.5-1: Flow for network service health analysis

#	Actor/Role	Action/Description
Begins when	NFVO	The NFVO determines to request the MDA to analyse the health of an NS in its management domain.
Step 1	NFVO -> MDA	The NFVO sends a request to the MDA for health analysis of a certain NS.
Step 2	MDA <-> NFVO, VNFM, VIM	The MDA interacts with other NFV-MANO functional entities (e.g. the NFVO, the VNFM and/or the VIM) to collect necessary information for NS health analysis (e.g. NS status, NS PM/FM information, indicators of VNFs, configurations related to the analysed NS).
Step 3	MDA	The MDA uses its internal AI/ML models and algorithms for analysing the input information collected in step 2, and derives an analytics report including the health state (e.g. healthy, unhealthy) and corresponding illustration of the health state of the NS.
Step 4	MDA -> NFVO	The MDA returns the analytics report to the NFVO.
Ends when	NFVO	The NFVO is aware of the health status of the NS.

5.3.4 Network service resource utilization analysis

5.3.4.1 Use case description

This use case describes the analysis of NS resource utilization with assistance of the MDA function. By grasping the resource utilization of an NS, the NFVO manages the resources in its management domain which serve multiple NSs in an efficient way. The MDA can collect NS resource utilization analysis required information periodically per analytics request from the NFVO. Based on the NS resource utilization analytics report of the MDA, the NFVO may further initiate operations for resolving NS resource utilization issues identified in the analysis, e.g. scale the NS or update corresponding NFV-MANO policies impacted by NS resource utilization issues.

5.3.4.2 Actors and roles

Table 5.3.4.2-1 describes the use case actors and roles.

Table 5.3.4.2-1: Actors and roles for network service resource utilization analysis

#	Role	Description
1	NFVO	Consumer who initiates a request for resource utilization analysis of a certain NS.
2	MDA	Producer who performs the operations for NS resource utilization analysis and returns the analytics report to the NFVO.

5.3.4.3 Pre-conditions

Table 5.3.4.3-1 describes the use case pre-conditions.

Table 5.3.4.3-1: Pre-conditions for network service resource utilization analysis

#	Pre-condition	Additional description
1	The MDA is equipped with AI/ML models and algorithms for NS resource utilization analysis. Historical alarms, performance measurements on resources and NS topology data can be used as foreknowledge of the MDA.	

5.3.4.4 Post-conditions

Table 5.3.4.4-1 describes the use case post-conditions.

Table 5.3.4.4-1: Post-conditions for network service resource utilization analysis

#	Post-condition	Additional description
1	The report of NS resource utilization analysis is returned to the NFVO.	

5.3.4.5 Flow description

Table 5.3.4.5-1 describes the use case flow for network service resource utilization analysis.

Table 5.3.4.5-1: Flow for network service resource utilization analysis

#	Actor/Role	Action/Description
Begins when	NFVO	The NFVO determines to have an analysis on the resource utilization of an NS.
Step 1	NFVO -> MDA	The NFVO sends a request to the MDA for analysing periodically resource utilization of a certain NS.
Step 2	MDA <-> NFVO, VNFM, VIM	The MDA interacts with corresponding NFV-MANO functional entities to collect necessary information for NS resource utilization analysis during a time period (the information may include virtual compute related measurements for each constituent VNF of the NS, network data volume related measurements of an SAP belonging to the NS, network data volume related measurements of an external CP belonging to the constituent VNF of the NS, indicators of constituent VNFs of the NS, etc.).
Step 3	MDA	The MDA uses its internal AI/ML models and algorithms for analysing the information collected in step 2, and derives an analytics report including the indication of under-utilized, over-utilized or normal utilization of certain type of resource (compute, storage or network) and optionally corresponding recommendations to resolve the resource utilization issues that be identified in the analytics report.
Step 4	MDA -> NFVO	The MDA returns the analytics report to the NFVO.
Ends when	NFVO	The NFVO is aware of the resource utilization of the NS during a time period.

5.3.5 Cross administrative domain management data analytics

5.3.5.1 Use case description

This use case describes an MDA process which occurs cross administrative domains in NFV-MANO. The analytics subject uses NS health analysis described in clause 5.3.3 as an example. The purpose of this process is to analyse the health of a composite NS in one administrative domain with assistance of the health analytics report of the nested NS in a different administrative domain. The MDA is assumed to be unaware of administrative domain and only communicates with the NFVO in the same administrative domain.

5.3.5.2 Actors and roles

Table 5.3.5.2-1 describes the use case actors and roles.

Table 5.3.5.2-1: Actors and roles for cross administrative domain MDA

#	Role	Description
1	NFVO-C	Consumer who initiates a request for health analysis of a certain composite NS in an administrative domain.
2	MDA-C	The MDA in the administrative domain of NFVO-C. Producer who performs the operations for health analysis and returns the analytics report for the composite NS to NFVO-C.
3	NFVO-N	The NFVO managing the nested NS in a different administrative domain, the nested NS is part of the composite NS. Consumer who initiates a request for health analysis of the nested NS in that administrative domain.
4	MDA-N	The MDA in the administrative domain of NFVO-N. Producer who performs the operations for health analysis and returns the analytics report for the nested NS to NFVO-N.

5.3.5.3 Pre-conditions

Table 5.3.5.3-1 describes the use case pre-conditions.

Table 5.3.5.3-1: Pre-conditions for cross administrative domain MDA

#	Pre-condition	Additional description
1	MDA-C/MDA-N is equipped with AI/ML models and algorithms for NS health analysis. Historical alarms, performance measurements and NS topology data in the administrative domain can be used as foreknowledge of the MDA.	

5.3.5.4 Post-conditions

Table 5.3.5.4-1 describes the use case post-conditions.

Table 5.3.5.4-1: Post-conditions for cross administrative domain MDA

#	Post-condition	Additional description
1	The report of health analysis on the composite NS is returned to NFVO-C.	

5.3.5.5 Flow description

Table 5.3.5.5-1 describes a possible use case flow for cross administrative domain MDA when the health analytics report of the nested NS from another administrative domain is assumed to be available in the administrative domain of the composite NS per request of MDA-C.

Table 5.3.5.5-1: Flow#1 for cross administrative domain MDA

#	Actor/Role	Action/Description
Begins when	NFVO-C	NFVO-C determines to request the MDA-C to analyse the health of a composite NS in its administrative domain.
Step 1	NFVO-C -> MDA-C	NFVO-C sends a request to MDA-C for health analysis of the composite NS.
Step 2	MDA-C <-> NFVO-C, VNFM, VIM	MDA-C interacts with NFV-MANO functional entities (e.g. NFVO-C, the VNFM and/or the VIM) in the same administrative domain to collect necessary information for NS health analysis (e.g. composite NS status, composite NS PM/FM information, indicators of constituent VNFs, configurations related to the analysed composite NS).
Step 2a	MDA-C <-> NFVO-C	Step 2 also includes an option that MDA-C requests NFVO-C for obtaining NS health analytics report of the nested NS(s) belonging to the composite NS.
Step 3	NFVO-C <-> NFVO-N	NFVO-C identifies the nested NS is deployed in a different administrative domain. NFVO-C interacts with NFVO-N via Or-Or reference point for obtaining NS health analytics report of the nested NS. This step implicitly includes the interaction between NFVO-N and MDA-N for NS health analysis of the nested NS in that administrative domain.
Step 4	NFVO-C <-> MDA-C	NFVO-C returns the health analytics report of the nested NS to MDA-C.
Step 5	MDA-C	MDA-C uses its internal AI/ML models and algorithms for analysing the input information collected in step 2 and step 4, and derives an analytics report including the health state (e.g. healthy, unhealthy) and corresponding illustration of the health state of the composite NS.
Step 6	MDA-C -> NFVO-C	MDA-C returns the analytics report to NFVO-C.
Ends when	NFVO-C	NFVO-C is aware of the health status of the composite NS.

Table 5.3.5.5-2 describes a possible use case flow for cross administrative domain MDA when the health analytics report of the nested NS from another administrative domain is assumed to be available in the administrative domain of the composite NS prior to the request of MDA-C.

Table 5.3.5.5-2: Flow #2 for cross administrative domain MDA

#	Actor/Role	Action/Description
Begins when	NFVO-C	NFVO-C determines the need to analyse the health of a composite NS and determines the part of the composite NS that uses nested NS in a different administrative domain.
Step 1	NFVO-C <-> NFVO-N	NFVO-C interacts with NFVO-N via Or-Or reference point for obtaining NS health analytics report of the nested NS. This step implicitly includes the interaction between NFVO-N and MDA-N for NS health analysis of the nested NS in that administrative domain.
Step 2	NFVO-C -> MDA-C	NFVO-C sends a request to MDA-C for health analysis of the composite NS. The request includes as input the NS health analytics report of the nested NS.
Step 3	MDA-C <-> NFVO-C, VNFM, VIM	MDA-C interacts with other NFV-MANO functional entities (e.g. NFVO-C, the VNFM and/or the VIM) in the same administrative domain to collect necessary information for NS health analysis (e.g. composite NS status, composite NS PM/FM information, indicators of constituent VNFs, configurations related to the analysed composite NS).
Step 4	MDA-C	MDA-C uses its internal AI/ML models and algorithms for analysing the input information collected in step 2 and step 3, and derives an analytics report including the health state (e.g. healthy, unhealthy) and corresponding illustration of the health state of the composite NS.
Step 5	MDA-C -> NFVO-C	MDA-C returns the analytics report to NFVO-C.
Ends when	NFVO-C	NFVO-C is aware of the health status of the composite NS.

5.3.6 Cross management domain NFV-MANO data analytics consumed by the OSS/BSS

5.3.6.1 Use case description

This use case is similar to the cross-administrative domain MDA use case described in clause 5.3.5 of the present document, with the exception that the consumer of the MDA analytics on NS analytics data is not the NFVO, but another management function in the OSS/BSS.

The purpose of this process is to provide an analytics report containing the analysis requested, e.g. for the virtualised resource utilization of an NS instance, or the health for that NS instance, estimation of future availability of resources for NSs, etc.

When the 3GPP subnet slice uses an NS instance, the MDA analytics reports for the virtualised resources used by that NS instance can be used by OSS management functions as input, into the context of their overall decisions. As described in 3GPP TR 28.809 [i.3], clause 6.2, some of the typical resource analytics, including virtual resources, used by the OSS management functions include resource utilization, shortage or excess, allocation or reservation for a specific network subnet slice.

This use case describes the request from the OSS/BSS management functions, for the needed analytics reports from the MDA functions that work with NFV-MANO domain specific data. The request is fulfilled when the analytics report is provided by MDA to the OSS/BSS.

5.3.6.2 Actors and roles

Table 5.3.6.2-1 describes the use case actors and roles.

Table 5.3.6.2-1: Actors and roles for MDA analytics reports on NS virtualised resources utilization, consumed by the OSS/BSS

#	Role	Description
1	OSS/BSS	Consumer who initiates an NS analytics request, e.g. for virtualised resource utilization analysis of an NS instance over a given period of time.
2	MDA	The MDA functions which have the knowledge of NFV-MANO data and the capability to process NS data analytics reports and recommendations, including the NS virtualised resources utilization analysis.
3	NFVO	The NFVO managing the NS instance for which the analytics report is requested by OSS/BSS.
4	VNFM	The VNFMs that are managing the VNF instances that are part of the NS instance.
5	VIM	The VIMs that are managing the infrastructure virtualised resources used by constituents of the NS instance.

5.3.6.3 Pre-conditions

Table 5.3.6.3-1 describes the use case pre-conditions.

Table 5.3.6.3-1: Pre-conditions for MDA analytics reports on NS virtualised resources utilization, consumed by the OSS/BSS

#	Pre-condition	Additional description
1	The MDA is equipped with the required AI/ML models, algorithms and can access a knowledge base with previous analytics reports recommendations that used as input previously collected NFV-MANO data and context, which can be further used as reference in the process of the analysis of the NS virtualised resources utilization.	
2	The MDA has access to NFV-MANO data collected/managed by the NFVO, VNFMs and VIMs.	

5.3.6.4 Post-conditions

Table 5.3.6.4-1 describes the use case post-conditions.

Table 5.3.6.4-1: Post-conditions for MDA analytics reports on NS virtualised resources utilization, consumed by the OSS/BSS

#	Post-condition	Additional description
1	The report of NS instance resource utilization analysis is returned to the OSS/BSS.	

5.3.6.5 Flow description

Table 5.3.6.5-1 describes a possible use case flow for MDA reports on virtualised resource utilization analysis of an NS instance, requested by other OSS/BSS management function/s (as MDA consumer/s).

Table 5.3.6.5-1: Flow on MDA analytics reports on NS virtualised resources utilization, consumed by the OSS/BSS

#	Actor/Role	Action/Description
Begins when	OSS/BSS	The OSS/BSS identifies the need to use resource utilization analytics report for an NS instance that is being used for a network subnet slice.
Step 1	OSS/BSS -> MDA	The OSS/BSS sends a request to the MDA for the virtualised resource utilization analytics of the NS instance.
Step 2	MDA <-> NFV-MANO functional entities	The MDA interacts with NFV-MANO functional entities (e.g. the NFVO, VNFM, CISM, WIM and/or VIM) to collect necessary information for the given NS instance's resource utilization over the requested period. That can include, but not restricted to, the NS instance's PM/FM information, indicators of constituent VNFs, configurations related to the analysed NS instance, NS instance runtime information over the requested period of time.
Step 3	MDA	The MDA uses its internal AI/ML models, algorithms and analytics knowledge base to analyse the input information collected in step 2. The MDA generates an analytics report on the NS instance virtualised resource utilization within the requested period of time, together with the recommended actions for improvement (e.g. scaling out shortly ahead of known peak hours, a better resource allocation for the NS instance based on past history and learned behaviour, such as patterns of the past LCM actions on this NS instance, or NS instances with similar resource requirements).
Step 4	MDA -> OSS/BSS	The MDA returns the analytics report to the OSS/BSS.
Ends when		The OSS/BSS has received from MDA the analytics report on the NS instance virtualised resource utilization.

5.4 Autonomous container infrastructure management

5.4.1 Overview

The Container Infrastructure Service Management (CISM) function, whose management service interface requirements are specified in ETSI GS NFV-IFA 040 [i.14], provides services for NFV-MANO to manage container infrastructure in an intent based, declarative way. As one de-facto standard solution of the CISM, Kubernetes® implements container resource management, Pod scheduling, elastic scaling, security control, system monitoring and error correction of containerized workloads in an autonomous manner. With assistance of the CISM, the existing NFV-MANO functional entities like the NFVO or the VNFM are freed from complex container infrastructure management, and can focus on management logic of the containerized workloads and network services constructed of the containerized workloads.

The following use cases on autonomous container infrastructure management are included as input for analysis, but are not exhaustive:

- Auto-scaling of the Managed Container Infrastructure Object (MCIO)

- Auto-repairing CIS cluster nodes
- Auto-upgrading CIS cluster nodes

5.4.2 Auto-scaling of the MCIO

5.4.2.1 Use case description

This use case describes a process of auto-scaling of the MCIO in the CISM. Other NFV-MANO functional entities (e.g. the NFVO or the VNFM) are not involved in this process.

As a pre-condition of this use case, the CISM is allocated with sufficient infrastructure resources (either VMs or bare metal) for managing its CIS instances. The NFVO can also configure a policy of MCIO auto-scaling (e.g. the threshold of the monitored MCIO metrics for trigging MCIO auto-scaling) to the CISM in advance. After the containerized VNF is instantiated, the CISM monitors the performance metrics of each MCIO invoked by the VNF, e.g. the CPU usage of the MCIO. When the performance metrics of the MCIO exceeds a threshold (determined by the policy), the CISM triggers the execution of scaling in/down or out/up of the MCIO, which eventually results in the decrease or increase of infrastructure resources assigned to the MCIO. Neither the NFVO nor the VNFM is aware of the change of MCIO infrastructure resources during this process.

An example of MCIO auto-scaling in de-facto standards is the Horizontal Pod Autoscaler (HPA) or Vertical Pod Autoscaler (VPA) function in Kubernetes®.

5.4.3 Auto-repairing CIS cluster nodes

5.4.3.1 Use case description

This use case describes the process of auto-repairing Container Infrastructure Service (CIS) cluster nodes managed by the CIS Cluster Management (CCM). The CCM periodically monitors the health status of each CIS cluster node in the CIS cluster, and initiates a repair process for the CIS cluster node which has failed consecutive health checks over an extended time period.

The CCM uses the CIS cluster node's health status to determine if a CIS cluster node needs to be repaired. A CIS cluster node in unhealthy status may refer to the cases that:

- A CIS cluster node reports a "NotReady" status on consecutive check over the given time threshold.
- A CIS cluster node does not report any status at all over the given time threshold.
- A CIS cluster node's boot disk is out of disk space for an extended time period.

If the CCM detects that a CIS cluster node needs to be repaired, the CIS cluster node is evacuated and re-created. The CCM waits for a time period for the evacuation to complete. If the evacuation does not complete, the CIS cluster node is shut down and a new CIS cluster node is created.

If multiple CIS cluster nodes require repair, the CCM might repair CIS cluster nodes in parallel. The CCM balances the number of repairs depending on the size of the CIS cluster and the number of broken CIS cluster nodes. The CCM will repair more CIS cluster nodes in parallel on a larger CIS cluster, but fewer CIS cluster nodes as the number of unhealthy CIS cluster nodes grows.

An example of auto-repairing CIS cluster nodes is "Auto-repairing nodes" function in Google® Kubernetes® Engine (GKE).

5.4.4 Auto-upgrading CIS cluster nodes

5.4.4.1 Use case description

This use case describes the process of auto-upgrading CIS cluster nodes managed by the CCM. The process keeps the nodes in a CIS cluster up to date with the version of the CISM when the CISM function is upgraded.

As part of the lifecycle of a CIS cluster, the CISM function is often upgraded to its latest version, e.g. to apply the latest CISM security release, or get the latest features. Upgrade of CIS cluster nodes managed by the CCM is triggered as part of the upgrade of the CISM automatically. The nodes in the CIS cluster are scheduled by the CCM for upgrades when they meet certain selection criteria. Meanwhile, the containerized workloads running on the CIS cluster nodes to be upgraded should be minimally disrupted by this process. When a CIS cluster node is being upgraded, the new MCIOs are not scheduled onto it but be scheduled onto other CIS cluster nodes which are not in the process of upgrade. A component external to the CIS cluster monitors the upgrade of CIS cluster nodes. The upgrade completes when all selected nodes in the CIS cluster have been upgraded to the version which fits in with the version the CISM to be updated.

An example of auto-upgrading CIS cluster nodes is "Auto-upgrading nodes" function in Google® Kubernetes® Engine (GKE).

6 Key issue analysis

6.1 Introduction

In the present clause, key issues related to clause 5 use cases are identified and analysed, and potential solutions of NFV-MANO functionality enhancement are proposed for resolving key issues. The key issues and potential solutions are organized for each category of NFV-MANO autonomous management use cases.

6.2 Key issues on intent based NS management

6.2.1 Key issue #1: Intent for NFV-MANO in a layered management architecture

3GPP TR 28.812 [i.2], clause 4.1.2.4 identifies different roles associated with several management layers. Navigating top-down through the orchestration layers using intents between them, this study has identified several roles: Communication Service Customer (Intent-CSC), Communication Service Provider (Intent-CSP) or Network Operator (Intent-NOP). The top level intents are the CSC's business goals. Conversely, the lower the hierarchy position of an intent, the more it reflects a concrete requirement for the network. There are also other intent scenarios for different levels of operators, e.g. intents from Infrastructure Operator, intents from (application) Service Provider on top of data center of Network Operator. Those intent scenarios are out of the scope of this study.

An example of the intents applied for NFV-MANO is the intent received from Network Operator (Intent-NOP). It enables the Network Operator to deploy or maintain an NS without knowing how the detailed management operations (including the usage of NFV templates like NS deployment flavour during the process) will be initiated and executed in the domain of NFV-MANO. The Network Operator expresses the intent as a requirement to the NS functionality and desired dimensions of performance metrics via the OSS/BSS, then the intent is transferred to NFV-MANO and interpreted by the Intent Management of NFV-MANO to concrete management operations (e.g. NS LCM) to be executed in NFV-MANO. NFV-MANO returns the feedback information on the fulfilment of the intent to the Network Operator.

As an example, the intent applied for NFV-MANO is handling the needs of the Network Slice Subnet Management Function (NSSMF) to consume NS LCM operations provided by NFV-MANO.

6.2.2 Key issue #2: Relation with policy management in NFV-MANO

Policy management interface has been specified for each reference point in NFV-MANO. By using a policy management interface operation, a higher layer functional entity (acting as Policy Administration Point) can transfer a policy expressing the management logic in either "what to do" or "how to do" to a lower layer functional entity (acting as Policy Function) for the execution.

Furthermore, a policy can also be encapsulated in an NFV template for addressing a pre-defined rule to achieve a goal, such as affinity/anti-affinity rules, auto-scale/auto-heal rules specified in the VNFD. Both functional entities acting as Policy Administration Point (PAP) and Policy Function (PF) use an information model of policy management in the same level of granularity (like a common language or very close background knowledge) in communicating with each other.

Unlike with the policies, the consumer of Intent Management expresses its intent in a more abstract level of information which does not indicate to the producer of Intent Management how to fulfil the goals expressed in the intent. That is the reason why an interpretation or translation function is necessary to be included in the Intent Management.

One main motivation to introduce intent based NS management to NFV-MANO is the increase of management complexity in the evolution towards cloud-native, in which multiple forms of VNFs (e.g. VM based VNFs, containerized VNFs) and heterogeneous infrastructure resource services rush into the framework of NFV-MANO.

With the assistance of Intent Management of NFV-MANO, the consumer of NFV-MANO functions (e.g. the OSS/BSS) can simplify its management views with more focus on managing global, high-level management goals in a consistent way.

In its realization, the Intent Management can make use of static (meaning pre-defined and configured) IM related policies to interpret the Intent and to decide how to infer the set of actions to fulfil the Intent. Intent Management can also make use of dynamic policies and of intelligent functions that are capable to dynamically learn from Intent Management's handling of Intents.

Intent based NS management can work side by side with policy management in the framework of NFV-MANO. For the comparison and compatibility analysis in the present clause, policies at the NS level that can be onboarded onto the NFVO using the policy management framework are hereafter referred in the present clause as NS management policies. Intent was originally seen to be similar to a declarative policy (compared to imperative policy such as an event-condition-action rule). The intent concept has evolved in time into a knowledge object, with different modelling needs beyond policies. Policies handled via the policy management framework (as a part of the system's overall decision-making mechanisms, e.g. by indicating certain actions when given conditions occur) are complementary to intents and can be used as part of the intents handling process, in conjunction with other factors and with support from intelligent functions.

When NFV-MANO detects that an NS LCM operation recommended by the Intent Management of NFV-MANO has a conflict in the targeted actions (e.g. interferes with other actions requested on the same NS instance, or on resources belonging to the same NS instance, or with the outcomes of NS management policies), NFV-MANO reports this conflict event to its upper layer management entities (e.g. the OSS/BSS). The conflict resolution can be handled in the following forms:

- OSS/BSS Upper-layer handling: It depends on the logic of upper layer management entities to further decide whether to update a new intent with no conflict, or update the applicable IM related policies, or to update the NS management policies to mitigate the conflicts detected for that intent.

- Intent Management handling: The Intent Management, as receiver or processor of the outcome of a conflicting action (e.g. via a NS LCM Coordination notifications, or NS LCM notifications) can further process such an outcome, reassess and derive a new set of actions that can fulfil the Intent and are expected to resolve the conflict, and then request their execution to NFV-MANO. In addition, and as way to avoid deriving possible conflicting actions, the Intent management could pro-actively retrieve and interpret the NS management policies during the intent handling and use them to derive non-conflicting actions. The Intent Management can also escalate if it cannot resolve the conflict by itself, to the upper layer OSS/BSS management entities to inform that the intent fulfilment has failed. The Intent Management can potentially evaluate alternative intents with equivalent or similar goals and expectations as the originally received intent and include them as suggested alternatives in the intent fulfilment report.

6.2.3 Key issue #3: Management operations of intent

According to the description of use cases in clause 5.2, there exists a common procedure of transferring an intent from the OSS/BSS to NFV-MANO for fulfilment. From the producer of Intent Management (NFV-MANO) point of view, it provides service interfaces on intent management and exposes these services to the consumer of Intent Management (the OSS/BSS). Similar to generic use case study on policy management in clauses 5.2 to 5.7 of ETSI GR NFV-IFA 023 [i.15], service interfaces on intent management can include the following CRUD operations on intent:

- Create intent
- Query intent
- Delete intent
- Subscription /notification related to intent management
- Reporting on intent fulfilment

NOTE 1: The request of an intent is assumed to be always one-time and does not happen cyclically, therefore activate/deactivate operations do not apply for intent management.

NOTE 2: Among CRUD operations, update operation can always be regarded as a combination of deletion operation and creation operation. An intent should contain a complete desire or goal for fulfilment. Following this assumption, an updated intent will be regarded as a new intent to be created and then there is no need to specify update intent operation on Intent Management interface. This is also aligned with analysis on operations and/or notifications used for intent in clause 6.2 of 3GPP TR 28.812 [i.2].

It is the semantics encapsulated in the intent that determines which NS management operations to map for the fulfilment of intent, such as the intent semantics "the NS functionality delivered by the NSD together with high-level performance metrics in association with the functionality delivered at the service access points" for mapping to NS instantiation operations in clause 5.2.2, and the intent semantics "an instantiated NS functionality with updated dimensions specified in association with the functionality delivered at the service access points" for deriving NS scaling operations in clause 5.2.3. There are no association or dependency on execution between certain Intent Management operations provided by NFV-MANO and certain NS management operations interpreted from the intent, e.g. the creation of an intent does not imply accompanying an NS instantiation operation, and the deletion of an intent does not imply following an NS termination operation. The use cases in clause 5.2 describe independent NS lifecycle management operations derived from the transfer of different intents.

6.2.4 Key issue #4: Design of information model for intent

The intent, a kind of declarative policy, specifies the goals to be achieved. There are two alternatives to determine the information model of an intent.

The first alternative comes from the study of 3GPP TR 28.812 [i.2], the intent is modelled as Intent Expression which includes both Intent Driven Object and Intent Driven Action. Intent Driven Object provides the management object information according to intent requirements, and Intent Driven Action provides abstract and simplified network operation information according to intent requirements.

Adapting this modelling to the scenarios of intent based NS management in the present document, Intent Driven Object can be NSs or other managed objects in the NS level, e.g. NSD. Intent Driven Action can be related to one or multiple lifecycle management operations acting on the NSs, e.g. instantiation, scaling. Management operations encapsulated in Intent Driven Action can also be represented by high-level and abstract operations, e.g. deploy an NS.

There is another alternative for designing the information model for intent, in which the intent is represented by Intent Driven Object and its desired state. The examples of intent in use case description of clauses 5.2.2, 5.2.3 and 5.2.4 can be categorized into this modelling. The producer of Intent Management (NFV-MANO) maintains a state machine in a certain dimension of Intent Driven Object, such as performance metrics of the NS in clause 5.2. With the change of the state of Intent Driven Object, the producer of Intent Management will derive corresponding actions to execute, which finally achieves the desired state addressed in the intent. In this alternative, the consumer of Intent Management (the OSS/BSS) will not directly initiate Intent Driven Actions (as a part of intent creation), but will express the desired state of the Intent Driven Object, which is interpreted by the producer of Intent Management to corresponding actions aiming to change the current state to the desired state.

In both alternatives, the consumer of the Intent Management monitors the progress of actions, e.g. by subscribing to corresponding notifications.

6.2.5 Summary of potential solutions

This clause provides potential solutions for fulfilling intent based NS management from the perspective of a functional view, according to key issue analysis in the previous sub-clauses of clause 6.2. A logical function Intent Management is introduced in NFV-MANO. NFV-MANO receives the intent from its consumers (i.e. the OSS/BSS) and the Intent Management of NFV-MANO interprets the intent to corresponding NS management operations to be executed by NFV-MANO, which eventually fulfil the intent.

CRUD operations of intent include:

- Create intent: An intent is newly created in the Intent Management of NFV-MANO.
- Query intent: The information of an intent is queried.
- Delete intent: An intent is outdated and will not express the goal of the consumer any more, therefore it is deleted.
- Subscription/Notification related to intent management: Consumers (e.g. the OSS/BSS) subscribe to the notifications related to changes of intent management, and NFV-MANO sends subscribed notifications to consumers when the corresponding events occurs.
- Reporting on intent fulfilment: The intent fulfilment is reported by the Intent Management.

An intent is represented by one or more Intent Driven Objects and their desired states.

6.3 Key issues on MDA assisted management

6.3.1 Key issue #1: MDA role in NFV-MANO domain

In the study of 3GPP TR 28.809 [i.3], clause 5.1, the MDA plays a role of Analytics in the management loop (which consists of the closed loop of Observation, Analytics, Decision and Execution). The MDA adds intelligent functions and generates value by processing and analysis of management and network data, where the AI and ML techniques may be utilized.

With regards to an administrative domain of NFV-MANO, the introduction of MDA function aims at supporting the NFVO in the process of making autonomous closed-loop decisions related to NSs it manages. The NFVO is a centralized functional entity in the NFV-MANO administrative domain, and it creates a huge number of complex communications with its subordinate entities (e.g. the VNFM, VIM, WIM or CISM) and has a global view on the underlying infrastructure resources and constituent VNFs belonging to an NS. Therefore, the NFVO plays a role of Decision in the management loop and be assisted with Analytics role provided by the MDA function.

The MDA function is management domain specific. No matter whether a management domain is categorized vertically (e.g. the category of CSMF, NSMF or NSSMF in 3GPP slice management) or horizontally (e.g. Core Network management domain, Transport Network management domain or RAN management domain), a domain specific MDA function is associated with the analytics capability for the data of that management domain. The analytics can be used for improving autonomous management in that management domain, as well as an input to autonomics improvements and decisions in the wider scope of the OSS/BSS management domain.

The MDA function in context of the present document will focus on collecting, processing and analysing information in the NFV-MANO administrative domain and providing analytics report for each subject of analytics (e.g. NS health analysis) to the NFVO.

6.3.2 Key issue #2: Information collection mechanism used by the MDA

When the MDA receives a request from the NFVO for analytics of a certain subject, it collects necessary information from its surrounding NFV-MANO functional entities. There are two basic mechanisms which can be used by the MDA for information collection: Request/Response and Subscription/Notification. Compared with Request/Response mechanism, Subscription/Notification is more efficient in information collection among a big range of information samples in a management domain, since it decouples the producers and consumers of notification events related to collected information. The producers can return the collected information asynchronously with the subscription to the information initiated by the consumer.

The MDA has the knowledge to determine which information to be collected according to a subject to be analysed. Then it initiates subscription requests to corresponding NFV-MANO functional entities for collecting the information. NFV-MANO functional entities return subscription responses to the MDA for the confirmation of subscriptions. When corresponding events related to collected information occurs and be available in the NFV-MANO functional entity, the NFV-MANO functional entity sends a notification containing the collected information to the MDA.

6.3.3 Key issue #3: NFVO as a consumer of analytics

MDA is a logical component which can be part of the management loops (either open or closed loops). The MDA provides intelligence and exposes the analytics report of the management and resource data it has collected.

The MDA services can be offered to MDA consumers in several ways. In order to optimize the accuracy of the MDA outputs, the MDA could rely on Machine Learning (ML) technologies, which in some cases might require the involvement of the consumer.

NFV-MANO can also be a consumer of the results of the management data analytics provided by an MDA. As example, the NFVO can consume analytics data for NS lifecycle management purposes, in which case the NFVO requests analytics for specific resources, management objectives (e.g. NS LCM with certain characteristics) and a given time window.

The MDA processes the data according to the request and will use asynchronous operation(s) to return analytics report, as shown in the example depicted in Figure 6.3.3-1 below.

When the MDA receives the Analytics request from the NFVO, the MDA returns an Analytics response to the NFVO but it does not include the result of analytics in the response. Instead, the MDA sends a notification to the NFVO to indicate the start of asynchronous operation of analytics. The MDA then executes the information collection and the data analysis according to its internal algorithms. As a result, the MDA sends a notification to the NFVO to indicate the end of asynchronous operation of analytics, and includes analytics report in that notification.

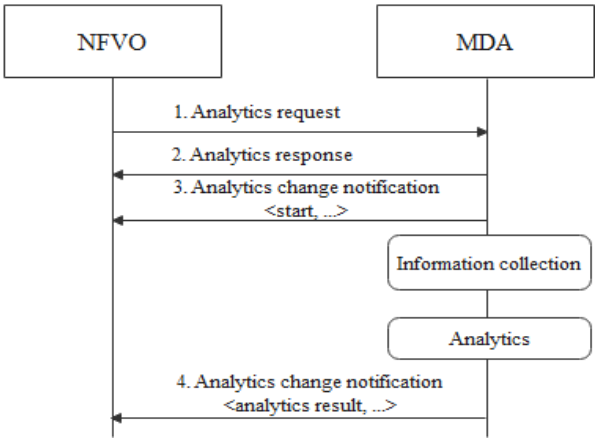

Figure 6.3.3-1: Analytics reporting mechanism

6.3.4 Key issue #4: Input data for the MDA process

Input data provided for the MDA is analytics subject specific. 3GPP TR 28.809 [i.3] clause 6 studies a couple of MDA use cases and investigates the input data required for each use case. In the present document, it is not intended to study input data for each MDA use case described in clause 5.3, but analyse what categories of management data or information in NFV-MANO can be used as input data for the MDA from a general standardization perspective. This will help to identify the gap of current specifications for fulfilling input data for the MDA, on what category of input data is already in the specifications, what is missing and might be further added to the specifications for fulfilling the MDA.

The following categories of data in NFV-MANO can be used as input data for the MDA:

- Performance measurement data specified in ETSI GS NFV-IFA 027 [i.16], on the NFV object of SAP, VNF, VNFC, Virtual Compute, Virtual Storage, Virtual Network, VNF internal CP and VNF external CP.
- Alarms specified by fault management interface in ETSI GS NFV-IFA 005 [i.17], ETSI GS NFV-IFA 006 [i.18], ETSI GS NFV-IFA 007 [i.19], ETSI GS NFV-IFA 013 [i.20], especially for MDA use cases related to fault root cause analysis/alarm incident correlation analysis.
- Configurations related to the analysed NS and its constituent VNFs specified in ETSI GS NFV-IFA 013 [i.20] and ETSI GS NFV-IFA 007 [i.19].
- Runtime NFV object instance information, such as VNFInfo specified in ETSI GS NFV-IFA 007 [i.19], NSInfo specified in ETSI GS NFV-IFA 013 [i.20] and any update of the information.
- Indicators of constituent VNFs specified in ETSI GS NFV-IFA 008 [i.36].
- Analytics report in a multiple administrative domain NS management scenario, in which the analytics report from an MDA in administrative domain in which the nested NS is deployed can be input for the MDA in administrative domain in which the composite NS is deployed.

Operational and historical data such as LCM operations performed in the administrative domain.

6.3.5 Key issue #5: Output data from the MDA process

Analytics report as output data from the MDA is analytics subject specific as well. 3GPP TR 28.809 [i.3], clause 6 elaborates the output data for each use case, which includes a series of 3GPP domain-specific target metrics (specific to that analytics subject) to evaluate the results of analytics and optionally recommended next step actions.

The MDA which processes the NFV-MANO data analytics acts on the domain-specific data of the NFV-MANO management domain.

From standardization point of view, it is more appropriate to define the output data specification from the MDA in an abstraction level of information modelling. The concrete target evaluation metrics (e.g. list of correlated alarms, root cause or root alarms, affected objects in NS alarm incident analysis) and recommended actions should be represented by abstracted information elements and not be exposed to the external management interface transferring the output data. Aggregated information elements of evaluation metrics on the results of analytics and recommended actions can be specified for representing analytics report. Recommended actions of the analytics report can include identification information of the recommended action(s), optionally human readable descriptions of the action(s), associated analytics subject and additional parameters associated to the action(s), which are further used by the MDA consumer for deriving follow-up actions.

The benefits of the NFV-MANO analytics are expected not only as a support to augment the NFVO level of autonomy but to also contribute to increasing the autonomy of overall OSS/BSS.

A generic meta-model for MDA analytics reports facilitates analytics consumption within OSS and enables closed loop automation that traverses OSS/BSS management domains. Then each management domain is left with the task to determine, define and populate, its own domain-specific data in the analytics reports.

6.3.6 Key issue #6: ML model training for the MDA

The MDA is equipped with Machine Learning (ML) model for deriving analytics report of a certain analytics subject from the analytics input information. The ML model needs to be trained to align the analytics report of the MDA with the MDA consumer's expected output. 3GPP TR 28.809 [i.3] analyses the basic ML model training process for MDAS, in which the MDAS consumer is involved in the ML model training to help refine the data and improve the analytics accuracy.

As a consumer of MDA analytics, NFV-MANO (e.g. the NFVO, VNFM or VIM) provides the training data including training input and the desired output to the MDA for training ML model. The MDA returns an ML model training report as the output data of training to NFV-MANO (i.e. the NFVO). NFV-MANO can also validate the training output data provided by the MDA, and provide the validation data as feedback to the MDA. The MDA will use the validation data for further ML model training with historical data that are used to generate the validated output data.

Input data described in clause 6.3.4 can be reused as training input for ML model training. Different subset of input data will be selected for different analytics subjects. Furthermore, NFV object templates such as VNFD or NSD can also be used as training input, which assist for the establishment of the basic and relatively stable part of ML model independent of analytics subjects.

Output data described in clause 6.3.5 can be reused as training output for ML model training. The training output includes the analytics report of a certain subject that the ML model should aim to achieve based on the training input.

6.3.7 Summary of potential solutions

This clause provides potential solutions for fulfilling MDA assisted management from the perspective of a functional view, according to key issue analysis in the previous sub-clauses of clause 6.3.

A logical function Management Data Analytics (MDA) is introduced in NFV-MANO and the MDA function in the context of the present document is specific to NFV-MANO administrative domain. The MDA provides two types of processing to its analytics consumers: the ML model training and data analytics.

In respect of data analytics, the MDA receives the request for analytics of a certain subject from its analytics consumer, and collects input information for data analytics from its surrounding NFV-MANO functional entities (e.g. the NFVO, VNFM, CISM, WIM and VIM) in the same administrative domain, and returns analytics report to its analytics consumer after executing a set of asynchronous operations of analytics.

The input information used for MDA data analytics can include PM/FM data spread in NFV-MANO, runtime NFV object instance information such as VnfInfo and NsInfo, analytics report from an administrative domain in which the nested NS is deployed. The output data from MDA data analytics can include aggregated information that represent the results of the analytics and recommended actions in analytics report.

In respect to ML model training, the MDA receives the request for training ML model from its analytics consumer, which provides training data including training input and desired output of the training. The MDA returns an ML model training report as the output data of training to its analytics consumer. However, as more study is expected on ML modelling and their specific training actions required, the ML training functionality is left for a later stage.

6.4 Key issues on autonomous container infrastructure management

6.4.1 Key issue #1: mechanism of MCIO policy configuration

ETSI GS NFV-IFA040 [i.14] has specified the CISM northbound interface for configuring policies for MCIOs, which is finally consumed by the NFVO. This is a basic mechanism to support autonomous container infrastructure management (e.g. auto-scaling of the MCIO, auto-repairing CIS cluster nodes). In this case, neither the NFVO nor the VNFM initiates MCIO related scaling or healing interface operations (associated with the change of infrastructure resources consumed by the MCIO) to the CISM, instead, the NFVO configures corresponding MCIO policies to the CISM in advance for providing necessary guidance in the autonomous container infrastructure management performed by the CISM.

6.4.2 Key issue #2: Desired state of the MCIO

As specified in ETSI GS NFV-IFA 040 [i.14], MCIO is characterized by the desired state and actual state of a containerized workload. The desired state of an MCIO is specified in a declarative descriptor which is interpreted by the CISM. MCIOs are lifecycle managed via change requests on their desired state, utilizing a modified declarative descriptor sent to the CISM, which adapts the infrastructure resource allocations according to the changed infrastructure requests.

Enforcing desired state can be regarded as a control loop for the MCIO, which is executed in the following three stages:

- Observe: What is the desired state of the MCIO?
- Check difference: What is the actual (current) state of the MCIO and the differences between the desired state and the actual state of the MCIO?
- Take action: Make the actual state like the desired state of the MCIO.

The CISM manages many control loops running simultaneously, each of which has a specific set of tasks to handle for achieving the desired state of the MCIO.

6.4.3 Key issue #3: Namespace quota

As specified in ETSI GS NFV-IFA 040 [i.14], namespace quota are used to track the aggregate usage of infrastructure resources in the scope of a namespace and allow operators of CIS clusters to specify resource usage limits that MCIOs created within the scope of a namespace may consume.

Namespace quota can be regarded as a resource management mechanism configured by operators of CIS clusters via the NFVO to limit (or restrict) the number of resources that can be used. This mechanism, targeting on managing infrastructure resources within CIS clusters, makes effect on corresponding container namespace and its aggregate MCIOs in the CIS cluster. By consuming namespace quota management, the NFVO can reserve an amount of infrastructure resources in the CIS cluster for a namespace, and the CISM further allocates infrastructure resources of individual MCIOs deployed in that namespace within the limits of namespace quota autonomously.

6.4.4 Key issue #4: CISM and VNFM role in autonomous management

The relationship between the CISM and VNFM role is a fundamental issue to be addressed in the scenario of autonomous container infrastructure management. Although the CISM is an NFV-MANO logical function which can monitor and scale MCIOs, repair CIS cluster nodes in an autonomous manner, it does not replace or weaken the role of the VNFM. Table 6.4.4-1 summarizes the comparison of both roles in the context of containerized VNF management.

Table 6.4.4-1: CISM and VNFM role comparison

Criteria of comparison	CISM	VNFM
Granularity of managed objects	MCIOs (visible to CISM northbound consumers) CIS instances (invisible to CISM northbound consumers)	Aggregated VNFCs and VLs constructing containerized VNF (consequently be converted into the management of MCIOs invoked by the VNFM, which are executed by the CISM).
Infrastructure resource management	Not aware of the VIM The CISM is assigned a pool of nodes hosting infrastructure resources (either VM or bare metal) belonging to a CIS cluster, which are further used by the CISM for scheduling MCIOs.	Express the infrastructure resource management requirements of the VNF in the management of MCIOs.
Scaling of managed objects	Autonomous MCIO scaling, triggered by the difference of desired state and actual state of the MCIO detected by the CISM.	VNF scaling on demand, either trigged by executing operations and maintenance plan via the NFVO, or triggered by VNF application level scaling conditions via the EM/VNF. VNF auto-scaling triggered by the VNFM based on the VNFD. VNF scaling is consequently converted to creation or deletion of MCIOs invoked by the VNFM.
Healing of managed objects	Autonomous MCIO healing, triggered by the CISM consecutive health checks on CIS cluster nodes running MCIOs.	VNF healing on demand, either trigged by NS level fault/failures detected by the NFVO, or triggered by VNF application level fault/failures detected by the EM/VNF. VNF auto-healing triggered by the VNFM based on the VNFD. VNF healing is consequently converted to creation or deletion of MCIOs invoked by the VNFM.

From the viewpoint of the CISM, MCIOs are monitored, scaled or healed autonomously with resources associated to the CIS cluster that the CISM belongs to. The CISM does not own the view of VNF internal composition or topology, and the mapping between the VNF and the MCIOs it uses is maintained by the VNFM. The VNFM is the only entry point for managing the VNF, no matter the VNF is VM based or containerized. Under the control of the VNFM, the requirements for scaling or healing VNFs inherited from the upper layer of NS management or VNF application level are handled by the VNFM, or VNF auto-scaling/auto-healing are triggered by the VNFM based on the VNFD, and converted to the management requests of MCIOs invoked by the VNFM. The CISM, on the other hand, executes autonomous MCIO management in a closed loop with the CIS clusters.

6.4.5 Summary of potential solutions

The functionality of the CISM has already been analysed in ETSI GR NFV-IFA 029 [i.35] clause 6.2 and corresponding service based interface requirements produced by the CISM are specified in ETSI GS NFV-IFA 040 [i.14]. This clause summarizes the key issues analysis in clause 6.4 from an angle of coordination between the CISM and other NFV-MANO functional entities in context of autonomous management.

The CISM has the capability to manage MCIOs (e.g. scale, heal) in an autonomous way by changing an MCIO to its desired state and allocating infrastructure resource associated to this change. This can be regarded as a CLA mechanism inside the CISM and the CIS cluster that it belongs to. The CISM can receive MCIO polices from the NFVO for being provided necessary guidance for this autonomous management process. On the other hand, the CISM does not exclude the on-demand MCIO management requests from the VNFM which are triggered by top-down operations and maintenance plans or application level conditions of the containerized VNF.

The CISM is not aware of the Intent Management in NFV-MANO, but is in a functional chain of executing NFV-MANO operations for fulfilling the intent after the intent is interpreted by Intent Management.

The MDA is one CISM northbound consumer who collects necessary input information from the CISM for ML model training or management data analytics purpose.

7 Architectural impacts

7.1 Introduction

7.1.1 Intent Management

The Intent Management functions receive requests via an intent based interface which allows for management operations of intent objects in a generic manner, as highlighted in clause 6.2.3. "Key issue #3: Management operations of intent" of the present document. In addition, typical Intent Management functions also report on fulfilment status of intents and can perform evaluations for feasibility of intents.

Intent Management functions treat intents as knowledge objects with distinct lifecycles, therefore they typically expose a generic knowledge management API. That positions the Intent Management functions in a producer role, exposing to any consumer OSS functions the Intent Management operations over an interface named herein IM-1, for an easy reference throughout the present document.

Such intent management operations of an intent management interface, are one or more of the following:

- Creation of intents
- Query intents
- Deletion of intents
- Subscription and notifications to updates on fulfilment status of intents
- Reporting on intent fulfilment

These operations are depicted under the IM-1 interface shown in Figure 7.1.1-1 below.

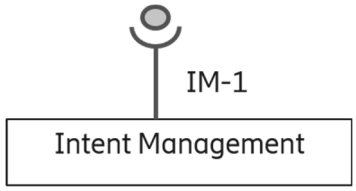

Figure 7.1.1-1: Intent Management interface, IM-1

As part of the overall processing of intents and until it deems the intent fulfilment was achieved, the Intent Management functions perform in a continuous loop, one or more of the following categories of tasks, depending on the complexity of the intent being processed:

- Interactions with a knowledge base, to extract previous data e.g. from handling of similar intents.
- Request for recommendations from machine reasoning functions, for given sets of input, state and contextual data.
- Actuation tasks, to perform the actions resulting from the decisions taken throughout the processing steps.

However, the domain-specific knowledge is carried by the various intent objects exchanged over the Intent Management interface.

In the context of NFV-MANO, the Intent Management functions receive intent-driven management requests related to NS performance and lifecycle goals. The Intent Management functions then interact with NFV-MANO to either request information, or to request certain actions to be executed by NFV-MANO. For the intents containing NS related goals, the Intent Management functions consume NS related information.

7.1.2 Management Data Analytics

The Management Data Analytics plays an essential role in the management loops (closed or open) at different stages, to diagnose ongoing issues impacting the performance of the NSs or VNF instances, to predict any potential issues (e.g. potential failure and/or performance degradation). The MDA also handles requests for ML model training from its consumers, it provides reports with identified issues and recommended actions.

An MDA Service (MDAS) framework is described in 3GPP TR 28.809 [i.3], and depicts the MDAS using input data for analysis from various sources, with the capability to assemble analytics based on information obtained from MDA Services across different domains, including virtualised resources utilization and performance for core networks and RAN. In NFV-MANO case, that translates into the ability to interact with MDA/s, irrespective whether the MDA/s are dedicated to processing NFV-MANO data only, or they are also performing analytics tasks for other management functions in OSS/BSS besides NFV-MANO (e.g. NF level, subnet slice level, etc. Such interactions include:

- the MDA/s collecting data from NFV-MANO as input for analysis; and
- the MDA/s exposing their services over MDA-1 interface, offering analytics services to NFV-MANO.

Using a common interface model for requests for Management Data Analytics services greatly simplifies the interactions with MDA. Such common MDA interface model, named MDA-1 for a simplified reference throughout the present document, is depicted in Figure 7.1.2-1 below.

The domain specific data for NFV-MANO, exchanged across the MDA-1 interface, is to be defined for interactions with the NFVO and/or the OSS/BSS. That includes the content of the NFV ML models to be trained by an MDA, content of the analytics reports, and the NFV data on which analytics service can be requested.

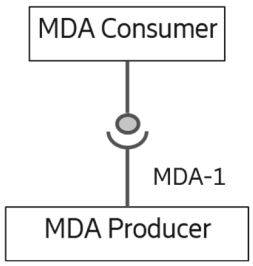

Figure 7.1.2-1: MDA-1 interface exposed by an MDA for MDA consumers

7.2 Analysis of potential solutions

7.2.1 Analysis of potential solutions related to intent based NS management

According to high-level use case description in clause 5.2 and key issue analysis in clause 6.2, the following architectural options for the Intent Management functions with NFV-MANO can be derived:

NOTE 1: For all options, the Intent Management functions expose the IM-1 interface for intent management.

NOTE 2: Whether the software components of multiple functional blocks are co-located, merged or separated is an implementation decision outside the scope of the present document.

Option #1: Intent Management functions reside in the NFVO

With this architectural option, the Intent Management functions of NFV-MANO reside within the NFVO. The Intent Management interface IM-1 can be seen as an addition to the Os-Ma-nfvo set of interfaces since the overall producer exposing IM-1 functionality is the NFVO, exposing an enhanced Os-Ma-nfvo reference point to other OSS/BSS functions. The NFVO (as the producer of the Intent Management interface IM-1) receives the intent from the OSS/BSS (as the consumer of the Intent Management) via Os-Ma-nfvo reference point. The Intent Management functions of the NFVO interpret the intent and derives the corresponding NS lifecycle management operations to be further executed by NS LCM function of the NFVO as shown in Figure 7.2.1-1.

In this case, Os-Ma-nfvo reference point is enhanced with a new interface IM-1 for intent management. There are no impacts on other reference points of NFV-MANO and the functionality offered by the NFVO to the OSS/BSS.

NOTE 3: Within the NFVO the Intent Management functions can be implemented inside other functions or intertwined with them, or can be self-contained independent functions.

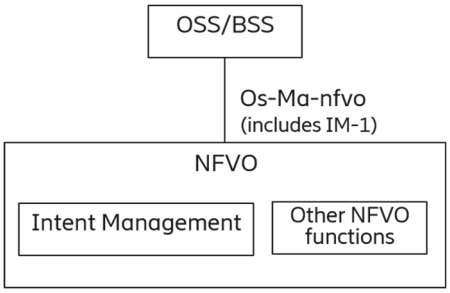

Figure 7.2.1-1: Intent Management resides in the NFVO

Option #2: Intent Management functions provided and represented via a new Intent Management functional block in NFV-MANO.

In this architectural option, the Intent Management (IM) functions used by NFV-MANO are represented by a new dedicated NFV-MANO functional block, named Intent management which exposes its functionality via the interface IM-1. The Intent Management functions can be either dedicated to handling intent-driven management requests for NFV-MANO domain, or they can leverage generic functionality for handling intents used also for other management domains within OSS.

The Intent Management functions interpret the intent, derive any corresponding NS lifecycle management operations required and then transfer them to the NFVO for execution. The Intent Management functional block communicates with the NFVO using Im-Or consisting of the applicable interfaces of the Os-Ma-nfvo reference point (e.g. NS LCM, NSD management, VNF Package Management, NS FM, NS PM, etc. After the NFVO completes the execution of NS lifecycle management operations, the NFVO returns the operation results to the Intent Management functional block. The Intent Management functions continuously verify that the intent is fulfilled and inform the OSS/BSS consumer about the status of the intent fulfilment. The new interface for intent management IM-1 is exposed to the OSS/BSS consumer as shown in Figure 7.2.1-2 below.

In this option, the NFVO continues offering all existing functionality (i.e. not Intent Management related) towards the OSS/BSS without any impact over the Os-Ma-nfvo reference point.

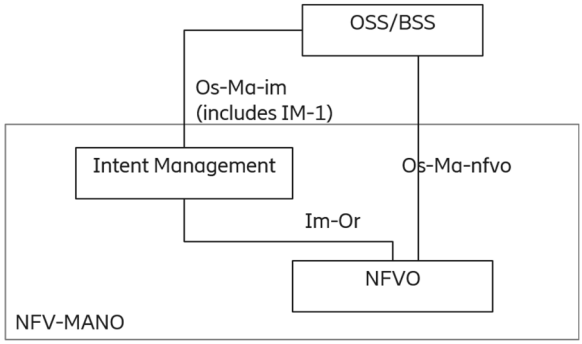

Figure 7.2.1-2: Intent Management provided and represented by a new functional block in NFV-MANO

Option #3: Intent Management functions provided reside in the OSS/BSS functional block.

The IM functions and IM-1 exposure are similar to Option#2, the main difference is that the Intent Management (IM) functions are shared within the OSS/BSS functional block, between multiple OSS management functions including NFV-MANO.

In this option, the NFVO continues offering all existing functionality (i.e. not Intent Management related) towards the OSS/BSS without any impact over the Os-Ma-nfvo reference point.

This option is represented in Figure 7.2.1-3 below.

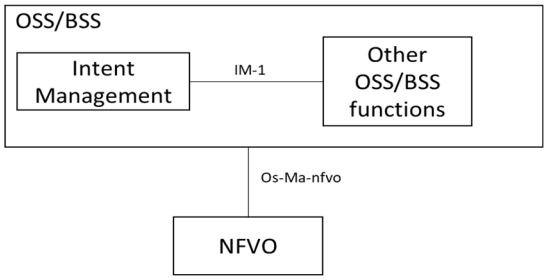

Figure 7.2.1-3: Intent Management resides in the OSS/BSS functional block

7.2.2 Analysis of potential solutions related to MDA assisted management

According to high-level use case description in clause 5.3 and key issue analysis in clause 6.3, there are several aspects analysed which influence the possible options for integrating MDA functions with NFV-MANO. These are:

a) How the MDA exposes its functionality.

b) How NFV-MANO consumes the MDA functionality.

c) How the MDA consumes NFV-MANO data.

The following options are analysed and described for the MDA:

1) The MDA resides in the NFVO.

2) The MDA as a separate set of functions, is represented by its own NFV-MANO functional block. MDA functionality can be generic, and the MDA can be dedicated to NFV-MANO or be shared with other OSS/BSS functions (e.g. knowledge base, machine reasoning, actuation agents).

3) The MDA resides in the OSS/BSS functional block. MDA functionality can be generic, and the MDA can be dedicated to NFV-MANO or be shared with other OSS/BSS functions (e.g. knowledge base, machine reasoning, actuation agents).

NOTE 1: For all options, the MDA functions expose the MDA-1 interface.

NOTE 2: Whether the software components of multiple functional blocks are co-located, merged or separated is an implementation decision outside the scope of the present document.

Irrespective of the internal MDA architecture, the MDA is expected to provide the same analytics functionality for NFV-MANO data over MDA-1 interface. The different MDA data collection options are:

a) the MDA collecting NFV-MANO data via the NFVO; or

b) the MDA collecting NFV-MANO data from all NFV-MANO FBs.

Option #1: MDA functions reside in the NFVO

With this architectural option, the MDA functions used by NFV-MANO reside within the NFVO and the NFVO consumes the MDA services.

Since the overall producer exposing MDA-1 functionality is the NFVO, the functionality exposed by MDA via interface MDA-1 can be seen as an addition to the Os-Ma-nfvo set of interfaces, leading to an enriched Os-Ma-nfvo reference point between NFVO and the other OSS/BSS functions. There are no impacts on how NFVO offers previous functionality (i.e. not MDA related) to the OSS/BSS or to other NFV-MANO functional blocks.

This is shown in Figure 7.2.2-1 below.

NOTE 3: Within the NFVO the MDA functions can be implemented inside other functions or intertwined with them, or can be self-contained independent functions.

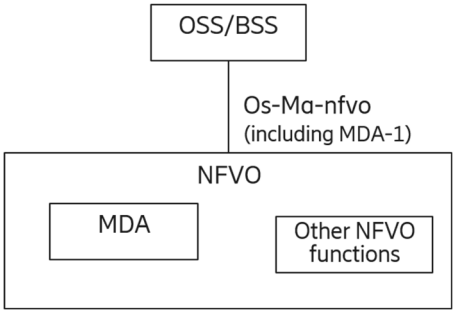

Figure 7.2.2-1: The MDA resides in the NFVO functional block

Option #2: MDA functions provided and represented by a new MDA functional block.

With this architectural option, the MDA functions used by NFV-MANO are a set of logical functions represented by a new NFV-MANO functional block named MDA, which exposes its functionality via the interface MDA-1. The MDA-1 interface is consumed by the NFVO, as well as other OSS/BSS functions that request NFV-MANO data analytics to use them as input into a wider context, e.g. at NF level, or at subnet slice level or at slice level.

The MDA functions can be:

- dedicated to NFV-MANO data analytics; or
- can be shared with other OSS management functions, where the knowledge and analysis of the different domain specific data objects is handled.

In this option, the NFVO continues offering all existing functionality (i.e. not MDA related) towards the OSS/BSS without any impact over the Os-Ma-nfvo reference point.

The MDA functions are aware of the NFV-MANO specific data and collect it from NFV-MANO. There are 2 alternatives for the MDA data collection from NFV-MANO:

NOTE 4: The figures of the two alternatives below do not preclude that the MDA collects MDA data from other NFV-MANO functional entities (e.g. the CISM, the WIM) using their existing interfaces.

a) **Option#2.a:** The MDA collects the NFV-MANO data via the NFVO, as shown in Figure 7.2.2-2 below.

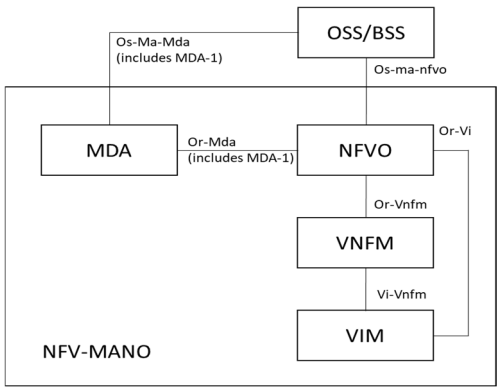

Figure 7.2.2-2: Option #2.a: The MDA as new NFV-MANO functional block shared within NFV-MANO and with data collection via the NFVO

b) **Option#2.b:** The MDA collects NFV-MANO data from all NFV-MANO FBs, as shown in Figure 7.2.2-3 below.

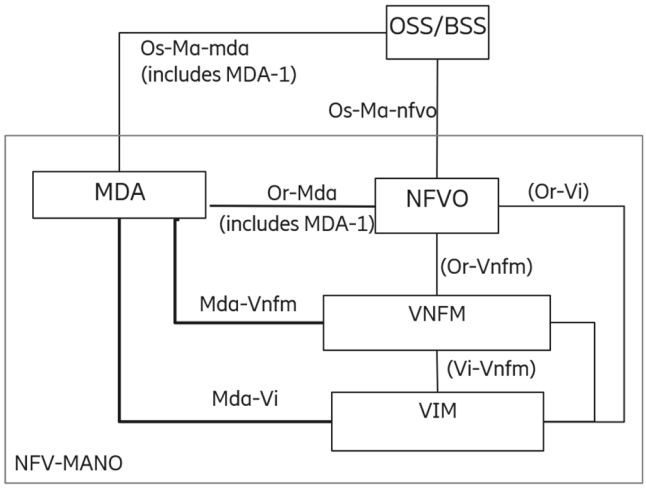

Figure 7.2.2-3: Option #2.b: The MDA represented as new functional block with data collection from all NFV-MANO FBs

Option #3: MDA functions reside in the OSS/BSS functional block.

With this architectural option, the MDA functions used by NFV-MANO reside in the OSS/BSS functional block. The MDA-1 interface is consumed by the NFVO, as well as other OSS/BSS functions that request NFV-MANO data analytics to use them as input into a wider context, e.g. at NF level, or at subnet slice level or at slice level.

The MDA functions can be:

- dedicated to NFV-MANO data analysis; or
- can be shared with other OSS management functions, where the knowledge and analysis of the different domain specific data objects is handled.

In this option, the NFVO continues offering all existing functionality (i.e. not MDA related) towards the OSS/BSS without any impact over the Os-Ma-nfvo reference point.

The MDA functions in the OSS/BSS are aware of the NFV-MANO specific data and collect it from the NFVO, as shown in Figure 7.2.2-4 below.

NOTE 5: Figure 7.2.2-4 does not preclude that the MDA in the OSS/BSS collects MDA data from NFV-MANO functional entities (e.g. the CISM, the WIM) using their existing interfaces.

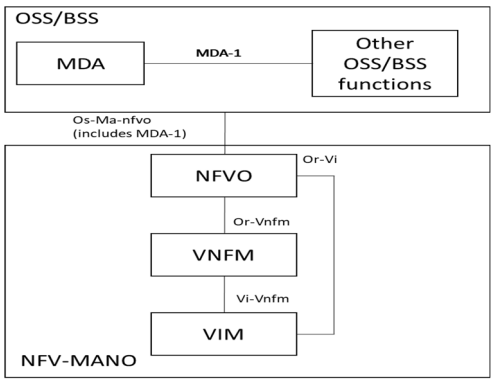

Figure 7.2.2-4: Option #3: The MDA residing in the OSS/BSS functional block with data collection via the NFVO

7.2.3 Analysis of potential solutions related to autonomous container infrastructure management

Architectural impact analysis on autonomous container infrastructure management overlaps with the analysis in clause 7.2 of ETSI GR NFV-IFA 029 [i.35] and is out of the scope of the present document.

According to the outcome of ETSI GR NFV-IFA 029 [i.35], the CISM is a logical function in NFV-MANO architectural framework and produces service based interfaces specified in ETSI GS NFV-IFA 040 [i.14] to its northbound NFV-MANO consumers (e.g. the NFVO or VNFM).

7.3 Evaluation

The comparison of different architectural options in clause 7.2 is provided in Table 7.3-1, with respect to logical architecture aspects of each option.

Table 7.3-1: Logical architecture comparison for different architectural options

Evaluation Criteria	Option#1-IM: The Intent Management resides in the NFVO	Option#2-IM: The Intent Management as a functional block in NFV-MANO	Option#3-IM: The Intent Management resides in the OSS/BSS	Option#1-MDA: The MDA resides in the NFVO	Option#2-MDA: The MDA as a functional block in NFV-MANO	Option#3-MDA: The MDA resides in the OSS/BSS
Provides a clear separation of concerns for the management of automation aspects (see note 1)	Yes	Yes	Yes	Yes	Yes	Yes
Assigns the new functional roles to one and only one functional block (see note 2)	Yes	Yes	Yes	Yes	Yes	Yes
New functional roles become part of NFV-MANO	Yes	Yes	No	Yes	Yes	No
Exposure of collection and reporting of NFV-MANO information to more than one functional block (other than the current NFV-MANO) (see note 3)	Not applicable	Not applicable	Not applicable	No	Yes	No
Consolidates management of automation aspects of NS level management into a single NFV-MANO functional block (see note 4)	Yes	No	No	Not applicable	Not applicable	Not applicable

Evaluation Criteria	Option#1-IM: The Intent Management resides in the NFVO	Option#2-IM: The Intent Management as a functional block in NFV-MANO	Option#3-IM: The Intent Management resides in the OSS/BSS	Option#1-MDA: The MDA resides in the NFVO	Option#2-MDA: The MDA as a functional block in NFV-MANO	Option#3-MDA: The MDA resides in the OSS/BSS
NOTE 1: This criterion indicates whether the automation aspects of NFV-MANO are spread among different functional blocks or functions. In the context of the present document, management of automation aspects includes the Intent Management and MDA.						
NOTE 2: This criterion indicates that for either option among the three, whether the new functional role (either the IM or MDA) belongs to only one functional block (the NFVO, a new FB or the OSS/BSS).						
NOTE 3: This criterion indicates whether new information flows or path for NFV-MANO information collection and reporting are introduced by this option.						
NOTE 4: This criterion indicates whether automation aspects of the NS level management are logically consolidated in one single NFV-MANO functional block at that level.						

For architectural options described in clause 7.2, their functional impacts on the NFV-MANO architectural framework are depicted in Table 7.3-2.

Table 7.3-2: Architectural option impacts on NFV-MANO architectural framework

New functionality	Option	Impacts on NFV-MANO architectural framework (see notes 3, 4 and 5)
Intent Management (see note 6)	**Option #1:** IM functions reside in the NFVO.	No new FBs or reference points to be documented, but only additional interface IM-1 to be specified.
	Option #2: Separate IM FB, exposing a standard interface (IM-1) and consuming NFVO functions via NFV-MANO standard interfaces exposed by the NFVO.	• New Intent Management (IM) functions or FB (see note 1) to be added, and the exposed interface IM-1 to be specified. • Specify which interfaces exposed by NFVO are consumed by the IM (see note 1).
	Option #3: IM represented by IM functions shared within the OSS.	• Specify which interfaces exposed by NFVO are consumed by the IM (see note 1).
MDA (see note 7)	**Option #1:** MDA functions reside in the NFVO.	No new FBs or reference points to be documented, but only additional interface MDA-1 to be specified. If MDA does not participate in closed loops for cross-management domain scenarios, the MDA-1 does not need to be exposed to OSS/BSS.
	Option #2a: Separate MDA FB, exposing a standard interface (MDA-1), consuming NFV-MANO data via NFV-MANO standard interfaces exposed by the NFVO.	• New MDA functions or FB (see note 1) to be added and the exposed MDA-1 interface to be specified (see note 1). MDA-1 interface is consumed by NFVO and OSS/BSS. • Specify which interfaces exposed by NFVO are consumed by the MDA (see note 1).
	Option #2b: Separate MDA FB, exposing a standard interface (MDA-1), consuming NFV-MANO data via NFV-MANO standard interfaces exposed by the NFVO, VNFM, VIM.	• New MDA functions or FB to be added and the exposed MDA-1 interface to be specified (see note 1). MDA-1 interface is consumed by the NFVO and the OSS/BSS. • Specify which interfaces exposed by the NFVO, VNFM, VIM and CISM are consumed by the MDA (see note 1). • Detailed information and correlation of data from the different NFV-MANO FBs is needed (see note 2).
	Option #3: MDA functions reside in the OSS/BSS.	• MDA-1 interface is consumed by the NFVO and the OSS/BSS. • Specify which interfaces exposed by the NFVO, VNFM, VIM and CISM are consumed by the MDA (see note 1).

New functionality	Option	Impacts on NFV-MANO architectural framework (see notes 3, 4 and 5)
NOTE 1: The specification of the new interfaces IM-1 and MDA-1 can be done as individual specifications or wrapped into reference points to bind exchanges between producer and each of its consumers. The specification of the new functionality can be done as definition of new functions or as new FBs.		
NOTE 2: In certain cases, detailed information that is not available in the NFVO (e.g. VNFC instance ids) can be necessary for the data analysis, and to allow the MDA to determine the recommended actions.		
NOTE 3: All options described in clause 7.2 are backward compatible with the existing NFV-MANO framework, the IM and the MDA reuse the existing NFV-MANO information and data models to communicate with NFV-MANO. No impact to the existing NFV-MANO interfaces, data models, and their current exposure to the existing consumers (e.g. the OSS/BSS).		
NOTE 4: All options described in clause 7.2 consider future compatibility and standards development.		
NOTE 5: All options described in clause 7.2 have no impacts on NFV template models (e.g. the NSD, the VNFD).		
NOTE 6: The model of the NFV-MANO intents is expected to be specified in all options.		
NOTE 7: The model of the NFV-MANO analytics reports is expected to be specified in all options.		

Different architectural options for the Intent Management and MDA have their own implementation scenarios and each addresses different needs of the service providers. Various technical constraints and requirements on the management services of the NFV-MANO are considered for an optimal integration of either the Intent Management functions, or the MDA functions, or both, into the NFV-MANO architecture.

The implementation implications of such requirements of the NFV-MANO services on the architectural options are listed in Table 7.3-3 below.

Table 7.3-3: Evaluation on architectural options with NFV-MANO service requirements on various implementation scenarios

NFV-MANO service comparison criteria	Recommended Intent Management option	Recommended MDA option	Comments
Time sensitive management services (e.g. for uRLLC VNFs) when low latency is an essential factor (reference ETSI GR NFV-EVE 017 [i.37])	**Option #1:** The IM resides in the NFVO, when the implementation of the IM functions are collocated or merged with the implementation of other NFVO functions communicating with them **Option #2:** Separate IM functional block, exposing a standard interface (IM-1) and consuming NFVO functions via NFV-MANO standard interfaces, when the IM FB implementations are collocated or merged with the NFVO implementation	**Option #1:** The MDA resides in the NFVO, when the implementation of the MDA functions are collocated or merged with the implementation of other NFVO functions communicating with them **Option #2:** Separate MDA functional block, exposing a standard interface (MDA-1), consuming NFV-MANO data via NFV-MANO standard interfaces, when the MDA FB implementations are collocated or merged with the NFVO implementation	Shortens and optimizes the interaction time for the interfacing between the NFVO and the new functions (the Intent Management and MDA). For Intent Management, it also shortens the interactions between the IM and other NFVO functions (e.g. NS LCM), when the IM holistically uses other policies within the NFVO.

NFV-MANO service comparison criteria	Recommended Intent Management option	Recommended MDA option	Comments
Support for NFV-MANO extensions for management of automation aspects, i.e. intents and data analytics	**Option #1:** The IM resides in the NFVO **Option #2:** Separate IM functional block, exposing a standard interface (IM-1) and consuming NFVO functions via NFV-MANO standard interfaces **Option#3:** The IM resides in the OSS/BSS	**Option #1:** The MDA resides in the NFVO **Option #2:** Separate MDA functional block, exposing a standard interface (MDA-1), consuming NFV-MANO data via NFV-MANO standard interfaces **Option#3:** The MDA resides in the OSS/BSS	It is assumed that both the Intent Management and the MDA provide data extensibility mechanisms for the NFV-MANO intents and analytics data, regardless of the option.
Reuse intelligent functions, or cognitive framework architecture across several OSS management functions (see note)	**Option#2:** Separate IM functional block, exposing a standard interface (IM-1) and consuming NFVO functions via NFV-MANO standard interfaces. **Option#3:** The IM resides in the OSS/BSS	**Option#2 (a or b):** Separate MDA functional block, exposing a standard interface (MDA-1), consuming NFV-MANO data via NFV-MANO standard interfaces (either via NFVO, or with each NFV-MANO FB) **Option #3:** The MDA resides in the OSS/BSS	Common and generic functions are reused for Intent Management functions in OSS. These can include, but are not limited to, an OSS knowledge base, machine reasoning functions, actuation agents which trigger the actions following a decision. Similar, common and generic functions are used for all OSS MDA functions, where extensions for each OSS management functions is added. The knowledge on handling NFV-MANO specific data and analytics is added into the generic OSS management functions (similar to other OSS management domains-specific data).
NOTE: Option#1 is excluded from this NFV-MANO service comparison criterion since the IM or the MDA functions are implemented inside the NFVO and will not be reused across OSS management functions.			

There can be also mixed cases, where for some features the MDA functions are expected to handle low latency requirements while some other features are already available in an existing, or external MDA functions. In such cases, an NFV-MANO system can use both options (Option #1 and Option #2) for MDA services at the same time, i.e. from the MDA inside the NFVO and/or from separate MDA functional block (e.g. for different consumers, or for different NSs).

7.4 Potential NFV architecture

Based on the outcome of clause 7.3 evaluation, the recommended NFV architecture for fulfilling use case of intent based NS management and MDA assisted management is NFV-MANO service or scenario specific:

- **Option #1** The Intent Management functions and MDA functions reside in the NFVO, is applicable for:
  - NFV-MANO scenario of time sensitive management services when low latency is an essential factor, providing that the implementations of the IM or MDA functions are collocated or merged with the implementation of other NFVO functions communicating with them.
  - Support for NFV-MANO extensions for management of automation aspects, i.e. intents and data analytics.
- **Option #2** Defining one new functional block for each of the Intent Management and respectively for the MDA in NFV-MANO, is applicable for:
  - NFV-MANO scenario of time sensitive management services when low latency is an essential factor, in case that the IM or MDA FB implementations are collocated or merged with the NFVO implementation.

  - Support for NFV-MANO extensions for management of automation aspects, i.e. intents and data analytics.
  - Reuse intelligent functions, or cognitive framework architecture across several OSS management functions.

- **Option #3** The Intent Management functions and MDA functions reside in the OSS/BSS, is applicable for:
  - Support for NFV-MANO extensions for management of automation aspects, i.e. intents and data analytics.
  - Reuse intelligent functions, or cognitive framework architecture across several OSS management functions.

Either the Intent Management or the MDA can be a common functional block that can be reused by NFV-MANO and other OSS/BSS functions. When deployed within NFV-MANO, in case of Intent Management functional block, it has a new reference point Im-Or with the NFVO. The Intent Management exposes a standard interface (IM-1) to the OSS/BSS and consumes NFVO functions via NFV-MANO standard interfaces exposed by the NFVO. In case of MDA functional block, new reference points between the MDA and the NFVO, VNFM and VIM (named Or-Mda, Mda-Vnfm, Mda-Vi respectively) are specified for the MDA to consume functions via NFV-MANO standard interfaces exposed by respective NFV-MANO functional block for collecting information as input for analytics. The MDA also consumes interfaces produced by the WIM and CISM for the same purpose of information collection in MDA processes. The NFVO or the OSS/BSS consumes interfaces (MDA-1) produced by the MDA for ML model training or data analytics over respective Or-Mda or Os-Ma-mda reference point.

8 Recommendations for future work

8.1 Summary of the study

The present document studies three areas of autonomous networks based on use cases on intent based NS management, MDA assisted management and autonomous container infrastructure management, which can be regarded as closed-loop automation mechanisms enabling autonomous management in NFV-MANO. Key issue analysis and architectural impact analysis are made for each category of use cases. Based on that, recommendations on the next step normative work are concluded in clause 8, mainly on:

- architecture and framework aspects (refer to clause 8.2);
- functional aspects (refer to clause 8.3).

8.2 Recommendations for architectural aspects in general

8.2.1 Intent-based NS Management

One advantage of using intents in the exchange between two functions is the simplification of the interaction and the separation of concerns between functions. While this is suitable for some interactions such as indicating NS management goals and expectations, the intents are not well suited for some of the lower level interactions where precise indications on how a request is expected to be executed are provided in the request.

The study in the present document focuses on the intents being used for NS management scope, for which some example use cases analysed are described in clause 5.2.

Hence the Intent Management interface IM-1, offered by the Intent Management functions to the OSS/BSS should offer the management of NS related intents.

As intents are knowledge objects, which have to capture knowledge graphs, the intent object definition and their management interfaces are new, to be defined. As the present document is followed up in the normative specifications, careful consideration is recommended for the reuse and alignment with other industry work done on the intents modelling and the interfaces for intent management, such as the work in the TM Forum Autonomous Networks project and 3GPP SA5.

It is recommended that ETSI ISG NFV will define the domain specific content of the NS related intents objects.

The Intent Management consumes the interfaces offered by the NFVO, such as NSD management, NS LCM, NS PM, NS FM, VNF Package management.

8.2.2 MDA

The MDA can be used to diagnose ongoing issues impacting the performance, the health or the behaviour of an NS instance, or even in a bigger context in the OSS/BSS, as stated in ETSI TS 128 550 [i.13], impacts to the service assurance, or the performance of the mobile network. The NFV-MANO analytics can be used as well as to predict any upcoming potential issues (e.g. potential failure and/or performance degradation).

From the architecture perspective, a new interface MDA-1 is expected to be specified, to expose the following MDA capabilities:

- Support for requests on producing NFV-MANO analytics, scoped at this stage for NS-level data only.
- Providing asynchronous analytics reports.

The MDA consumes the existing NFV-MANO interfaces, exposed by the NFVO, VNFM and VIM, to query and retrieve PM, FM, descriptors and runtime data of the NFV-MANO instances. The MDA can also consume data related to the WIM, CISM, CIR and CCM via interfaces exposed by them.

It is recommended that the functional architectural requirements on the NFVO are updated to reflect how the NFVO makes use of the functionality over MDA-1.

MDA aspects that are out of scope of the present document and of the architecture analysis include:

- LCM of NFV-MANO ML models and their modelling aspects.
- ML models sharing between NFVOs and federated learning.

NOTE: The specification of the new interface MDA-1 can be done as an individual specification or wrapped into reference points to bind exchanges between the producer and each of its consumers. The specification of the new functionality can be done as definition of new functions or as new FBs.

8.2.3 Autonomous container infrastructure management

The NFV-MANO can leverage automation features offered by the CISM. There is no impact for this on the NFV-MANO architecture framework.

8.3 Recommendations for functionality enhancement

8.3.1 Intent based NS management

The present clause provides recommendations on functional aspects related to the Intent Management. These are listed in Table 8.3.1-1, and provide the recommendations related to functional aspects of the Intent Management.

Table 8.3.1-1: Recommendations on functional aspects of the Intent Management for NFV-MANO

Identifier	Recommendation description	Comment/Traceability
It is recommended that a requirement set be specified for the Intent Management to support:		
Intent.Mgmt.001	Intent-based management requests initiated by a consumer of Intent Management, containing NFV-MANO specific intents.	The consumer is the OSS/BSS. Refer to clauses 6.2.1 and 6.2.3. This includes specification of the interface used for the management of intents.
Intent.Mgmt.002	Fulfilment of the intent-based requests.	The Intent Management processes the intent and performs the necessary actions for intent fulfilment. These actions can include (e.g. NS LCM, NS PM, etc.), leveraging use of policies for the IM decision-making process, in conjunction with potential support from intelligent functions to complement the analysis and decision making process. Refer to clauses 6.2.1, 6.2.2 and 6.2.3.
Intent.Mgmt.003	Intent fulfilment reporting provided to the consumer.	The Intent Management provides fulfilment reports as requested by consumers in the intent requests. Refer to clause 6.2.3. This includes specification of the interface used to provide the intent fulfilment reporting and the models of the analytics reports provided by NFV-MANO. The fulfilment reports can use a common meta-model within OSS/BSS, but the NFV-MANO domain-specific data is expected to be specified further in ETSI NFV.
Intent.Mgmt.004	Standard NFV-MANO domain specific intent objects and their models.	This includes the specification of the content of the intent objects that is NFV-MANO domain-specific (to be defined in ETSI NFV), possibly reusing common intents meta-model across the OSS/BSS. This enables the requests that are supported by the Intent Management for NS related intents. Refer to clauses 6.2.4 and 7.1.1.

8.3.2 MDA assisted management

The present clause provides recommendations on functional aspects related to the MDA assisted management:

Table 8.3.2-1 provides the recommendations related to functional aspects of MDA.

Table 8.3.2-1: Recommendations related to functional aspects of the MDA for NFV-MANO

Identifier	Recommendation description	Comment/Traceability
It is recommended that a requirement set be specified for the MDA to support:		
Mda.Mgmt.001	Data analytics requests initiated by a consumer of MDA services.	The consumer can be either the NFVO or the OSS/BSS. Refer to clauses 6.3.1 and 6.3.5. This includes specification of the interface used for the data analytics.
Mda.Mgmt.002	ML model training requests initiated by a consumer of MDA services.	The consumer can be the NFVO. Refer to clause 6.3.6. However as more study is expected on ML modelling and their specific training actions required, the ML training functionality is left for a later stage.
Mda.Mgmt.003	Data analytics reports provided by MDA to consumers.	The MDA provides analytics reports as requested by consumers in the data analytics requests. Refer to clause 6.3.3.
Mda.Mgmt.004	Standard NFV-MANO domain specific MDA analytics objects and their models.	The includes the specification of the content of MDA analytics objects that is NFV-MANO domain specific, which are applied in processes of data analytics in NFV-MANO. Refer to clauses 6.3.4 and 6.3.5.

Annex A:
Change History

Date	Version	Information about changes
<Month year>	<#>	<Changes made are listed in this cell>
October 2019	0.0.1	First draft, introducing the skeleton and the scope of the GR NFVIFA(19)000859r2, NFVIFA(19)000860r1
December 2019	0.1.0	Early draft including the following contributions approved in IFA#177 F2F meeting: NFVIFA(19)000959, NFVIFA(19)000960r1, NFVIFA(19)000961r2, NFVIFA(19)000962r2
February 2020	0.2.0	Early draft including the following contributions approved in IFA#179 and IFA#181 meeting: NFVIFA(19)000963r2, NFVIFA(20)000017r1, NFVIFA(20)000021
April 2020	0.3.0	Early draft including the following contributions approved until IFA#186 meeting: NFVIFA(20)000051r2, NFVIFA(20)000134r1
May 2020	0.4.0	Early draft including the following contributions approved until IFA#195 meeting: NFVIFA(20)000230r1, NFVIFA(20)000245r1, NFVIFA(20)000246r1, NFVIFA(20)000247r2, NFVIFA(20)000248r1, NFVIFA(20)000279r1, NFVIFA(20)000280r1, NFVIFA(20)000319
July 2020	0.5.0	Early draft including the following contributions approved until IFA#203 meeting: NFVIFA(20)000281r3, NFVIFA(20)000353r1, NFVIFA(20)000354r2, NFVIFA(20)000355r1, NFVIFA(20)000416r2, NFVIFA(20)000418r2, NFVIFA(20)000445r1, NFVIFA(20)000446r1, NFVIFA(20)000447r1, NFVIFA(20)000472r2
October 2020	0.6.0	Early draft including the following contributions approved until IFA#212 meeting: NFVIFA(20)000557, NFVIFA(20)000566r3, NFVIFA(20)000591, NFVIFA(20)000592, NFVIFA(20)000593, NFVIFA(20)000594r3, NFVIFA(20)000623r4, NFVIFA(20)000624r1, NFVIFA(20)000651r1, NFVIFA(20)000652r3
November 2020	0.7.0	Early draft including the following contributions approved until IFA#218 meeting: NFVIFA(20)000622r1, NFVIFA(20)000713r1, NFVIFA(20)000720r3, NFVIFA(20)000726r1, NFVIFA(20)000729r3, NFVIFA(20)000732r3, NFVIFA(20)000761r1, NFVIFA(20)000764r1, NFVIFA(20)000782r1
December 2020	0.8.0	Early draft including the following contributions approved until IFA#220 meeting: NFVIFA(20)000781r1, NFVIFA(20)000793r1, NFVIFA(20)000794r1, NFVIFA(20)000797r3, NFVIFA(20)000821, NFVIFA(20)000878r1, NFVIFA(20)000879r1
February 2021	0.9.0	Early draft including the following contributions approved until IFA#226 meeting: NFVIFA(21)000013, NFVIFA(21)000014r2, NFVIFA(21)000022r1, NFVIFA(21)000058r1, NFVIFA(21)000060, NFVIFA(21)000067, NFVIFA(21)000068r4, NFVIFA(21)000069r1, NFVIFA(21)000070r1 and NFVIFA(21)000073
May 2021	0.10.0	Early draft including the following contributions approved until IFA#235 meeting: NFVIFA(21)000131r2, NFVIFA(21)000133r2, NFVIFA(21)000134r5, NFVIFA(21)000135r2, NFVIFA(21)000148r3, NFVIFA(21)000149r7, NFVIFA(21)000159r1, NFVIFA(21)000268, NFVIFA(21)000276, NFVIFA(21)000277r3, NFVIFA(21)000278, NFVIFA(21)000279r1, NFVIFA(21)000280r1, NFVIFA(21)000281r3, NFVIFA(21)000282r4, NFVIFA(21)000284r2, NFVIFA(21)000285r2, NFVIFA(21)000302, NFVIFA(21)000303, NFVIFA(21)000321r3 and NFVIFA(21)000322r1
May 2021	0.11.0	Stable draft including the following contributions approved until IFA#237 meeting: NFVIFA(21)000062r7, NFVIFA(21)000348, NFVIFA(21)000351, NFVIFA(21)000362r1, NFVIFA(21)000388r2
June 2021	0.12.0	Stable draft including the following contributions approved until IFA#242 meeting: NFVIFA(21)000413, NFVIFA(21)000431r1, NFVIFA(21)000432, NFVIFA(21)000433, NFVIFA(21)000434r1, NFVIFA(21)000435r1, NFVIFA(21)000436r2, NFVIFA(21)000452, NFVIFA(21)000453, NFVIFA(21)000455r1, NFVIFA(21)000429r4, NFVIFA(21)000430r2, NFVIFA(21)000497r1, NFVIFA(21)000547r1
July 2021	0.13.0	Final draft including the following contributions approved until IFA#244 meeting: NFVIFA(21)000584r1, NFVIFA(21)000585r2, NFVIFA(21)000586

History

Document history		
V4.1.1	August 2021	Publication