ETSI GS ZSM 001 V1.1.1 (2019-10)

Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios

Disclaimer

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

Reference
DGS/ZSM-001ed111_UCs

Keywords
management, network, requirements, service, use case

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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 defines requirements on the zero-touch E2E (End-to-End) network and service management. Scenarios will be documented and used to derive the requirements.

The requirements will also be considered for the work on the topics Zero-touch network and Service Management (ZSM) reference architecture [1], ZSM End to end management and orchestration of network slicing [i.7], and ZSM Inter management domain lifecycle management [i.8].

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

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

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

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 ZSM 005: "Zero-touch network and Service Management (ZSM); Means of Automation".

[i.2] ETSI GR NFV-IFA 023: "Network Functions Virtualisation (NFV); Management and Orchestration; Report on Policy Management in MANO; Release 3".

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

[i.4] NGMN Alliance: "Architecture Proposal for the Handling of Network Operations Data with Specific Focus on Virtualized Networks", version 1.0, 2017-12-22.

[i.5] ETSI TS 138 300 (V15.6.0): "5G; NR; Overall description; Stage-2 (3GPP TS 38.300 version 15.6.0)".

[i.6] ETSI TS 123 501 (V15.5.0): "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 15.5.0)".

[i.7] ETSI GS ZSM 003: "Zero-touch network and Service Management (ZSM); End to end management and orchestration of network slicing".

[i.8] ETSI GS ZSM 008: "Zero-touch network and Service Management (ZSM); Inter management domain lifecycle management".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS ZSM 007 [2] and the following apply:

NOTE: If the same term is defined in both ETSI GS ZSM 007 [2] and in the present document, the definition in the present document takes precedence.

data governance: processes to define and enforce access restrictions to data, and to attach related metadata to the data

federated orchestration: orchestration performed by multiple autonomous management domains

NOTE: Autonomous domains in this context is related to independent (or self-regulating), not to be confused with the degree of automation.

hierarchical orchestration: orchestration decomposed into one or more hierarchical interactions where parts of the service are delegated to a sub-ordinate orchestrator

key performance indicator: measurement of a specific aspect of the performance of a service that can be used in a service level objective

service level agreement: part of a business agreement between a service provider and a customer, specifying the committed service quality and quantity in terms of service level specifications, and the associated consequences in case the service level objectives are not met

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ZSM 007 [2] and the following apply:

NOTE: If the same abbreviation is defined in both ETSI GS ZSM 007 [2] and in the present document, the definition in the present document takes precedence.

3GPP	3rd Generation Partnership Project
5GC	5G Core
AI	Artificial Intelligence
AMF	Access and Mobility management Function
AR	Augmented Reality
BBU	BaseBand Unit
BSS	Business Support System
CD	Continuous Delivery
CEM	Customer Experience Management
CFS	Customer Facing Service
CI	Continuous Integration
CPU	Central Processing Unit
CSC	Customer Service Consumer
CSP	Communication Service Provider
DCN	Data Centre Network
DN	Data Network

DNS	Domain Name System
E2E	End-to-End
EMS	Element Management System
ETSI	European Telecommunications Standards Institute
FCAPS	Fault-, Configuration-, Accounting-, Performance-, Security-management
FM	Fault Management
gNB	next generation NodeB
GR	Group Report
GS	Group Specification
GUI	Graphical User Interface
HW	HardWare
IFA	InterFaces and Architecture
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPR	Intellectual Property Rights
IPsec	Internet Protocol Security
ISG	Industry Specification Group
IT	Information Technology
KPI	Key Performance Indicator
LCM	Life Cycle Management
LTE	Long Term Evolution
M2M	Machine-to-Machine
MANO	Management And Network Orchestration
MEF	Metro Ethernet Forum
mIoT	massive Internet of Things
ML	Machine Learning
MLaaS	ML as a Service
MnS	Management Service
MR	Mixed Reality
NaaS	Network-as-a-Service
NF	Network Function
NFMF	Network Function Management Function
NFV	Network Functions Virtualisation
NFVI	NFV Infrastructure
NFVIaaS	NFV Infrastructure as a Service
NFVO	Network Functions Virtualisation Orchestrator
NG	Next Generation
NG-RAN	Next Generation-RAN
NOC	Network Operators Council
NOP	Network Operator
NS	Network Slice
NSaaS	Network Slice-as-a-Service
NSI	Network Slice Instance
NSSI	Network Slice Subnet Instance
NW	NetWork
OLA	Operational Level Agreement
ONAP	Open Network Automation Platform
OPEX	Operational Expenditures
OS	Operations System
OSS	Operations Support System
PAP	Policy Administration Point
PF	Policy Function
PM	Performance Management
PNF	Physical Network Function
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
REST	REpresential State Transfer
RL	Reinforcement Learning
SaaS	Software as a Service
SBMA	Service Based Management Architecture
SDN	Software-Defined Network

SDO	Standardization Organization
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SW	SoftWare
TCO	Total Cost of Ownership
TMF	TeleManagement Forum
TTM	Time To Market
URLLC	Ultra Reliable and Low Latency Communications
VIM	Virtualized Infrastructure Manager
VNF	Virtualized Network Function
VNFaaS	VNF as a Service
VNFM	VNF Manager
VPN	Virtual Private Network
VR	Virtual Reality
WAN	Wide Area Network
XaaS	X-as-a-Service (Anything as a Service)
ZSM	Zero-touch network and Service Management

4 Introduction

The present document describes the scenarios and requirements for zero-touch network and service management investigated by the ETSI ISG ZSM with the focus on automation as well as an E2E perspective.

These scenarios and derived requirements are used in other documents by ETSI ISG ZSM such as ETSI GS ZSM 002 [1], ETSI GS ZSM 003 [i.7] and ETSI GS ZSM 008 [i.8].

The scenarios and requirements allow the ZSM reference architecture and corresponding solutions to be aligned in scope and to be industry-relevant. The scenarios are grouped into key areas for automation and zero-touch operation respectively. They show the value of the ZSM framework reference architecture towards an E2E view and towards automated management functionalities as well as management services applicable to future-proof scenarios. Legacy environments are also considered for incremental deployment of automation and zero-touch technologies.

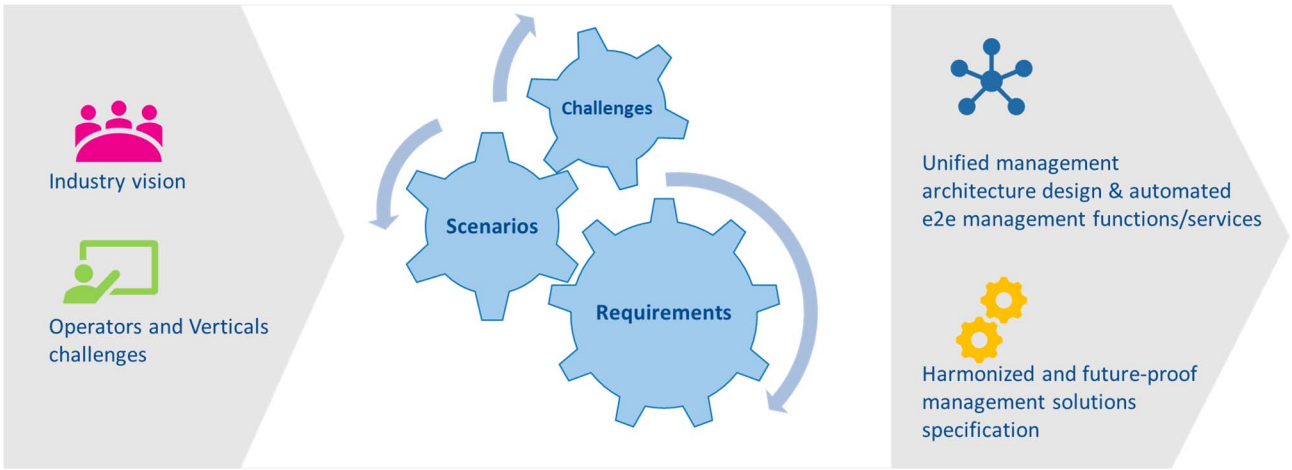

Figure 4-1: From operators and vertical industry problem statements and towards requirements for an E2E automated management architecture and solutions

The scenarios described in the present document identify business-oriented and automation-related challenges faced by operators and vertical industries, and allow deriving architectural, functional, non-functional and operational requirements.

The present document defines 39 scenarios grouped in different categories (and sub-categories) outlining the importance and emphasis of topics such as the management and operation of network slicing in 5G networks, the Network as a Service model, the use and integration of machine learning techniques for network management and operation, collaborative or federated service management, security, testing, tracing, and other important topics like integration and interoperation.

Analysing the scenarios and requirements from another angle allows identifying categories in slightly different dimensions such as:

- Scenarios and requirements related to use cases and which are more technology- or implementation-specific, e.g. network slicing management, edge computing, applied in 5G network, etc.
- Scenarios and requirements that can be considered as building blocks for automatic management for example concerning software management, policy management, bandwidth management, AI techniques, security management, etc.
- Scenarios and requirements that describe ways of implementing E2E automation and zero-touch management, e.g. closed loop automation, coordination between domains, integration of management services, etc.

These different viewpoints can be helpful in case the goal of the reader/stakeholder is to derive priorities among the requirements.

The scenario categories are listed below with short descriptions concerning their contents.

E2E network and service management

The scenarios and requirements that are categorized into this group are related to automating the operational tasks of managing the network. The scope of the ETSI ISG ZSM covers the management of the different technological domains such as Core, RAN and Transport domains, and also includes the management of different types of resources such as VNFs, SDNs, virtual and physical resources, etc., This scenario category focuses on the automation of E2E lifecycle management of all of different types of the network resources and services, including installation, commissioning, configuration, day-2 operations, software upgrades and decommissioning. This category also includes the E2E management solutions for network slicing such as network slice cloning, isolation of network slices to ensure a sufficient level of independency between the network slice instances with tolerable interference, cross-domain network slicing management capability, etc.

Network-as-a-Service (NaaS)

This group focuses on the need for service capabilities exposure from all domains to enable zero touch automation, and to allow for a seamless integration of new products in the network. Network slicing is taken as an example to show what capabilities could be exposed from each domain to allow E2E automation management.

Analytics & machine learning

This group focuses on the scenarios that drive the need for analytics, machine learning and AI capabilities in the ZSM framework. Examples of business requirements that are categorized into this group include the capability to determine the root cause of a network anomaly, and the capability to predict network capacity exhaustion. These requirements drive further functional requirements such as collection of historical data, access to continuous up-to-date network traffic information and ML sandbox environment for self-learning. Analytics and machine learning capabilities are used in the closed-loop automation of the ZSM framework.

Collaborative/federated service management

This group focuses on the business requirements for management and collaboration across multiple operators' domains. An example of requirement includes the advertisement and discovery of the management services from other operators' management domains.

Security

Security, regulatory and privacy requirements for ZSM framework reference architecture are captured in ETSI ZSM 002 [1], and there are a few security-related requirements that are included in other groups such as NaaS and analytics & machine learning. This security group captures additional security-related features such as the handling of decrypting management traffic for troubleshooting purposes.

Testing

Testing group captures the business requirements for features such as automated testing of a managed resource as it is being deployed or testing of an E2E service in the production network. These automated testing features could be incorporated into the closed-loop automation of a resource or service deployment, and in support of finding the root cause of an anomaly. Additionally, requirements related to CI/CD for network services and the automated testing capabilities in connection with AI and machine learning functionalities are also included in this group.

Tracing

Tracing group includes the business requirements for automated tracing that can be triggered by events such as anomaly detection where troubleshooting and root cause analysis need to be performed. Automated tracing capabilities and execution are based on information such as rules, policies, data models, configuration data, etc.

Integration/interoperation

This group focuses on the integration and interoperation between the ZSM framework and other entities such as ZSM framework consumers e.g. user portal, other providers' domains, and human interactions.

5 List of requirements

5.1 Introduction

This clause lists the requirements which are derived from the documented scenarios in clause 6 to the corresponding scenarios are included in the table for each of the requirements. The requirements are assigned to different categories.

For further clarifications and the related detailed context of the requirements, please refer to clause 6.

Some of these requirements are further refined and broken down into multiple functional and non-functional requirements for example in ETSI GS ZSM 002 [1].

5.2 Requirements

Requirements captured from clause 6 are listed in the table 5.2-1.

Table 5.2-1: Requirements based on documented scenarios that are described in clause 6

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
1	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of cloning of network slice instance(s).	6.2.1.1	Network slice lifecycle management
2	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of identifying network functions and resources by analysing the requirements for creating network slice instances.	6.2.1.1	Network slice lifecycle management
3	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of analysing the status of the network resources in the commissioning phase.	6.2.1.1	Network slice lifecycle management

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
4	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of scaling of network slice instances within available network resources.	6.2.1.1	Network slice lifecycle management
5	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of updating the configuration of network slice instances during the operation without disruption.	6.2.1.1	Network slice lifecycle management
6	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of rebalancing network resources in use to improve the network utilization efficiency without service disruption after deleting network resource(s).	6.2.1.1	Network slice lifecycle management
7	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of defining tolerable level of performance deterioration of each network slice instance in the commissioning phase by analysing SLA.	6.2.1.2	Network slice isolation management
8	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of monitoring the status of all the network slice instances and should identify the network slice instance which causes high utilization of network resource(s).	6.2.1.2	Network slice isolation management
9	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of monitoring the utilization of the network resources.	6.2.1.2	Network slice isolation management
10	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of identifying when the performance deterioration of a network slice instance(s) goes beyond the tolerable level, and the reconfiguration of network functions as well as the reallocation of network resources maximal until the tolerable level of the performance deterioration.	6.2.1.2	Network slice isolation management

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
11	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability of collecting performance data and fault data for a network instance. NOTE 1: The network instance can be network resource, network function, network slice and network services, etc.	6.2.1.3	Network slice monitoring
12	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework should support the capability of identifying root cause of a network issue based on the analysis on the collected data.	6.2.1.3	Network slice monitoring
13	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework should support the capability of taking actions to mitigate the performance degradation of a network instance. NOTE 2: The network instance can be network resource, network function, network slice and network services, etc.	6.2.1.3	Network slice monitoring
14	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework should support the capability of taking actions to perform predictive maintenance of a network instance. NOTE 3: The network instance can be network resource, network function, network slice and network services, etc.	6.2.1.3	Network slice monitoring
15	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability to make the management coordination across different technical domains, including at least Core network domain, RAN network domain, transport network domain and virtualization part to support network slicing management.	6.2.1.4	E2E network slicing provisioning in support of 5G services
16	6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration	ZSM framework shall support the capability to coordinate between different managed domains to support the performance monitoring of the end to end network services and the end to end network slicing.	6.2.1.5	Performance monitoring of E2E network slicing and service in support of 5G network and service
17	6.2.2 E2E automation of 5G network slice management and orchestration in support of 5G services (network slice as a service)	It should be possible for an authorized vertical industry customer to access the exposed information about NSaaS including performance and fault information of the network slice.	6.2.2.1	Exposure to support management and orchestration of NSaaS

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
18	6.2.2 E2E automation of 5G network slice management and orchestration in support of 5G services (network slice as a service)	It shall be possible for authorized vertical industry customer to access network slicing management services exposed by the ZSM framework.	6.2.2.2	E2E 5G network slicing management and orchestration in support of 5G services
19	6.2.2 E2E automation of 5G network slice management and orchestration in support of 5G services (network slice as a service)	It shall be possible to verify the interoperability of the management services for E2E network slicing whether the vertical industry customers can access and use them.	6.2.2.2	E2E 5G network slicing management and orchestration in support of 5G services
20	6.2.3 Automation of E2E network and service management	ZSM framework shall support capabilities to perform FCAPS management automatically for compute, storage and network resources, NFs, slices and services for an automated operation.	6.2.3.1	Zero-touch full automation of 5G network and service management
21	6.2.3 Automation of E2E network and service management	ZSM framework shall support automated LCM of a 5G network including DN.	6.2.3.1	Zero-touch full automation of 5G network and service management
22	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of utilizing the benefits offered by cloud-native NF design and Software Defined Network (SDN) environments to realize fast operational response.	6.2.3.1	Zero-touch full automation of 5G network and service management
23	6.2.3 Automation of E2E network and service management	ZSM framework shall support automated management of network slicing for the 5G network as a payload.	6.2.3.1	Zero-touch full automation of 5G network and service management
24	6.2.3 Automation of E2E network and service management	ZSM framework shall support the exposure of management interfaces to third parties without any adverse effect on exposing network operator.	6.2.3.1	Zero-touch full automation of 5G network and service management
25	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of utilizing management interfaces exposed by third parties to realize an automated operation of the operator's own services built on the top of the provided networks.	6.2.3.1	Zero-touch full automation of 5G network and service management
26	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to expose the network utilization (such as CPU, memory, bandwidth, and data throughput) of managed resources for a given Customer-Facing Service (CFS) and over a given time period. An example of where this information can be used is in a closed-loop automation where CFS-level network troubleshooting needs to be performed by ZSM framework.	6.2.3.2	Automated network bandwidth management
27	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to locate the resources that are the bottleneck(s) for a given E2E service.	6.2.3.2	Automated network bandwidth management

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
28	6.2.3 Automation of E2E network and service management	ZSM framework should support the capability to predict the growth or reduction of traffic volume for managed resources for a Customer-Facing Service (CFS) and over a given time period. An example of where this information can be used is in a closed-loop automation where CFS-level network troubleshooting needs to be performed by ZSM framework.	6.2.3.2	Automated network bandwidth management
29	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to optimize the routes of traffic for a given CFS to meet the service requirements.	6.2.3.2	Automated network bandwidth management
30	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to predictively detect abnormal behaviours of the managed networks and services.	6.2.3.3	ZSM automated healing
31	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to automatically restore the managed networks and services to normal operation.	6.2.3.3	ZSM automated healing
32	6.2.3 Automation of E2E network and service management	ZSM framework shall have the capability to perform recovery actions based on the required KPIs of the managed networks and services.	6.2.3.3	ZSM automated healing
33	6.2.3 Automation of E2E network and service management	ZSM framework shall have the capability to interoperate with non-automated management systems.	6.2.3.3	ZSM automated healing
34	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to automatically display such as show or report on E2E service topology, including network functionalities and their relationships.	6.2.3.4	Automated E2E network and service topology management
35	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to automatically display such as show or report on network topology across domains, including physical and logical links between physical and virtualized resources of a given managed network.	6.2.3.4	Automated E2E network and service topology management
36	6.2.3 Automation of E2E network and service management	ZSM framework shall have the capability to automatically update the topology information upon network or service changes.	6.2.3.4	Automated E2E network and service topology management
37	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of E2E, automated management and orchestration of ultra-low latency communication services.	6.2.3.5	Scenario for a zero-touch E2E 5G network and service management as well as orchestration including edge computing
38	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of E2E, automated management and orchestration of ultra-reliable low latency communication services.	6.2.3.5	Scenario for a zero-touch E2E 5G network and service management as well as orchestration including edge computing

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
39	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of automated management and orchestration of edge computing.	6.2.3.5	Scenario for a zero-touch E2E 5G network and service management as well as orchestration including edge computing
40	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of zero-touch, E2E management and orchestration of 5G networks and services covering network slicing and edge computing.	6.2.3.5	Scenario for a zero-touch E2E 5G network and service management as well as orchestration including edge computing
41	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of automatic pre-verification to ensure the management software deployment condition is met.	6.2.3.6	Automatic software deployment
42	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of automatic installation of management software.	6.2.3.6	Automatic software deployment
43	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of automatic configuration of management software parameters.	6.2.3.6	Automatic software deployment
44	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to automatically verify the management software status after deployment.	6.2.3.6	Automatic software deployment
45	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of automatic pre-verification of network functions normality and infrastructure conditions before deployment.	6.2.3.6	Automatic software deployment
46	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to automatically install physical and virtualized network functions software.	6.2.3.6	Automatic software deployment
47	6.2.3 Automation of E2E network and service management	ZSM framework shall support automatic configuration of physical and virtualized network function parameters.	6.2.3.6	Automatic software deployment
48	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of automatic verification of physical and virtualized network functions normality after deployment.	6.2.3.6	Automatic software deployment
49	6.2.3 Automation of E2E network and service management	ZSM framework shall support automatic network function SW upgrade within a production environment, at least to the latest released version.	6.2.3.7	Automatic software upgrade

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
50	6.2.3 Automation of E2E network and service management	ZSM framework shall support automatic upgrade of management services within a production environment, at least to the latest released version.	6.2.3.7	Automatic software upgrade
51	6.2.3 Automation of E2E network and service management	ZSM framework shall support automatic verification before SW upgrade to ensure the upgrade conditions are meet.	6.2.3.7	Automatic software upgrade
52	6.2.3 Automation of E2E network and service management	ZSM framework shall support automatic verification after SW upgrade to ensure success of upgrading.	6.2.3.7	Automatic software upgrade
53	6.2.3 Automation of E2E network and service management	ZSM framework shall support automatic rollback to the previous SW version if rollback condition is met during or after upgrade process.	6.2.3.7	Automatic software upgrade
54	6.2.3 Automation of E2E network and service management	ZSM framework should support the capability to perform in-service SW upgrading of management services.	6.2.3.7	Automatic software upgrade
55	6.2.3 Automation of E2E network and service management	ZSM framework should support the capability to perform in-service SW upgrading of network functions.	6.2.3.7	Automatic software upgrade
56	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to specify policies.	6.2.3.8	Automation using policies
57	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to define the policies in a technology independent policy definition language. NOTE 4: Further characteristics are beyond of the scope of the present document.	6.2.3.8	Automation using policies
58	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to at least store, delete, activate and deactivate policies.	6.2.3.8	Automation using policies
59	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to make use of the policy capabilities of the entities it manages.	6.2.3.8	Automation using policies
60	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to manage the defined policies.	6.2.3.8	Automation using policies
61	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to detect policy conditions.	6.2.3.8	Automation using policies
62	6.2.3 Automation of E2E network and service management	ZSM framework shall have the capability to decide on policy execution.	6.2.3.8	Automation using policies

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
63	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to trigger the actions defined in the policies.	6.2.3.8	Automation using policies
64	6.2.3 Automation of E2E network and service management	ZSM framework shall have the capability to detect conflicting policies.	6.2.3.8	Automation using policies
65	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to allow different sets of collected data to be used in different closed loops inside a domain and cross-domain.	6.2.3.9	Closed loop automation
66	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to normalize data that are not in common format, so that their meaning and significance can be understood in the proper context.	6.2.3.9	Closed loop automation
67	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to analyse the collected data to detect the undesired states and derive the root cause. The past, current and future states of the managed entities can be modelled to help to detect the undesired states and move the state of managed entities to the desired state.	6.2.3.9	Closed loop automation
68	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to decide which actions and when to execute, and then execute the actions based on the analytics results.	6.2.3.9	Closed loop automation
69	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability to detect and resolve any conflict between different closed loops inside a domain and in different domains.	6.2.3.9	Closed loop automation
70	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of nested closed loops.	6.2.3.9	Closed loop automation
71	6.2.3 Automation of E2E network and service management	ZSM framework shall support standardized interface(s) for VNF provisioning to realize E2E network service.	6.2.3.10	Full automation of VNF provisioning
72	6.2.3 Automation of E2E network and service management	ZSM framework shall support fully automated flow of data which are used in each process. NOTE 5: Processes here refer to but not limited to equipment planning, designing, testing and deployment process.	6.2.3.10	Full automation of VNF provisioning
73	6.2.3 Automation of E2E network and service management	ZSM framework shall support the capability of demand forecast for capacity planning.	6.2.3.10	Full automation of VNF provisioning
74	6.2.3 Automation of E2E network and service management	ZSM framework shall enable automated detection of management services offered by a management domain.	6.2.3.11	Automated detection of services offered by management domains

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
75	6.2.3 Automation of E2E network and service management	ZSM framework shall enable automated detection of changes in management services offered by a management domain.	6.2.3.11	Automated detection of services offered by management domains
76	6.2.3 Automation of E2E network and service management	ZSM framework shall enable automated detection of management service termination.	6.2.3.11	Automated detection of services offered by management domains
77	6.2.3 Automation of E2E network and service management	ZSM framework shall support the interoperation with APIs (MANO) for management of NFV network services.	6.2.3.12	Service management by 3GPP management system and ETSI NFV MANO
78	6.2.3 Automation of E2E network and service management	ZSM framework shall support the interoperation with APIs (3GPP SBMA) for management of 3GPP services and functions.	6.2.3.12	Service management by 3GPP management system and ETSI NFV MANO
79	6.3 Network as a service	ZSM framework shall support interworking with legacy management systems.	6.3.1	NaaS lifecycle and exposure with a network slicing scenario
80	6.3 Network as a service	ZSM framework shall support monitoring of managed services (network as a service including network slicing as a service) originating from different network/infrastructure domains including but not limited to NFVI, IP/SDN networks, Front haul, and Radio.	6.3.1	NaaS lifecycle and exposure with a network slicing scenario
81	6.3 Network as a service	ZSM framework shall support reconfiguration of any domain NaaS as required, e.g. in support of closed-loop assurance.	6.3.1	NaaS lifecycle and exposure with a network slicing scenario
82	6.3 Network as a service	ZSM framework shall support managing the complete lifecycle of the network services/capabilities exposed per management domain, and shall provide an interface that hides internal details (such as the resource layer).	6.3.1	NaaS lifecycle and exposure with a network network slicing scenario
83	6.3 Network as a service	ZSM framework shall support security capabilities when delivering automated network and service management.	6.3.1	NaaS lifecycle and exposure with a network slicing scenario
84	6.4 Analytics & machine learning	ZSM framework shall support the capability to collect up-to-date telemetry data (such as performance data, KPIs, and alarms).	6.4.1	Access to up-to-date telemetry data
85	6.4 Analytics & machine learning	ZSM framework shall support the capability of common access to the collected up-to-date telemetry data, both inside a domain and cross-domain.	6.4.1	Access to up-to-date telemetry data
86	6.4 Analytics & machine learning	ZSM framework shall support the capability of enforcing a data governance scheme for the common access to telemetry data.	6.4.1	Access to up-to-date telemetry data
87	6.4 Analytics & machine learning	ZSM framework shall support the capability to store telemetry data (or to steer their appropriate storage).	6.4.1	Access to up-to-date telemetry data

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
88	6.4 Analytics & machine learning	ZSM framework shall support the capability to (pre-)process and filter the telemetry data, and to perform cross-domain data aggregation. NOTE 6: Filtering can be applied at the source or the destination of the data, or in intermediate entities.	6.4.1	Access to up-to-date telemetry data
89	6.4 Analytics & machine learning	ZSM framework shall support the capability to check/validate the integrity of telemetry data, in particular in case of distributed data stores/replication.	6.4.1	Access to up-to-date telemetry data
90	6.4 Analytics & machine learning	ZSM framework shall support the capability to manage the distribution of telemetry data, and keep distributed data consistent.	6.4.1	Access to up-to-date telemetry data
91	6.4 Analytics & machine learning	ZSM framework shall support the capability to provide telemetry data to the data consumer according to the data consumer's requirements concerning but not limited to relevant data, relevant time, and relevant form).	6.4.1	Access to up-to-date telemetry data
92	6.4 Analytics & machine learning	ZSM framework shall support the management of composite services.	6.4.2	Machine learning for network & service automation
93	6.4 Analytics & machine learning	ZSM framework shall support interfaces that facilitate the integration of Machine Learning-as-a-Service frameworks into a zero-touch automation environment.	6.4.2	Machine learning for network & service automation
94	6.4 Analytics & machine learning	ZSM framework shall allow for ways of measuring KPIs. NOTE 7: The exact types of KPIs and their evolution could be considered in the next version of the present document.	6.4.2	Machine learning for network & service automation
95	6.4 Analytics & machine learning	ZSM framework should support stepwise introduction of ML based management, allowing a mixed environment of traditional and ML algorithms while the maturity of and confidence in ML assets increase.	6.4.2	Machine learning for network & service automation
96	6.4 Analytics & machine learning	ZSM framework shall support the capability to store historical data that is needed for the prediction and make it accessible to the analytics.	6.4.3	Predictive analytics
97	6.4 Analytics & machine learning	ZSM framework shall support the capability to introduce data analytics for predicting KPI changes and failure conditions.	6.4.3	Predictive analytics
98	6.4 Analytics & machine learning	ZSM framework shall support the capability to set conditions (KPIs or policy conditions) that need to be monitored.	6.4.4	Real time monitoring analysis
99	6.4 Analytics & machine learning	ZSM framework shall support the capability to monitor the state of the managed resources.	6.4.4	Real time monitoring analysis
100	6.4 Analytics & machine learning	ZSM framework shall support the capability to detect undesired conditions and trigger appropriate actions.	6.4.4	Real time monitoring analysis
101	6.4 Analytics & machine learning	ZSM framework should support the capability to analyse conditions to detect root causes.	6.4.4	Real time monitoring analysis
102	6.4 Analytics & machine learning	ZSM framework should support passive access to continuous up to date traffic in the network or service topology for an authorized consumer within the ZSM framework via relevant streaming APIs.	6.4.5	Proposal for analytics domains and concepts for interaction

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
103	6.4 Analytics & machine learning	ZSM framework shall support means to provide the current logical and physical topology of a network and service for an authorized consumer within the ZSM framework.	6.4.5	Proposal for analytics domains and concepts for interaction
104	6.4 Analytics & machine learning	ZSM framework shall support the ability for the authorized consumer within a management domain to relay a specific request for telemetry, trace or traffic to another management domain. Responding management domain shall be able to decline requests for telemetry, trace or traffic based on policy, security, operational or other considerations.	6.4.5	Proposal for analytics domains and concepts for interaction
105	6.4 Analytics & machine learning	ZSM framework shall support capabilities to evaluate and report the QoS of a network or a service, over either a specific duration of time or continuously over the service usage in near-real time.	6.4.5	Proposal for analytics domains and concepts for interaction
106	6.4 Analytics & machine learning	ZSM framework shall support capabilities to identify the root cause of a network or service degradation. The root cause provided should be deterministic.	6.4.5	Proposal for analytics domains and concepts for interaction
107	6.4 Analytics & machine learning	ZSM framework shall support capabilities to evaluate and report the QoE of a service or a network service over either a specific duration of time or continuously over the service usage.	6.4.5	Proposal for analytics domains and concepts for interaction
108	6.4 Analytics & machine learning	ZSM framework shall support collection of data from all managed entities within the ZSM framework that are necessary to perform automated network and service management based on AI. NOTE 8: Data here refer to but not limited to configuration data, history data, operational data, topological data, inventory data.	6.4.6	AI for network and service automation
109	6.4 Analytics & machine learning	ZSM framework shall ensure that data is available not only inside management domains but also outside them so that such data can be available to any authorized consumer within the ZSM framework belonging to one operator.	6.4.6	AI for network and service automation
110	6.4 Analytics & machine learning	ZSM framework shall support the capability to make ZSM framework functional components as managed entities that can be deployed independently.	6.4.7	CI/CD for ZSM framework functional components
111	6.4 Analytics & machine learning	ZSM framework shall support the capability to change and upgrade functional components of ZSM framework without impacting other functional components and ZSM services.	6.4.7	CI/CD for ZSM framework functional components
112	6.4 Analytics & machine learning	ZSM framework shall support the capability for automated lifecycle management of ZSM framework functional components. NOTE 9: Examples are deploy, delete, upgrade, etc.	6.4.7	CI/CD for ZSM framework functional components
113	6.4 Analytics & machine learning	ZSM framework shall enable interoperation between DevOps and operator CI/CD systems, in a way that does not require changes to the CI/CD systems themselves.	6.4.7	CI/CD for ZSM framework functional components
114	6.4 Analytics & machine learning	Functional components of ZSM framework should be reusable and interchangeable.	6.4.7	CI/CD for ZSM framework functional components
115	6.4 Analytics & machine learning	ZSM framework shall support the use of automated decision loops, with different characteristics and scope, as a means to perform network and service management.	6.4.8	Zero-touch self-optimizing network

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
116	6.4 Analytics & machine learning	ZSM framework shall provide an interface for the purpose of bringing decision criteria to the decision loops, i.e. triggers, policies.	6.4.8	Zero-touch self-optimizing network
117	6.4 Analytics & machine learning	ZSM framework shall provide means to hinder an overarching loop from infringing on a more local loop's responsibility. Exceptions from this rule shall be possible based on operator preferences.	6.4.8	Zero-touch self-optimizing network
118	6.4 Analytics & machine learning	ZSM framework shall enable the collection of all relevant and available data, and the corresponding context information, needed by a specific decision loop. NOTE 10: Care has to be taken not to overload the ZSM framework resources.	6.4.8	Zero-touch self-optimizing network
119	6.4 Analytics & machine learning	ZSM framework shall be able to evaluate the network resources needed to enable the collection of data for each decision loop. NOTE 11: The purpose is to perform a cost/benefit analysis.	6.4.8	Zero-touch self-optimizing network
120	6.4 Analytics & machine learning	ZSM framework shall enable monitoring of the effects of automation functions to build trust in every stage of increased automation towards a fully automated solution.	6.4.8	Zero-touch self-optimizing network
121	6.4 Analytics & machine learning	ZSM framework shall enable the network owner to disable any automation function in case of malfunction.	6.4.8	Zero-touch self-optimizing network
122	6.4 Analytics & machine learning	ZSM framework shall provide access to operational and historical data to authorized consumers.	6.4.9	Self-learning based on reinforcement learning
123	6.4 Analytics & machine learning	ZSM framework shall allow the creation and execution of ML sand-box environments where self-learning algorithms can get access and use data.	6.4.9	Self-learning based on reinforcement learning
124	6.4 Analytics & machine learning	ZSM framework shall provide means to store self-learning software´s knowledge in a persistent manner.	6.4.9	Self-learning based on reinforcement learning
125	6.4 Analytics & machine learning	ZSM framework shall support the capability of collecting and storing data obtained in both training phase and operation phase such as performance, log, alarm, topology, trouble information, etc.	6.4.10	Optimization of supervised/ unsupervised learning used in management services for closed loop
126	6.4 Analytics & machine learning	ZSM framework shall support the capability of exposing the stored data set obtained in training/operation phase to ML used in management services to enhance the accuracy of ML based on these data.	6.4.10	Optimization of supervised/ unsupervised learning used in management services for closed loop
127	6.5 Collaborative/federated service management	ZSM framework shall support the capability of the automated creation and management of communication services and network slice instances hosted across multiple operators.	6.5.1	Communication services hosted across multiple operators
128	6.5 Collaborative/federated service management	ZSM framework shall support the capability of the automated service advertisement to and discovery from other operators' management domains.	6.5.1	Communication services hosted across multiple operators
129	6.5 Collaborative/federated service management	ZSM framework shall support the capability of the communication service decomposition and the automated communication service requests to multiple other network operators.	6.5.1	Communication services hosted across multiple operators

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
130	6.5 Collaborative/federated service management	ZSM framework shall support the capability to provide the interfaces' exposures for the automated management of the services.	6.5.1	Communication services hosted across multiple operators
131	6.5 Collaborative/federated service management	ZSM framework shall support the capability of managing the private communication services based on requests coming from enterprises via APIs with minimal manual interaction.	6.5.2	Private communication services hosted by an operator
132	6.5 Collaborative/federated service management	ZSM framework shall support the capability to allow the network operator to instantiate the network slice subnet instance over the enterprise premises (networks).	6.5.2	Private communication services hosted by an operator
133	6.5 Collaborative/federated service management	ZSM framework shall support the capability of managing the private communication service with a network slice instantiated on the enterprise's network and the operator's network.	6.5.2	Private communication services hosted by an operator
134	6.5 Collaborative/federated service management	ZSM framework shall support the capability to offer APIs that allow enterprises to operate the private communication services according to their needs.	6.5.2	Private communication services hosted by an operator
135	6.5 Collaborative/federated service management	ZSM framework shall support hierarchical and federated orchestration. NOTE 12: Hierarchical and federated orchestration are not the only way of orchestration that ZSM framework supports. Others can be addressed by other requirements.	6.5.3	Automation in multi-stakeholder ecosystems
136	6.5 Collaborative/federated service management	ZSM framework shall support orchestration across management domains that belong to different administrative entities.	6.5.3	Automation in multi-stakeholder ecosystems
137	6.5 Collaborative/federated service management	ZSM framework shall support capabilities for abstracted exposure of resources and topology between different network providers.	6.5.3	Automation in multi-stakeholder ecosystems
138	6.5 Collaborative/federated service management	ZSM framework shall support automated composition of services based on service components provided by multiple stakeholders. NOTE 13: Examples of components that can be used to compose services are VNF components.	6.5.3	Automation in multi-stakeholder ecosystems
139	6.5 Collaborative/federated service management	ZSM framework shall support automated onboarding of service and services components provided by 3rd parties. NOTE 14: Examples of 3rd parties are verticals or other operators.	6.5.3	Automation in multi-stakeholder ecosystems
140	6.6 Security	ZSM framework shall support the capability of decryption of management traffic. NOTE 15: This is for troubleshooting purposes by an authorized consumer within the ZSM framework.	6.6.1	Troubleshooting of encrypted traffic in ZSM framework
141	6.6 Security	ZSM framework shall support the capability of decryption of traffic without support from the network entity involved in the communication.	6.6.1	Troubleshooting of encrypted traffic in ZSM framework
142	6.6 Security	ZSM framework shall not impact the network entity performance while decryption is supported.	6.6.1	Troubleshooting of encrypted traffic in ZSM framework
143	6.6 Security	ZSM framework shall inform the owner of the ZSM framework that decryption is possible by the authorized consumer for the traffic sent during the duration of the troubleshooting process.	6.6.1	Troubleshooting of encrypted traffic in ZSM framework
144	6.6 Security	ZSM framework shall inform the owner of the network entity/network entities involved that decryption is possible by the authorized consumer for the traffic sent during the troubleshooting process on demand.	6.6.1	Troubleshooting of encrypted traffic in ZSM framework

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
145	6.7 Testing	ZSM framework shall support the capability to perform automated system tests of a network service deployed in multiple network domains including but not limited to access, transport, core and cloud.	6.7.1	Automated system test in production network
146	6.7 Testing	ZSM framework shall support the capability to automatically deploy and configure necessary testing functions for automated system tests across multiple network domains including but not limited to access, transport, core and cloud.	6.7.1	Automated system test in production network
147	6.7 Testing	ZSM framework shall support the capability to perform system tests of a network service without interfering other unrelated services.	6.7.1	Automated system test in production network
148	6.7 Testing	While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability to treat network services as standalone units that can be deployed independently from other unrelated services.	6.7.2	CI/CD for network services
149	6.7 Testing	While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability to change and upgrade the services without any impact on other unrelated network services.	6.7.2	CI/CD for network services
150	6.7 Testing	While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability to expose the interfaces of network service testing, deployment and upgrade, so that these actions can be triggered by a CI/CD pipeline.	6.7.2	CI/CD for network services
151	6.7 Testing	While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability to make use of the existing CI/CD toolchains.	6.7.2	CI/CD for network services
152	6.7 Testing	While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability of additional automated tests of network services. NOTE 16: See the detailed testing requirements in scenario "Automated system test in production network".	6.7.2	CI/CD for network services
153	6.7 Testing	ZSM framework shall support the capability of enabling interoperation between CI/CD pipeline in vendor environment and service provider CI/CD pipeline for the managed entities, in a manner that does not require changes to the tools of the CI/CD pipelines.	6.7.2	CI/CD for network services
154	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for service tests within test networks.	6.7.3	Automated test capabilities concerning ZSM
155	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for service tests within production/live networks via single and/or several administrative and technical domains.	6.7.3	Automated test capabilities concerning ZSM
156	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for active and passive testing of E2E services and/or only parts of them.	6.7.3	Automated test capabilities concerning ZSM
157	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for active and passive testing of management functionalities/capabilities.	6.7.3	Automated test capabilities concerning ZSM
158	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities based on several information such as rules, policies, profiles, models, configuration data, performance data, and SLAs/OLAs.	6.7.3	Automated test capabilities concerning ZSM

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
159	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities in connection with the automated conflict resolution handling within a single or between several administrative and/or technical domains.	6.7.3	Automated test capabilities concerning ZSM
160	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities in connection with AI and machine learning functionalities and applications.	6.7.3	Automated test capabilities concerning ZSM
161	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for service tests after the modification/update of this service.	6.7.3	Automated test capabilities concerning ZSM
162	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for service tests to support the finding of the root cause.	6.7.3	Automated test capabilities concerning ZSM
163	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities to identify the failure segment within an E2E service chain.	6.7.3	Automated test capabilities concerning ZSM
164	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated testing and management capabilities to recommend and/or to trigger appropriate follow-up actions.	6.7.3	Automated test capabilities concerning ZSM
165	6.7 Testing	ZSM framework shall support the capability of enabling the provisioning and the support of automated management and orchestration capabilities for the automated testing capabilities including their follow-up actions triggered by them.	6.7.3	Automated test capabilities concerning ZSM
166	6.8 Tracing	ZSM framework shall support the capability of enabling the automated management of automated tracing capabilities.	6.8.1	Automated tracing capabilities
167	6.8 Tracing	ZSM framework shall support the capability of enabling several tracing levels on demand in an automated way.	6.8.1	Automated tracing capabilities
168	6.8 Tracing	ZSM framework shall support the capability of enabling automated tracing capabilities in production/live networks without any impairment of the running E2E services.	6.8.1	Automated tracing capabilities
169	6.8 Tracing	ZSM framework shall support the capability of enabling automated tracing capabilities based on several information e.g. rules, policies, profiles, information and data models, configuration and performance data.	6.8.1	Automated tracing capabilities
170	6.8 Tracing	ZSM framework shall support the capability of enabling automated tracing capabilities with the use of AI and machine learning functionalities and applications.	6.8.1	Automated tracing capabilities
171	6.9 Integration/ interoperation	ZSM framework shall have the capability of managing the lifecycle of customer facing services.	6.9.1	ZSM framework as entity in an ecosystem
172	6.9 Integration/ interoperation	ZSM framework shall have the capability of managing the lifecycle of resource facing services.	6.9.1	ZSM framework as entity in an ecosystem
173	6.9 Integration/ interoperation	ZSM framework shall be able to interact with entities outside of itself (owner, consumer, provider).	6.9.1	ZSM framework as entity in an ecosystem
174	6.9 Integration/ interoperation	ZSM framework shall support the capability to interact with humans and to adjust to conditions where human intervention/reaction is required, e.g. using a GUI, web portal or application.	6.9.1	ZSM framework as entity in an ecosystem
175	6.9 Integration/ interoperation	ZSM services shall offer machine-consumable interfaces.	6.9.1	ZSM framework as entity in an ecosystem

Req. #	Scenario category	Requirements	Clause of the related scenario	Scenario title
176	6.9 Integration/ interoperation	ZSM services may provide means for interfacing with human users.	6.9.1	ZSM framework as entity in an ecosystem

6 Scenarios

6.1 Introduction

This clause contains scenario descriptions which are informative. Requirements will be derived from these scenarios.

The requirements are listed in clause 5 and have references to the corresponding scenarios.

6.2 E2E network and service management

6.2.1 E2E automation of 5G network slice as operator-internal management and orchestration

6.2.1.1 Network slice lifecycle management

6.2.1.1.1 Description

ZSM can be applied for the lifecycle management of network slices which is described in ETSI TS 128 530 [i.3]. The use of ZSM is relevant to reduce time-to-market of network slice.

6.2.1.1.2 Rationale and challenges

Each process of network slice lifecycle management requires identification and management of relevant network functions and resources. The identification of relevant network functions and resources is complicated particularly in the following cases:

- The requested network slice instance has specific network characteristics and existing templates cannot be easily applied.
- The structure of underling network infrastructure is complex.
- The allocation and reallocation of the network functions and resources happen frequently due to the dynamic demands for the large number of network slice instances.

To reduce time-to-market of network slice instances, automated mechanism performing complex procedures for the lifecycle management is essential.

6.2.1.1.3 ZSM scenario details

The lifecycle management of network slices is described in ETSI TS 128 530 [i.3]. The whole process of lifecycle management is divided into four phases; preparation, commissioning, operation and decommissioning.

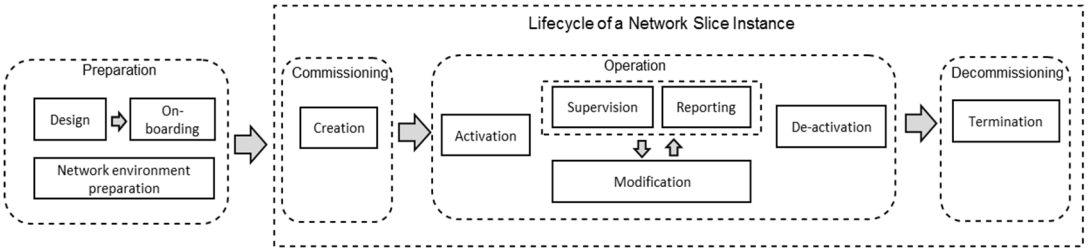

Figure 6.2.1.1.3-1: Management aspects of network slice (ETSI TS 128 530 [i.3])

Preparation

The preparation is a phase before the creation of network slice instances including template design and evaluation network slice requirements. Although basic templates with typical network characteristics can be produced by human involved process, ZSM can play some important roles in this phase to automate this. Template design can be automated by taking into account the previously produced network slice instances, as an example. The experience of the previously produced network slice instances can be feedback to template design for further improvement. In case that a demand for new types of network slice instances arises, the network slice provider can produce a new template based on the previous experience. ZSM can automate these processes (Req-1).

Commissioning

The network slice instances are created in the commissioning phase. Network slice instances with typical network characteristics can be created by utilizing a relevant slice template with minor adjustment and the creation process is simple. However, when a network slice instance with specific network characteristics for which no relevant template is available is requested, the network slice instance needs to be created from scratch collecting all the necessary network functions and resources without using a template (Req-2). This process is so complex that an automated mechanism is needed.

Identification of necessary network functions and resources needs understanding not only the requirements for the network slice instance but also available network resources to meet the objectives of the requested network slice instance (Req-3). Lack of technical knowledge as well as knowledge of available network resources of slice users makes the situation worse. Automated mechanism helps the slice users to identify the relevant network functions and resources.

Operation

The resources allocated to the network slice instances need to be continuously reviewed to ensure the expected performance of the slice customers. The allocated resources, for example bandwidth, need to be adjusted accordingly (Req-4). Addition of new functionalities or removal of unnecessary functionalities is also carried out (Req-5).

Decommissioning

When the network slice instance is terminated, all the allocated network functions and resources are released to be reallocated to other network slice instances. Although releasing the network functions and resources is a simple task, this process still has some room for further optimization of resource allocation. To improve the network performance, automated mechanism like ZSM should check the released resources and utilize them for further improvement of network performance (Req-6).

6.2.1.1.4 Related requirements for ZSM

The followings are the requirements extracted from the above scenario:

Req-1: ZSM framework shall support the capability of cloning of network slice instance(s).

Req-2: ZSM framework shall support the capability of identifying network functions and resources by analysing the requirements for creating network slice instances.

Req-3: ZSM framework shall support the capability of analysing the status of the network resources in the commissioning phase.

Req-4: ZSM framework shall support the capability of scaling of network slice instances within available network resources.

Req-5: ZSM framework shall support the capability of updating the configuration of network slice instances during the operation without disruption.

Req-6: ZSM framework shall support the capability of rebalancing network resources in use to improve the network utilization efficiency without service disruption after deleting network resource(s).

6.2.1.2 Network slice isolation management

6.2.1.2.1 Description

Isolation is a key feature of network slice. The slice customers expect that the performance of their network slice instances is independent from other slice instances. Conceptually, isolation is considered as a situation where one network slice instance avoids any interference from other network slice instances. However, complete isolation without interference between network slice instances is not feasible due to the technical constraint on the underlying network infrastructure.

In a practical sense, ensuring the sufficient level of independency between network slice instances is enough to meet the expectation of the slice customers although tolerable level of interference could happen between the network slice instances. To achieve sufficient level of independency with tolerable interference, the management system for network slice instances needs to carry out complex tasks such as analysis of the requirements of slice customers, status monitoring of the underlying network infrastructure and so on.

6.2.1.2.2 Rationale and challenges

In this scenario, isolation of network slice is defined as ensuring sufficient level of independency between the network slice instances with tolerable interference in respect of the requirements of the slice customers. To achieve this isolation, the following tasks should be carried out:

- Analysis of the requirements of the slice customer.
- Status monitoring of other network slice instances and the underlying network infrastructure that could give negative impacts.
- Assessment of negative impacts caused by the behaviour of other network slice instances and status change of the underlying network infrastructure.
- Carrying out necessary management on the network slice instance and related network functions and resources.

These are complex tasks which need an automated mechanism like ZSM.

6.2.1.2.3 ZSM scenario details

Depending on the underlying network infrastructure, the performance of the network slice instance may be affected by the behaviour of other network slice instances that are sharing certain resources with the network slice instance. For example, in case of packet based network infrastructure, network performance objectives such as packet loss, latency and jitter could be negatively affected by heavy traffic load from other network slice instances. A certain level of deterioration of network performance is tolerable depending on the requirement of the slice customers. For example, increase of 1 msec latency and jitter is tolerable for most video delivery services, but may not be tolerable for time critical M2M applications. This means that tolerable level of deterioration of network performance is case dependent. ZSM needs to analyse tolerable level of performance deterioration of each network slice instance based on the requirements of the slice customer (Req-1).

Deterioration of performance is caused by high utilization of resources. Identifying the network slice instance causing high utilization of resource(s) is important for making consequent reconfiguration and reallocation of network resources (Req-2). To ensure originally committed performance of affected network slice instance, reconfiguration and reallocation of network resources should be made. This reconfiguration and reallocation depend highly on the status of the available network resources (Req-3, Req-4).

6.2.1.2.4 Related requirements for ZSM

The followings are the requirements extracted from the above scenario:

Req-1: ZSM framework shall support the capability of defining tolerable level of performance deterioration of each network slice instance in the commissioning phase by analysing SLA.

Req-2: ZSM framework shall support the capability of monitoring the status of all the network slice instances and should identify the network slice instance which causes high utilization of network resource(s).

Req-3: ZSM framework shall support the capability of monitoring the utilization of the network resources.

Req-4: ZSM framework shall support the capability of identifying when the performance deterioration of a network slice instance(s) goes beyond the tolerable level, and the reconfiguration of network functions as well as the reallocation of network resources maximal until the tolerable level of the performance deterioration.

6.2.1.3 Network slice monitoring

6.2.1.3.1 Description

ZSM can be applied for the monitoring of the network slice instance during its lifecycle, such as fault, performance, status, configuration, etc. Based on the analysis on the monitoring data collected, the ZSM can automatically adjust the network slice instance resources, functions and the configurations with the pre-configured polices or experiences (e.g. machine learning) in a closed-loop way to ensure the requirements of slice customer continually satisfied.

6.2.1.3.2 Rationale and challenges

The fault or misconfiguration may degrade the performance of the network slice instance, and in the worst case will violate the committed SLA or even break down the network slicing instance operation. To ensure the requirements of slice customer, the following tasks should be carried out:

- Collecting of performance metrics data and fault data related to the slice instance.
- Analysing the monitoring data to identify the root causes of a network issue.
- Analysing the requirements of the slice customer.
- Determining the solutions when the requirements of slice customer are violated or executing predictive maintenance.
- Adjusting the functions, slice resources or configurations to ensure the committed SLA.

These tasks are very complex which need ZSM to be involved to avoid manual intervention.

6.2.1.3.3 ZSM scenario details

The fault happened to the underlying network infrastructure or network functions will affect the performance of the network slice instance. For example, the breakdown of a link or a function node in the network slice instance may negatively affect the packet and service processing capacity. As a result, the network performance will be degraded to satisfy the requirements of the slice customer. ZSM needs to re-evaluate the performance of each network slice instance based on the monitoring data collected with the requirements of the slice customer (Req-1, Req-2).

Identifying the root cause of a network issue with the network slice instance is important for taking the right actions to mitigate the performance degradation or perform predictive maintenance (Req-3, Req-4, Req-5). The automation actions taken by ZSM will ensure the SLA committed to the slice customer continuously satisfied (Req-2).

6.2.1.3.4 Related requirements for ZSM

The followings are the requirements extracted from the above scenario:

Req-1: ZSM framework shall support the capability of collecting performance data and fault data for a network instance.

NOTE 1: The network instance can be network resource, network function, network slice and network services, etc.

Req-2: ZSM framework should support the capability of identifying root cause of a network issue based on the analysis on the collected data.

Req-3: ZSM framework should support the capability of taking actions to mitigate the performance degradation of a network instance.

NOTE 2: The network instance can be network resource, network function, network slice and network services, etc.

Req-4: ZSM framework should support the capability of taking actions to perform predictive maintenance of a network instance.

NOTE 3: The network instance can be network resource, network function, network slice and network services, etc.

6.2.1.4 E2E network slicing provisioning in support of 5G services

6.2.1.4.1 Description

The 5G networks use network slices to achieve the necessary flexibility and scalability to support massive connections.

This first scenario focuses on provisioning the end to end network slice according to the customer service requirements. Day two operation and other life cycle management operations will be discussed in separate scenarios. Day two operation starts for example when a management service goes into operations and lasts until it is deleted or replaced with another one.

6.2.1.4.2 Rationale and challenges

The 5G E2E network slicing management provides the support to enable new business models and new communication services, such as eMBB, mIoT and Critical communication. Apart from the new access technology, 5G also enables new XaaS business model. Operators may act as both communication service provider and network services provider. The service quality, the service deployment efficiency, and network operational efficiency become rather critical to guarantee the desired services.

The key challenges are as follows:

Issue 1: The management system should be able to manage certain number of network slices. Network slice provisioning which could meet the operator new service deployment needs is critical.

Issue 2: The network slice may compose multi-vendor network nodes and multiple technical domains, the coordination needs to be resolved. An E2E network slice instance may be related with transport network part which includes Data Center Network (DCN) and Wide Area Network (WAN). The following diagram shows an example of the related domains in an E2E network slice instance. The coordination with different types of transport network is a challenge to build the E2E solution.

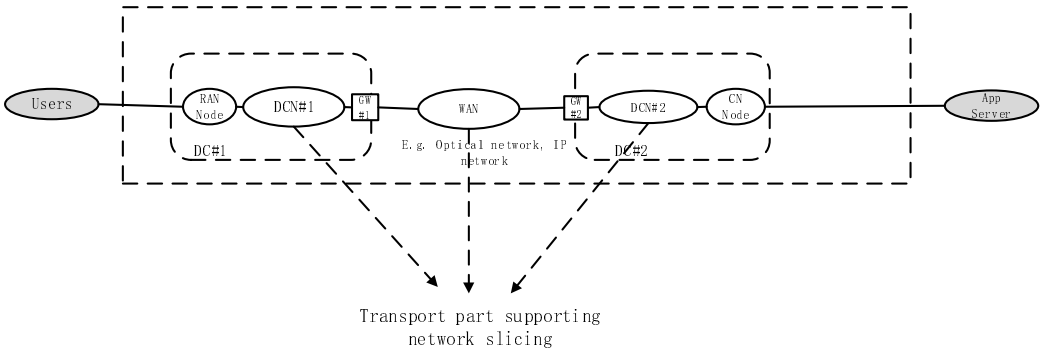

Figure 6.2.1.4.2-1: E2E network slice with different transport support

Issue 3: The network slice management system and the existing OSS need to be coordinated.

Issue 4: The services and resources used to instantiate the network slices need to provide the required isolation.

Issue 5: The management and orchestration for services and resources used to instantiate the network slices need to be able to manage the resource according to the slice characteristics.

6.2.1.4.3 ZSM scenario details

This scenario will describe the interactions between network slice customer and network slice provider.

The network slice customer plans to provide 5G services, e.g. eMBB, mIoT and critical communication etc. The customer will provide the 5G service requirements to the network slice provider.

The network slice provider uses these requirements in the following steps to deploy/instantiate slices:

- The customer-facing service related requirements are translated into network slice related requirements.
- The network slice related requirements are converted into the requirements on the constituent domains of the network slice (e.g. core/access/transport network domain related requirements).
- The requirements for each constituent domain are converted to network service related requirements on the network functions in each domain. Then the network functions can provide the network services satisfying the corresponding requirements on the constituent domain of the network slice.
- Each constituent domain of the network slice may prepare required network functions by using new network functions or reusing existing network functions via network virtualization technologies.
- Transport links within a constituent domain and between domains of the network slice are necessary to be setup.
- The network management functions of each domain provide configurations to the related network functions within each domain.

After these steps, the network slice, which satisfies the customer needs, is instantiated.

NOTE: Service related requirements from vertical industries have not been analysed. It could be considered in the next version of the present document.

6.2.1.4.4 Related requirements for ZSM

The requirement related to the ZSM includes:

Req-1: ZSM framework shall support the capability to make the management coordination across different technical domains, including at least Core network domain, RAN network domain, transport network domain and virtualization part to support network slicing management.

6.2.1.5 Performance monitoring of E2E network slicing and service in support of 5G network and service

6.2.1.5.1 Description

The 5G networks use network slices to achieve the necessary flexibility and scalability to support communication networks with more complexity and different communication services with more critical performance requirements.

This scenario focuses on the performance monitoring of end to end network slicing and service across different technical domains according to the performance measurements data.

6.2.1.5.2 Rationale and challenges

The 5G E2E network slice support to enable new communication services, such as eMBB, URLLC, mIoT and other critical communication services. Due to the diverse communication service types and corresponding service requirements, the performance of E2E network slicing and service is of great importance and with more complexity, the performance monitoring become rather critical to guarantee the desired services.

The key challenges are as follows:

Issue 1: A large number of performance measurements data of different domains need to be monitored.

Issue 2: The network slice may compose multi-vendor network nodes and multiple technical domains, the coordination needs to be resolved.

6.2.1.5.3 ZSM scenario details

This scenario will describe the performance monitoring to support end to end network slicing:

- Performance measurement data is reported of each technical domain to support performance monitoring of end to end network slicing and service.
- Reported PM data of different technical domains (e.g. latency of Core network, RAN network and transport network) are monitored to make sure if the end to end performance of communication services meets the desired services requirements.

NOTE: Service related requirements from vertical industries have not been analysed. It could be considered in the next version of the present document.

6.2.1.5.4 Related requirements for ZSM framework

The requirement related to the ZSM framework includes:

Req-1: ZSM framework shall support the capability to coordinate between different managed domains to support the performance monitoring of the end to end network services and the end to end network slicing.

6.2.2 E2E automation of 5G network slice management and orchestration in support of 5G services (network slice as a service)

6.2.2.1 Exposure to support management and orchestration of NSaaS

6.2.2.1.1 Description

The network slice can be used by the network slice customer in their working environment. From management point of view, the network slice customer needs convenient management interfaces. In the case of Network Slice as a Service (NSaaS) scenario as defined in ETSI TS 128 530 [i.3], clause 4.1.6, the network slice customer should be able to manage their own network slice instances.

6.2.2.1.2 Rationale and challenges

Network slice customer may need easy integration mechanism to integrate the usage of network slice into their own working environment. The information about the network slice should be clearly indicated in customer's management system.

6.2.2.1.3 ZSM scenario details

The exposure of the management capability depends on the different scenarios of the management requirements from the customer. For example:In the case of NSaaS business scenario as defined in ETSI TS 128 530 [i.3], the exposure management capability could be carried through the interface indicated in figure 6.2.2.1.3-1.

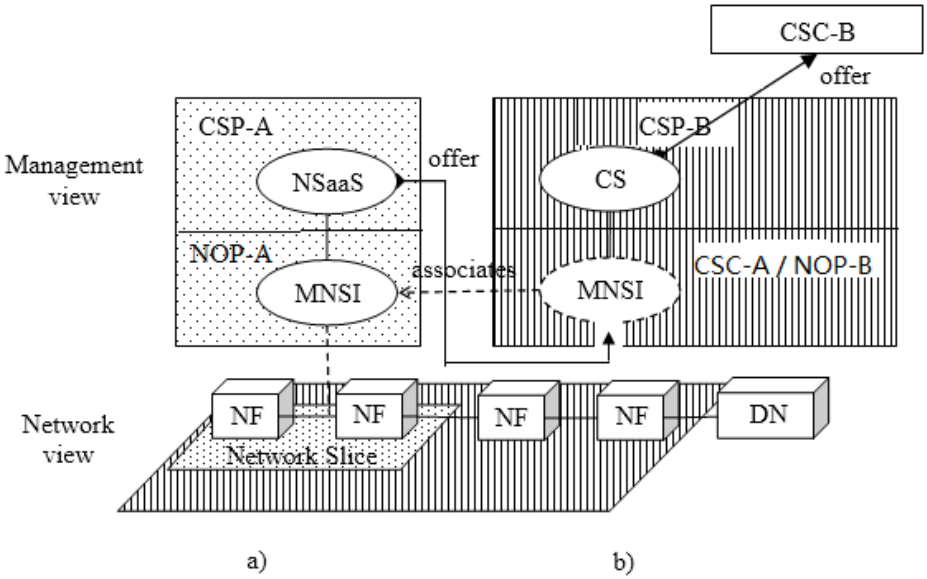

Figure 6.2.2.1.3-1: The exposure management capability could be carried through the interface indicated in the diagram

NOTE: The roles of CSP, CSC, NOP are described in ETSI TS 128 530 [i.3].

The network slice customer should be able to monitor the exposed performance and fault information of the network slice.

6.2.2.1.4 Related requirements for ZSM

This requirement is for the exposure capability to support management and orchestration of NSaaS:

Req-1: It should be possible for an authorized vertical industry customer to access the exposed information about NSaaS including performance and fault information of the network slice.

6.2.2.2 E2E 5G network slicing management and orchestration in support of 5G services

6.2.2.2.1 Description

The 5G networks need be more flexible and scalable to support massive connections. Operators will need to cope with vertical industry's needs to achieve the functions like Service diversity, guaranteed performance, fast deployment and short Time-To-Market (TTM), etc.

6.2.2.2.2 Rationale and challenges

The 5G E2E network slicing management provides the support to enable new business models and new communication services, such as eMBB, mIoT and Critical communication etc. Apart from the new access technology, 5G also enables new XaaS business model. Operators may act as communication service provider or network services provider depends on different requirements from the market. In addition to B2C service, operator may also need to provide B2B service. The service quality, the service deployment efficiency, and network operational efficiency become rather critical to guarantee the desired services in 5G.

The key challenges are as follows:

Issue 1: The requirements from vertical industries may need to be considered by the management system as the inputs for network design and deployment.

Issue 2: The management system may need to have the capability allowing vertical industry to manage certain aspects of network slice.

Issue 3: Because the network slice is built on multi-vendor network and across multiple technical domains, the coordination between different vendors and domains may be difficult.

Issue 4: The coordination between network slice management system and the existing OSS/EMS need further discussion.

6.2.2.2.3 ZSM scenario details

The E2E network slicing management and orchestration include the following aspects:

- Exposure capability support to the vertical industry.
- Life cycle management of network slicing.
- Performance management of network slicing.
- Fault management of network slicing.

The E2E network slice management and orchestration include the coordination with different standard or open source groups.

6.2.2.2.4 Related requirements for ZSM

The E2E network slicing management and orchestration include:

Req-1: It shall be possible for authorized vertical industry customer to access network slicing management services exposed by the ZSM framework.

Req-2: It shall be possible to verify the interoperability of the management services for E2E network slicing whether the vertical industry customers can access and use them.

6.2.3 Automation of E2E network and service management

6.2.3.1 Zero-touch full automation of 5G network and service management

6.2.3.1.1 Description

A 5G network consists of NG Radio Access Network (NG-RAN) [i.5], 5G Core (5GC) [i.6] and a transport network connecting different Network Functions (NFs) in NG-RAN and 5GC. A gNB is an example of NG-RAN NF, and an Access and Mobility Management Function (AMF) is an example of 5GC NF. 3GPP is continuing works to support network slicing in both NG-RAN and 5GC.

At present, taking 4G network as an example, operator-specific automated operation is available in different parts of a 4G network. Automated failure recovery, automated VPN setup, etc., are some examples of such automation. In many cases, such automation was achieved in an operator and/or vendor proprietary manner and are not standardized solutions. Besides, automated operations at different parts are not integrated in an E2E manner. As a result, operation of a complete 4G network, and the mobile cellular networks before that, requires manual intervention to fill out the gaps among the partially automated operations system mentioned before.

This ZSM scenario will support zero-touch full automation of the 5G network and service management.

6.2.3.1.2 Rationale and challenges

Instantiation, performing the Life Cycle Management (LCM), and termination of a nation-wide mobile cellular network is a formidable and costly task. A mobile cellular network is also mission-critical by nature, which requires significantly short operational response latency. Softwarization/virtualization of networks is a key technology to enable automated LCM operations, but at the same time, due to newer elements like hypervisor, guest OS, as well the decoupling of the software from the hardware and necessitating event correlation and analysis, it has made operation significantly more complex in terms of FCAPS management.

In order to enable the whole telecom ecosystem to reap the full benefit of 5G and network slicing, faster operational response, and reduction in operation cost (OPEX) are indispensable. Automation is already a well-recognized mean to achieve agility and cost efficiency.

Following key challenges need to be considered for this scenario (non-exhaustive lists):

- To define the appropriate closed feedback loop for LCM operation based on robust performance and fault monitoring as well as operator's policies for 5G network and its service network e.g. IMS, from end to end.
- To define the appropriate level of standardized interfaces as well as the reference architecture to enable fully automated operation with the management components provided by different vendors.
- To identify the gaps in and in-between the operation automation procedures and standards from relevant Standardization Organizations (SDOs), e.g. 3GPP SA5, TMF, MEF, ETSI ISG NFV, as well as open source solutions, and produce specification to fill them out.

6.2.3.1.3 ZSM scenario details

As a 5G network operator, he/she wants to perform the following items in fully automated manner in his/her 5G network, eliminating any human intervention:

- Instantiation of a complete 5G network that includes the RAN, mobile core, transport network, as well as the Data Network (DN) [i.6]. The 5G network may be logically separated and/or isolated for a certain aspect (e.g. service, user, etc.):
  - 5G network services may be incrementally deployed in the operator's network in logically separated and/or isolated manner from the other already deployed services.
  - 5G network services may be deployed and provided to other operators and/or service providers when requested, via open interfaces. This way, other operators and/or service providers can re-sell/extend the provided 5G network services.
- Fast LCM of the 5G network including corresponding DNs. This may be automatically triggered based on vendor-independent FCAPS management.
- Plug & Play of new components into a live 5G production network.
- Termination of one or more 5G network service(s), or 5G network as a whole.

NOTE: Deployment and removal of physical infrastructure is out of scope of this scenario.

To achieve the above, ZSM is expected, but not limited to:

- Fill out the gaps found in and in-between the operation automation procedures and standards from relevant SDOs, as well as open source solutions. When standards are found on operation automation for a particular part (e.g. NF, slice, transport network) of a 5G network, work should focus on specifying integration procedure of the available standards to achieve the full E2E automation of a complete 5G network. For the gaps, ZSM will provide standard specification to fill out the gaps.
- Operation system integration and inter-operability tests of the above-mentioned fully automated E2E operation system of a 5G network including DN, involving relevant solutions available from other SDOs, fora, and open source.

6.2.3.1.4 Related requirements for ZSM

To achieve a fully automated 5G network, the following requirements need to be met:

Req-1: ZSM framework shall support capabilities to perform FCAPS management automatically for compute, storage and network resources, NFs, slices and services for an automated operation.

Req-2: ZSM framework shall support automated LCM of a 5G network including Data Network (DN).

Req-3: ZSM framework shall support the capability of utilizing the benefits offered by cloud-native NF design and Software Defined Network (SDN) environments to realize fast operational response.

Req-4: ZSM framework shall support automated management of network slicing for the 5G network as a payload.

Req-5: ZSM framework shall support the exposure of management interfaces to third parties without any adverse effect on exposing network operator.

Req-6: ZSM framework shall support the capability of utilizing management interfaces exposed by third parties to realize an automated operation of the operator's own services built on the top of the provided networks.

6.2.3.2 Automated network bandwidth management

6.2.3.2.1 Description

Traditional methods for configuring network bandwidth resources are mainly based on human experience, which is cumbersome and error-prone. With a large amount of operation and maintenance workloads, in order to protect the important services, network administrators have to schedule network traffic at different special times, which requires rich experiences and meanwhile, will result in high operation and maintenance costs. Lack of experience may lead to network traffic failure. Besides, the bandwidth resource management lacks flexibility and the bandwidth resource could not be adjusted in real time according to the time, spatial and service characteristics of the traffic, such as for some tourist attractions, holidays or special events, the demand of bandwidth resources would be much higher than usual. Operators always provide the peak network capability to support all cases, which causes a large sum of resource waste.

With the development of new technologies such as NFV/SDN/5G, the network scale is rapidly expanding. Network topologies, hierarchies and services are more complicated. Users' demands for services are diversified. It is more difficult to maintain network bandwidth resources through manual operation planning.

This ZSM scenario is to support providing efficient and flexible ways to automate bandwidth resource bottleneck analysis and optimization.

6.2.3.2.2 Rationale and challenges

To analyze the network resource bandwidth automatically will not only greatly reduce the operator's OPEX, but also improve the efficiency of the network operation and maintenance and enhance the user experience by avoiding the possible traffic failure or congestion.

Following key challenges need to be considered:

- A traffic model of the entire network needs to be built through collection and analysis of the network traffic information and device bandwidth from different domains of an E2E network.
- The AI/ML and model-driven approach may need to be used to mine the network resource bottlenecks and calculate the optimal solution for bandwidth allocating base on the traffic model.
- The optimization strategy needs to be delivered to the specific domain of the E2E network and the related coordination mechanism should be provisioned.

6.2.3.2.3 ZSM scenario details

During the network operation and maintenance process, operators have much concerns on efficient management of the network bandwidth resources, for example, when the virtual machine is migrated in the data center, the locations of the virtual machines before and after the migration can be perceived, bandwidth should be adjusted synchronously; The needs of the bandwidth would be higher for the online service at night; The transport network could not adjust the bandwidth according to the dynamic service requirements in real time; The service quality of an E2E network is impacted for the lack of bandwidth in a certain domain.

The global view of the traffic in an E2E network would be much helpful for operators to notice the network bandwidth bottleneck and the expansion or optimization action can be triggered based on this information to avoid the potential traffic failure or congestion to reduce the service quality and user experience of an E2E network. The global view of the traffic can be established by collecting and analysing the traffic and bandwidth information from different domains of an E2E network and further form a traffic model of the E2E network, from which the time, space and/or service distribution of the traffic could be indicated clearly. The redundant bandwidth can be reduced, and the risk of insufficient bandwidth can be avoided as much as possible. Besides, it would be more beneficial if the growth of the future traffic can be predicated precisely, such as if the current network physical facilities could not meet the bandwidth requirements in the future, the risk that the traffic may exceed the threshold by a warning can be aware of in advance and the expansion decision can be determined accordingly.

6.2.3.2.4 Related requirements for ZSM

To realize the automated network traffic bandwidth management, the following requirements should be met:

Req-1: ZSM framework shall support the capability to expose the network utilization (such as CPU, memory, bandwidth, and data throughput) of managed resources for a given customer-facing service (CFS) and over a given time period. An example of where this information can be used is in a closed-loop automation where CFS-level network troubleshooting needs to be performed by ZSM framework.

Req-2: ZSM framework shall support the capability to locate the resources that are bottleneck(s) for a given E2E service.

Req-3: ZSM framework should support the capability to predict the growth or reduction of traffic volume for managed resources for a customer-facing service (CFS) and over a given time period. An example of where this information can be used is in a closed-loop automation where CFS-level network troubleshooting needs to be performed by ZSM framework.

Req-4: ZSM framework shall support the capability to optimize the routes of traffic for a given CFS to meet the service requirements.

6.2.3.3 ZSM automated healing

6.2.3.3.1 Description

In an automated network & service management environment, deviations from expected behaviours need to be detected and healed.

6.2.3.3.2 Rationale and challenges

In this scenario automated healing is defined as the ability to automatically recover from unexpected problems. Ideally problems are detected and healed before end users can take notice. Normally this task can be performed by the managed networks and services themselves. A managed network or service may fail to perform this task by internal errors or by unexpected side effects from other systems. Using a sliced network increases the risk. Healing actions themselves may have side effects to other managed networks and services. These have to be taken into account.

6.2.3.3.3 ZSM scenario details

In case of problems in a managed network or service, the service provided may not be able to meet the agreed SLAs. To avoid damage, it is critical to avoid such situations or to come back to normal operation as soon as possible. The managed network and services may have their own availability mechanisms. On the one hand it is important to ensure, that actions taken do not conflict with the mechanisms implemented in the managed networks and services. On the other hand, outages may have monetary effects and need to be avoided with high priority. An automated system needs to react fast, predictable and reliable at the same time. In addition, it has to be able to operate in an environment that consist of a mixture of legacy and state-of-the-art management systems and managed network and services.

6.2.3.3.4 Related requirements for ZSM

The following requirements are related to automated healing:

Req-1: ZSM framework shall support the capability to predictively detect abnormal behaviours of the managed networks and services.

Req-2: ZSM framework shall support the capability to automatically restore the managed networks and services to normal operation.

Req-3: ZSM framework shall have the capability to perform recovery actions based on the required KPIs of the managed networks and services.

Req-4: ZSM framework shall have the capability to interoperate with non-automated management systems.

6.2.3.4 Automatic E2E network and service topology management

6.2.3.4.1 Description

5G network faces growing complexity in cross-domain and changing environments. A key factor for an automated topology management is the ability to auto detects the environment in terms of type and location of the network elements and also their relationship, which will support the realization of E2E automatic network and service management.

6.2.3.4.2 Rationale and challenges

In most of the network management scenarios, user needs to make network and service topology clear first. For example, if alarms occur in some network elements, the relationship of network elements needs to be identified to find root cause. If certain network resources need to be modified, the network topology needs to be figured out to assess the influence to related resources.

Currently, in network management activities, human labour needed to make the relationships of related network and service elements clear sometimes more than it needed in deal with the core issues. There are some topology management functions, most of which limited in certain domains, and not dynamically refreshed. 5G network consists of elements from multiple domains (Wireless, Optical, IP, etc.) and different providers. Automatic E2E topology management is a key factor to realize E2E ZSM, such as automatic planning, fault location, modification, optimization, etc.

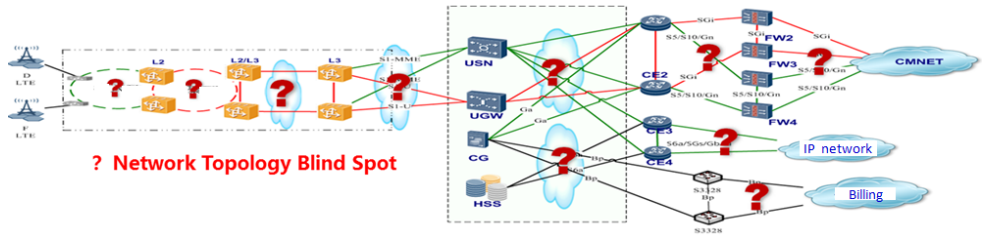

Figure 6.2.3.4.2-1: Example of a network topology

6.2.3.4.3 ZSM scenario details

A cloud network operator or provider wants to automate E2E topology management to be able to manage network in real time. This including followed aspects:

- Topology Generation:
  - Automatic retrieve network and service information and create topology after a network initiation or network elements changed.
  - Topology visualization in certain manners to support daily maintenance work.
- Passive management:
  - When errors occur, automatic troubleshooting functions need to locate fault elements based on topology.
  - When certain element needs to be modified (Remove, update, etc.), impact assessment on related network elements need to be performed base on topology.
- Active management:
  - Automatic topology compliance examination can help to find latent risk then fix it before service impact. Such as missing protection links, wrong connection of master and backup links, etc.

6.2.3.4.4 Related requirements for ZSM

To achieve automated topology management, following requirements need to be considered:

Req-1: ZSM framework shall support the capabilty to automatically display such as show or report on E2E service topology, including network functionalities and their relationships.

Req-2: ZSM framework shall support the capability to automatically display such as show or report on network topology across domains, including physical and logical links between physical and virtualized resources of a given managed network.

Req-3: ZSM framework shall have the capability to automatically update the topology information upon network or service changes.

6.2.3.5 Zero-touch E2E 5G network and service management as well as orchestration including edge computing

6.2.3.5.1 Description

The 5G networks and services as well as the management and orchestration of them need to cope with several challenges in the industry as well as in the public and private sector in the future.
In some cases, there is a strong need for ultra-low latency and ultra-reliable low latency communication, processing, and handling. This need will be also supported by edge computing. Therefore, the related management including orchestration parts have to be considered by the zero-touch network and service management reference architecture as well.

The providers and operators of the 5G networks and the corresponding services as well as applications have to manage and orchestrate these in an automated and flexible way E2E to the greatest possible extent. Sometimes the users/customers itself will be integrated in this process and have to cope with some management tasks as well.
This scenario will support the management including orchestration of edge computing in the context of the zero-touch E2E network and service management including orchestration via the identification and description of appropriate functionalities and interfaces.

6.2.3.5.2 Rationale and challenges

New and advanced topics such as remote robots, self driving cars, intelligent sensors, mIoT, Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR), mobile gaming, and the vertical industry as well as Industry 4.0, the private and public sectors e.g. for smart cities need in several cases the requested realization of the ultra-low latency and ultra-reliable low latency communication requirements. In addition to that, there is a stringent need to have a flexible zero-touch E2E network and service management including orchestration which can cope with these challenges.

Following key challenges have to be considered in this context, for example (non-exhaustive enumeration):

- E2E management and orchestration consideration of the 5G networks, services and applications.
- To find a good mix between the requested provision of the necessary networks, services and functionalities including interfaces and APIs and the necessary business revenue of the companies.
- To handle and to cope with the revolution aspects in the 5G environment.
- The necessary collection and coordination of the requirements from the Verticals, the industry 4.0, the private and public sectors, the operators, the service providers, etc.
- To have the appropriate zero-touch 5G E2E network and service management including orchestration reference architecture framework with their interfaces.
- To define and provide the requested flexible NW and service management as well as orchestration functionalities.
- To find mechanism and methods including architectures, interfaces, APIs and functionalities to converge several E2E network and service management as well as orchestration solutions and their operation.
- To find economically reasonable solutions for the realization of ultra-low latency and ultra-reliable low latency communication requirements and solutions in the context of networks, services and applications as well as their zero-touch E2E network and service management including orchestration.

6.2.3.5.3 ZSM scenario details

The zero-touch E2E network and service management including orchestration should handle automatically E2E network and customer service chains including their corresponding infrastructure as well as domains levels which need the usage of edge computing functionalities, components and mechanisms based on their requests.

There are functionalities, components and mechanisms which support the automated, flexible, dynamic, efficient and effective management including orchestration of the edge computing as part of an E2E chain on demand, Automated Lifecycle Management is one part of this construct.

That means the requirements about the management including orchestration can vary from time to time, e.g. several ultra-low latency and ultra-reliable low latency communication requirements could occur at specific times.

In addition, it could be that the edge computing functionalities should be moved and synchronized with one or several moving objects in order to fulfil the requirements for example concerning ultra-low latency and ultra-reliable low latency communication requirements. In that case, management functionalities could be needed as well.

Furthermore, a situation can appear where the edge computing parts are not needed longer or not needed for a certain time frame or will be reactivated again after that within the E2E chain. All these variants could be combined or provided and supported by Network Slices.

Zero-touch E2E network and service management including orchestration functionalities will be needed for these variants.

In order to achieve the targets of this scenario the following topics and aspects should be considered, for example:

- Coordination between the relevant SDOs, open source projects and initiatives for these topics.
- Coordination with the Verticals, the Industry 4.0, the other several relevant industries e.g. healthcare, energy and gaming, the private and public sectors, etc. concerning the requirements.
- Study and definition of the zero-touch 5G E2E network and service management as well as orchestration reference architecture framework including their interfaces which cover also edge computing.
- Definition of the requested flexible NW and service management including orchestration functionalities.

6.2.3.5.4 Related requirements for ZSM

This is a listing of related requirements (not a complete list):

Req-01: ZSM framework shall support the capability of E2E, automated management and orchestration of ultra-low latency communication services.

Req-02: ZSM framework shall support the capability of E2E, automated management and orchestration of ultra-reliable low latency communication services.

Req-03: ZSM framework shall support the capability of automated management and orchestration of edge computing.

Req-04: ZSM framework shall support the capability of zero-touch, E2E management and orchestration of 5G networks and services covering network slicing and edge computing.

6.2.3.6 Automatic software deployment

6.2.3.6.1 Description

Software deployment, including management applications (Orchestrator, VNFM, VIM, etc.) and network functions (including VNF and PNF, etc.), is the fundamental and basic step to build a network (5G, NFV, SDN, etc.). Until now, it needs a great deal of human intervention in the process of software deployment because of the heterogeneous private operation means and complicated dependency relationships. Standard in appropriate level needs to be specified to reduce, even eliminate human work and realize zero-touch in software deployment.

6.2.3.6.2 Rationale and challenges

Cloud network deployment has already been started and in the near future a booming growth can be foreseen. Fast and automatic deployment will be the first challenge to make the network and service online in ideal time period and cost:

- There is standard concerning network functions deployment, but some environment related parameters still need to be configured manually. It is still needed to be enhanced to realize zero-touch for Software and OS image installation, configuration and verification of network functions.

- There are complicated relationships of the components inside the management function entities, which also have strict dependence and sequence in the deployment process. It is hard for the users to figure them out and often result in time-consuming and error prone in the process.

6.2.3.6.3 ZSM scenario details

After the pre-condition works ready, as a cloud network operator or provider/integrator, he/she wants to perform the software deployment activities in fully automated manner.

Pre-conditions:

- The infrastructure hardware has been ready and power on.
- The software package, OS images, planning data are ready in specific location or directory.
- The hardware can be connected by a deployment platform or tool.

Activities:

- Management applications deployment:
  - Pre-verification: Perform basic check of management application deployment conditions to ensure successful deployment. The check may include network connectivity, software availability, hardware configuration, etc.
  - Automatic perform software installation, data configuration of the management applications.
  - Verification: Perform basic management application function test to ensure the applications are deployed successfully and running normally.
- Network functions deployment:
  - Pre-verification: Perform basic test of network functions to make sure the network function is in normal state. Check infrastructure layer condition to ensure it meets the needs of network functions which will be deployed.
  - Automatically perform physical and virtualized network functions deployment.
  - Verification: Automatically perform basic function test after deployment to ensure the network function running in normal state.

6.2.3.6.4 Related requirements for ZSM

To achieve fully automated software deployment of cloud network, the following requirements need to be considered:

Req-1: ZSM framework shall support the capability of automatic pre-verification to ensure the management software deployment condition is met.

Req-2: ZSM framework shall support the capability of automatic installation of management software.

Req-3: ZSM framework shall support the capability of automatic configuration of management software parameters.

Req-4: ZSM framework shall support the capability to automatically verify the management software status after deployment.

Req-5: ZSM framework shall support the capability of automatic pre-verification of network functions normality and infrastructure conditions before deployment.

Req-6: ZSM framework shall support the capability to automatically install physical and virtualized network functions software.

Req-7: ZSM framework shall support automatic configuration of physical and virtualized network function parameters.

Req-8: ZSM framework shall support the capability of automatic verification of physical and virtualized network functions normality after deployment.

6.2.3.7 Automatic software upgrade

6.2.3.7.1 Description

The software in management applications (Orchestrator, VNFM, VIM, etc.) and network functions (including VNF or software in PNF) may need to be upgraded occasionally for network ability enhancement, evolution or fixing issues. Automatic software upgrade will be essential to guarantee service continuity and efficiency.

6.2.3.7.2 Rationale and challenges

Software upgrade is sometimes a high-risk work which brings pressure to users if so much work needs to be performed manually. The challenges include:

- There often be on-gonging service running on the software which needs to be upgrade, and unexpected service impaction (such as service interruption, service quality decline, etc) will happen if mistake or so much time spends on upgrading process.
- If issues happen in upgrade progress which can not be fixed in acceptable time, it will be hard for the technicians to fallback the software to original versions and normal status, which will lead to more serious service impact.

6.2.3.7.3 ZSM scenario details

After the pre-condition works ready, as a cloud network operator or provider/integrator, he/she wants to perform the software upgrading activities in fully automated manner.

Pre-conditions:

- Software and associated data are ready.

Activities:

- Pre-verification needs to be performed to ensure the upgrade objects is normal, the network condition is meet.
- Perform software upgrading process automatically.
- Perform verification automatically, including basic functions and compatibility after upgrade process.

6.2.3.7.4 Related requirements for ZSM

To achieve fully automated software upgrade, the following requirements need to be considered:

Req-1: ZSM framework shall support automatic network function SW upgrade within a production environment, at least to the latest released version.

Req-2: ZSM framework shall support automatic upgrade of management services within a production environment, at least to the latest released version.

Req-3: ZSM framework shall support automatic verification before SW upgrade to ensure the upgrade conditions are meet.

Req-4: ZSM framework shall support automatic verification after SW upgrade to ensure success of upgrading.

Req-5: ZSM framework shall support automatic rollback to the previous SW version if rollback condition is met during or after upgrade process.

Req-6: ZSM framework should support the capability to perform in-service SW upgrading of management services.

Req-7: ZSM framework should support the capability to perform in-service SW upgrading of network functions.

6.2.3.8 Automation using policies

6.2.3.8.1 Description

In many cases, actions for automated execution can be described using policies. Many network deployments already now provide policy management that can drive automatic changes in life cycle management and other network configurations. It makes sense that ZSM framework use these mechanisms to control automation.

Policies as a means of automation are described in ETSI GR ZSM 005 [i.1].

Policy framework is also a part of NFV, see some details in ETSI GR NFV-IFA 023 [i.2].

6.2.3.8.2 Rationale and challenges

Using policy management, the trigger to execute measures of automation is moved more closely to the network, improving the speed of reaction and decoupling the OSS/BSS decisions from the fast execution in the network.

In most cases, policy driven automation will be used in combination with other means of automation.

The key idea with imperative type of policies is to create pre-defined rules that trigger automatic actions when certain situations occur.

The managing entity (e.g. ZSM framework) would inject policies for the managed entity (e.g. a network function). The managed entity would execute these pre-defined actions autonomously and notify the managing entity afterwards about changes.

In order to achieve policy driven automation, a number of issues need to be solved:

- Language for the policy.
- Management of policies.
- Security issues at the time of creation and management of the policies.
- Security issues at the time of execution.
- Mapping to administrative roles and domains.

6.2.3.8.3 ZSM scenario details

Policy based automation usually can be described as the following functionality:

- Policy definition:
  - The intended automatic behaviour is described in a language, the system (e.g. ZSM framework) can understand.
- Policy repository:
  - The policies are stored and can be activated, deactivated, deleted, etc.
- Detection of conditions:
  - The system (e.g. ZSM framework) needs to detect when a condition defined in a policy is fulfilled.
- Policy decision:
  - There might be additional things to consider in order to decide on the execution of the actions described in the policy.

- Policy execution:
  - The policy function would trigger the execution of the predefined actions

NOTE: The description of these steps or functionalities does not mean it needs to be separate functional components.

For the scenario it is helpful to distinguish the abstract roles of a Policy Administration Point (PAP) and a Policy Function (PF) as in NFV [i.2].

The PAP is responsible for defining policies according to the user (service provider) needs. In many cases the PAP will define the policies in an independent language to be able to inject the policies to a PF provided by a different party.

The PF is responsible to store the policies, discover policy conditions, decide and trigger the execution of the predefined actions.

Depending on the capability of the managed entities, these roles can be mapped differently:

- Option 1:
  - In case the managed entity provides a policy function, the ZSM frame work can act as PAP only. It will translate the service provider needs into a common policy language and inject the policy into to managed entity.
- Option 2:
  - The ZSM framework can also act as PAP and PF together. This is necessary in case a managed entity does not provide the capability of a PF, but can also be applied when it does.
  - In this case, the ZSM framework will not only translate the service provider needs into policies (common language is not necessary here), but also manage the policies, discover policy conditions and trigger the execution of the predefined actions.

In both cases, the ZSM framework is responsible to make sure there are no conflicts in the set of policies.

6.2.3.8.4 Related requirements for ZSM

The followings are the requirements extracted from the above scenario:

Req-1: ZSM framework shall support the capability to specify policies.

Req-2: ZSM framework shall support the capability to define the policies in a technology independent policy definition language.

NOTE: Further characteristics are beyond of the scope of the present document.

Req-3: ZSM framework shall support the capability to at least store, delete, activate and deactivate policies.

Req-4: ZSM framework shall support the capability to make use of the policy capabilities of the entities it manages.

Req-5: ZSM framework shall support the capability to manage the defined policies.

Req-6: ZSM framework shall support the capability to detect policy conditions.

Req-7: ZSM framework shall have the capability to decide on policy execution.

Req-8: ZSM framework shall support the capability to trigger the actions defined in the policies.

Req-9: ZSM framework shall have the capability to detect conflicting policies.

6.2.3.9 Closed loop automation

6.2.3.9.1 Description

This scenario describes how closed loops can be used in ZSM framework to enable management system to adapt the behaviour of the network and service to respond changes in user experience, business goals or environmental conditions.

The terminology of closed loop (observe, orient, decide, act) in this scenario is consistent with the architecture principles "Closed loop management automation" defined in ETSI GS ZSM 002 [1].

6.2.3.9.2 Rationale and challenges

Closed loops provide a generic mechanism for self-adaption. Closed loops operate to continuously observe and collect data about the set of managed entities, as well as the context that are operating. This enables the ZSM framework to understand the changes in the behaviour of the network and service being managed, analyse the changes, and provide actions to move the state of the managed entities toward a common goal.

6.2.3.9.3 ZSM scenario details

In the ZSM framework, closed loops can be used in different levels, inside a domain and cross-domain. In the closed loop inside a domain, only issues related to resources inside that domain can be solved. Cross-domain closed loops can solve issues related to resource in different domains. In this case, cross-domain closed loops may collaborate with closed loops inside domains. So, the closed loops may be nested.

Usually, closed loops include the following steps:

Observe:

Closed loops begin with input data. Without the proper input data, the closed loop will be inefficient at best, and likely useless. However, many data in their raw form are not easy to understand, and may not be compatible with other data. Hence, this stage is mostly a passive ability to collect data that is meaningful for the management process, and relies heavily on the next step.

Orient:

Two steps in the orientation:

Firstly, the normalization of the collected data to a common form contributes to the overall perception of the network and service. This step can be done by a model-based translation of received data. Without this step, the risk of the wrong decision being made is increased.

Then, analysis of data is critical for enabling the closed loop, which determines the critical properties that the closed loop is operating against. For example, the analysis might derive the current state of network and service, that can then be compared to the desired state to define an error function that can fed back to the closed loop. Another example, one or more attributes could be monitored to determine whether the system is operating as planned or not. Machine learning algorithms can be used to make the closed loop more adaptive.

Decide:

Once the analysis is done, ZSM framework understands whether its current behaviour needs to be modified or not. The closed loop should be able to generate one or more actions to govern the behaviour of the network and service. If multiple actions are to be executed, the closed loops shall define the order of the execution of the execution of the closed loops.

Act:

The ZSM framework executes the actions to adjust the behaviours of the managed network and service in sequence.

Typically, policies help in making decision, or they provide actions as part of the closed loops. ZSM framework shall detect and resolve conflicts.

Closed loops can help ZSM framework to different levels of automation. Firstly, automation may be implemented by step-by-step execution of rules without human intervention. Closed loops may rely on humans to defining the sequence of rules and may need manual adjustments if the environment changes. ZSM framework can be evolved to be autonomic. In an autonomic environment, closed loops can adapt on their own to a changing environment.

6.2.3.9.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to allow different sets of collected data to be used in different closed loops inside a domain and cross-domain.

Req-2: ZSM framework shall support the capability to normalize data that are not in common format, so that their meaning and significance can be understood in the proper context.

Req-3: ZSM framework shall support the capability to analyse the collected data to detect the undesired states and derive the root cause. The past, current and future states of the managed entities can be modelled to help to detect the undesired states and move the state of managed entities to the desired state.

Req-4: ZSM framework shall support the capability to decide which actions and when to execute, and then execute the actions based on the analytics results.

Req-5: ZSM framework shall support the capability to detect and resolve any conflict between different closed loops inside a domain and in different domains.

Req-6: ZSM framework shall support the capability of nested closed loops.

6.2.3.10 Full automation of VNF provisioning

6.2.3.10.1 Description

To deal with the increase of network traffic and various types of network slice in 5G environment, it is necessary for operator to provide the flexible VNF provisioning to satisfy the demand of short time-to-market and cost reduction.

In the present document, the automation of VNF provisioning from planning to deployment, testing process based on ZSM framework to reduce time and cost is proposed.

6.2.3.10.2 Rationale and challenges

In this scenario, realizing the automation of processes for equipment planning, designing, testing and deployment in VNF provisioning with short time-to-market becomes a big challenge, and the following tasks should be carried out:

1) Automatic coordination of data between the processes above without human intervention.

2) Making the future demand forecast and equipment planning automatically according to network usage condition and VNF configuration history.

3) Implementing VNF flexible scaling according to the network usage condition.

4) Rapid activation of deployed VNF in commercial network.

5) Carrying out the rapid provisioning which is vendor independent.

6.2.3.10.3 ZSM scenario details

The following scenario which eliminates any human intervention is needed:

1) Automatic design, on-boarding and commission of VNF configuration. Automatic VNF testing and information collection of VNF status and resource usage.

2) Automatically making demand forecast and equipment planning.

3) Automatic activation of additional VNF (e.g. DNS register).

4) Return to the normal state before the data input if failure occurs during the automatic designing process or application of VNF configuration.

5) Implement demand forecast according to the usage of deployed VNF and feedback the results from demand forecast to planning process in VNF provisioning.

6.2.3.10.4 Related requirements for ZSM

To achieve the full automation of VNF provisioning, the followings are the requirements extracted from the above scenario:

Req-1: ZSM framework shall support standardized interface(s) for VNF provisioning to realize E2E network service.

Req-2: ZSM framework shall support fully automated flow of data which are used in each process.

NOTE: Processes here refer to but not limited to equipment planning, designing, testing and deployment process.

Req-3: ZSM framework shall support the capability of demand forecast for capacity planning.

6.2.3.11 Automated detection of services offered by management domains

6.2.3.11.1 Description

The changes in the services exposed by a management domain have to be automatically discovered by the other management domains in the ZSM framework which are authorized to see them. For example: an operator may choose to add a new management domain, upgrade or delete an existing one.

6.2.3.11.2 Rationale and challenges

This scenario brings automation to the detection of services of other management domains, where, given the initial legal agreements are in place, a management domain can automatically detect the changes in services of other management domains.

For realizing complete automation of such services there are a number of challenges to consider:

1) The discovery of services should include the phase where a new management domain is added, upgraded or removed.

2) How can a management domain and its services be identified/registered in an automated way?

3) What are the suitable architectures for the discovery of services?

4) Where should the management domain discovery service be located?

6.2.3.11.3 ZSM scenario details

An operator may add a new management domain, upgrade or remove an existing management domain. The update of the management domain should be informed to other management domains.

In case the management domain is deleted, the services offered by the management domain should be removed from the ZSM framework.

The service changes have to be informed to the consumers authorized to view those services.

6.2.3.11.4 Related requirements for ZSM

The following requirements need to be fulfilled by the ZSM framework to enable the described scenario:

Req-1: ZSM framework shall enable automated detection of management services offered by a management domain.

Req-2: ZSM framework shall enable automated detection of changes in management services offered by a management domain.

Req-3: ZSM framework shall enable automated detection of management service termination.

6.2.3.12 Service management by 3GPP management system and ETSI NFV MANO

6.2.3.12.1 Description

To achieve the successful operation and maintenance in the virtualized environment, it is important to efficiently manage infrastructure resources and network functions (including applications). ETSI ISG NFV has standardized how network services and virtualized infrastructure resources are managed while 3GPP SA5 has standardized how 3GPP services and network functions (both virtualized and non-virtualized) are managed.

6.2.3.12.2 Rationale and challenges

In a network environment in which virtualized and non-virtualized functions coexist, they have to be comprehensively managed together to provide services. In that case (see figure 6.2.3.12.2-1), network services and corresponding virtualized resources such as NFVI and VNF can be considered to be managed by a MANO system (NFVO, VNFM and VIM). While, a 3GPP Management System (SBMA and MnS Producers) is also necessary to make the network services available.

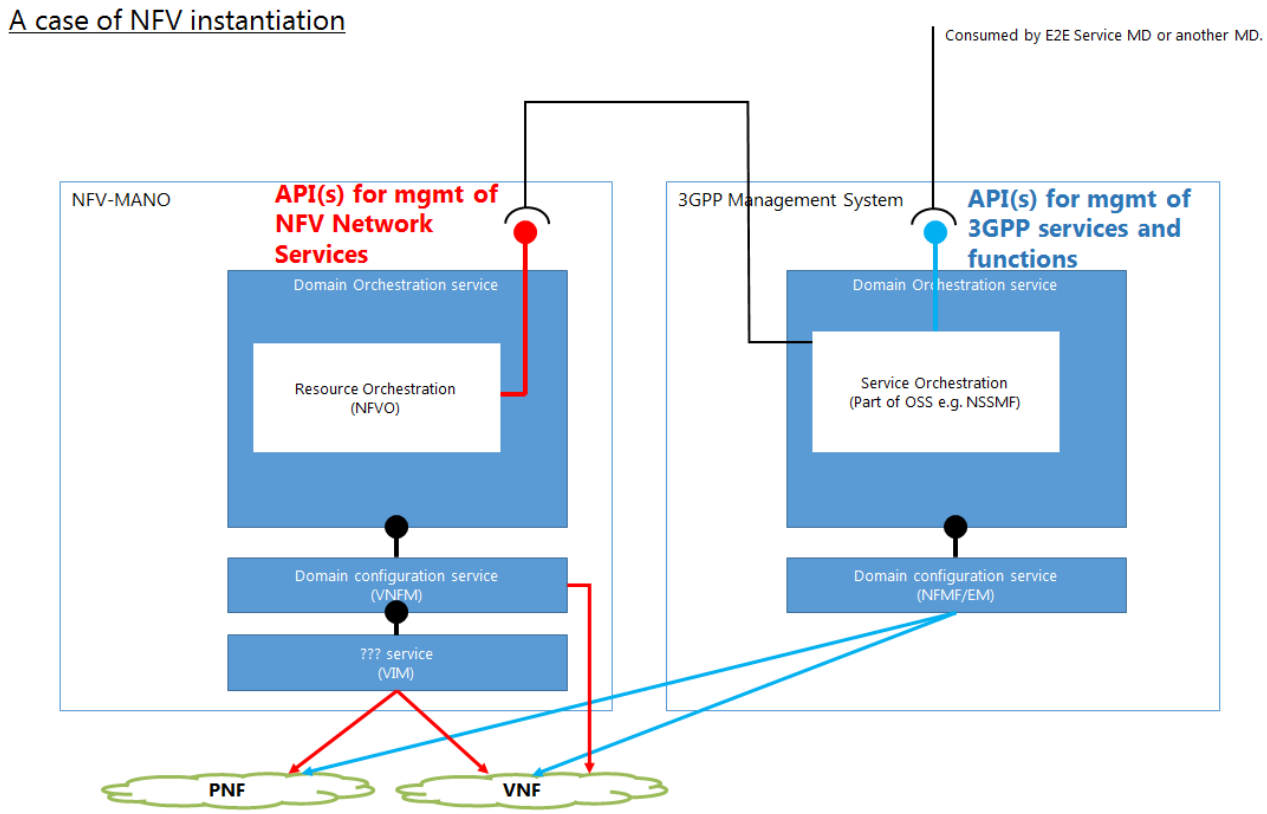

Figure 6.2.3.12.2-1: Example of management by different level of service

6.2.3.12.3 ZSM Scenario details

The following scenario is an example expected when creating a new network service based on the concept of ETSI NFV MANO in an automated manner.

[3GPP Management System]:

1) A 3GPP Management System requests NFVO (NFV Orchestrator) to prepare virtual resources (compute, storage and network) in order to create a new network service.

2) When the process of the instantiation by NFVO completed, the 3GPP Management System installs and/or configures corresponding applications and specific parameters of each VNF on the resources and activates them.

[NFV MANO]:

1) After the preparation of VNF instance(s) is requested by a 3GPP Management System, the availability of virtual resources is confirmed and the resources are reserved.

2) When needed, NFVO instantiates new VNF instance(s).

3) After the resources are instantiated or reserved, NFVO sets configuration data into the resources and activate them.

6.2.3.12.4 Related requirements for ZSM

Req-1: ZSM framework shall support the interoperation with APIs (MANO) for management of NFV network services.

Req-2: ZSM framework shall support the interoperation with APIs (3GPP SBMA) for management of 3GPP services and functions.

6.3 Network as a service

6.3.1 NaaS lifecycle and exposure with a network slicing scenario

6.3.1.1 Description

The present document proposes that resources being managed by network and service management platforms from any domain (e.g. Transport, IP, access, media, etc.) should expose service capabilities (i.e. Network as a Service) in the ZSM framework to allow for zero touch automation. This proposal would also have the least impact on the existing and future management system (e.g. OSS/BSS), and enable simple transition from each domain.

6.3.1.2 Rationale and challenges

6.3.1.2.1 CSP challenges and requirements

Today Communication Service Providers (CSPs) have a plethora of BSS and OSS by organizations (e.g. consumer, enterprise, wholesale, etc.), by suppliers, by technologies (e.g. wireless, transport, media, IP), etc. The cost to maintain these systems are exorbitant leaving less budget for innovation. Each network resource is so entrenched in these systems that products , services or resources cannot be exited for fear of breaking something. With the advances of virtualization, SDN, cloud and AI, the management (service and network level) platforms of the above mentioned domains are also becoming more autonomous and need to rely less on current OSS/BSS systems.

The challenges that CSPs face are:

- Every product sold and modified requires a large, lengthy and expensive integration project. Discussions centre on every resource that needs managing for every domain in support of every product and offer.
- Tight point to point coupling between resources (physical and virtual) and management platforms (e.g. OSS/BSS) cause increase time to market (for project and testing) and exorbitant costs for any addition/modification/exit of resource, service, supplier, etc.
- Lack of automation across domains (i.e. an IP VPN service requesting a specific transport layer service with QoS is done manually) inhibits the scalability required for massive service delivery (e.g. IoT).
- Existing E2E Service management would be in support of multi-vendors within one domain and not an E2E service level across multiple domains.
- Similarly, there are no E2E service management across virtualized and physical network resources from different domains (i.e. a 5G Next Generation Core slice dealing with LTE physical BBU - option 4a RAN).

- While network domains are becoming more virtualized and agile, customer products are still created with a "what resource need configuring" approach and operations are still using open-loops vs closed-loops.

The Telecom industry requires a rethink in its network domains to management architecture to obtain the level of agility, costs and time to market expected by customers.

6.3.1.2.2 ZSM challenges

ETSI ZSM challenge is to provide requirements or functional framework architecture to the industry that focuses on zero-touch automation while complementing the work that other SDO or Open-Source groups are leading avoiding overlaps.

6.3.1.3 ZSM scenario details

Taking as an example a Network Slice scenario, one could derive what each domain could/should expose (at a minimum) to understand what E2E automation could be derived in support of the ZSM framework architecture design.

Figure 6.3.1.3-1 shows the number of domains that are used in delivering a network slice.

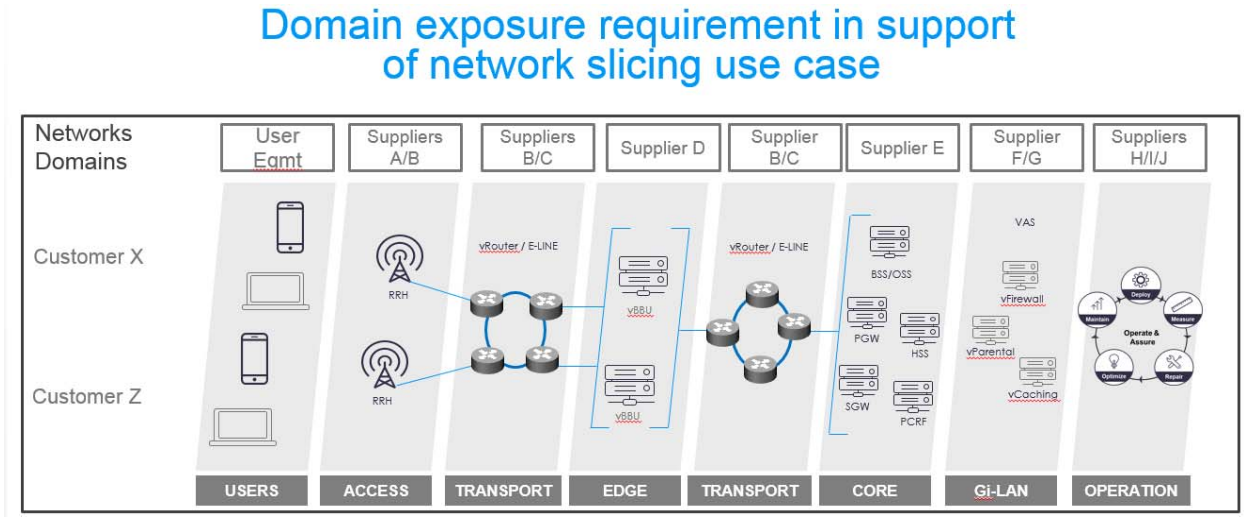

Figure 6.3.1.3-1: Example of domains that are used in delivering a network slice

Taking 2 slice scenarios with different QoS level offered, what are the services (i.e. Network as a Service) that should be exposed from each domain in support of each slice and how can these be managed in a zero-touch and automated fashion.

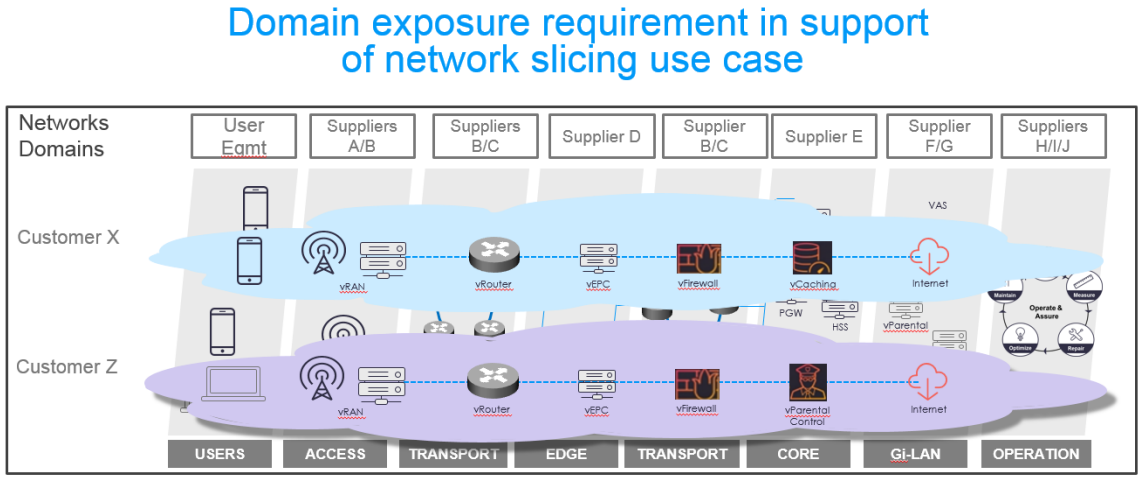

Figure 6.3.1.3-2: Domain exposure possibilities that are used in delivering a network slice

Each domain specific management system needs to expose its capabilities via a suite of unified interfaces (e.g. Config & Activation, Service Catalogue, Service inventory, etc.) in order to achieve a zero-touch" level of automation on upper level realized currently by legacy systems.

This concept requires alignment from suppliers of all domains (e.g. "transport suppliers, core suppliers, access suppliers, etc.") such that they expose their services/capabilities in a uniform way.

6.3.1.4 Related requirements for ZSM

ZSM framework enables operators to create or modify E2E services (or customer products), re-using services (NaaS) exposed by domains in a Zero-touch automated fashion. The following requirements are derived from the scenario above:

Req-1: ZSM framework shall support interworking with legacy management systems.

Req-2: ZSM framework shall support monitoring of managed services (network as a service including network slicing as a service) originating from different network/infrastructure domains including but not limited to NFVI, IP/SDN networks, Front haul, and Radio.

Req-3: ZSM framework shall support reconfiguration of any domain NaaS as required, e.g. in support of closed-loop assurance.

Req-4: The ZSM framework shall support managing the complete lifecycle of the network services/capabilities exposed per management domain, and shall provide an interface that hides internal details (such as the resource layer).

Req-5: ZSM framework shall support security capabilities when delivering automated network and service management.

6.4 Analytics & machine learning

6.4.1 Access to up-to-date telemetry data

6.4.1.1 Description

Telemetry data inform the management system about the performance and health of the network and the services. The functionality for automated/autonomous network management provided by the ZSM framework is data-driven and therefore needs access to telemetry data to perform its tasks. Assuming, that such functionality can be distributed, common access to up-to-date telemetry data is a prerequisite for building a zero-touch network and service management system.

NOTE: This scenario only deals with telemetry data that are part of the data typically processed in network management. It does not apply to data that are created by the network functions themselves as part of their operation (e.g. call session control data) but does apply to management data related to applications (such as application KPIs).

6.4.1.2 Rationale and challenges

Traditionally, telemetry data are collected and consumed by pre-defined network management components. Typically, these provide access to those data for external components only in the shape of aggregated information. Such approach is termed as "data silos" and is a hindrance for automation and distribution of the management tasks, and for the introduction of novel mechanisms for analytics, network and service intelligence.

To enable automated decision making based on knowledge about the state of the network, it is important that telemetry data can be accessed by all parts of the ZSM framework that need such information. A useful referential to categorize the requirements relating to the data being collected is the so-called three 'V's of data: Velocity, Volume and Variety which describes three defining properties or dimensions of data. Also, the data need to be up-to-date, where "up to date" is used as a general term related to different criteria such as "freshness", "real time", "streaming" and "notifications", which are further described below.

"Freshness" means that data were captured at a point in time close to time instant when they are consumed. For different data, different freshness criteria apply. "Real time" is the highest degree of freshness, denoting the fact that data are captured at high frequency and provided with low delay to the consumers. "Data streaming" is a technique to provide a series of data samples as a sequence ("stream") to (typically) multiple consumers. Data streaming can be capable of supporting real time, but can also consider lower degrees of freshness. "Notifications" are another technique of ensuring a high degree of freshness of the information without the need to stream the actual data samples. Notifications are emitted by a data collecting entity only if certain conditions are met by the measured data (e.g. a threshold has been crossed or an error has occurred).

In general, Notifications and Data streaming constitute new "push" approaches of telemetry data delivery, that deliver data continuously, compared to the traditional "pull" or "collect" paradigm which deliver the data at discrete intervals.

Telemetry data can potentially constitute a large data volume. Preprocessing and filtering allow to limit the data volume to the data of interest, and cross-domain data aggregation can distill higher-order data from lower-level domain-specific data. Filtering can be applied at the source or the destination of the data, or in intermediate entities.

Last but not least, common access to data always requires a data governance scheme to be put in place, to enforce that only authorized consumers can access the data. This includes aspects of ownership of the data, but also of common interest.

6.4.1.3 ZSM scenario details

The telemetry data that is required for the automated network management includes (not limited to):

- Performance counters that contain detail information about the performance of network resources and service at a particular point in time.
- Key performance indicators (KPIs) that are computed from performance counters to provide more abstract, aggregate information of performance.
- Fault information (alarms) that represents about abnormal conditions (faults) in the system.
- Logs, traces and other possible events generated by a system provide additional information about state changes of the managed system that may be relevant for the ZSM framework.

NOTE 1: The inclusion of other data (e.g. configuration data, repository data) is needed to make this list complete.

Such information is provided at the applicable level of freshness, and using different techniques such as streaming or notification.

Also, data can originate from one network or service domain and can be consumed in another. Cross-domain data access can involve data aggregation to abstract domain or resource details. Care needs to be taken that cross-domain data access does not inhibit the autonomy of the involved domains.

Mechanisms are required that collect the above information at the appropriate level of freshness, to store the information if required, and to provide access to that information to all interested entities in the system while enforcing data governance.

NOTE 2: Generic technologies such as SNMP or Syslog that collect raw data, apply first level processing to these data and provide access to the processed data are not considered data silos, but need to be incorporated into the necessary mechanisms described above.

6.4.1.4 Related requirements for ZSM

The following requirements need to be fulfilled by the ZSM framework to enable the described scenario:

Req-1: ZSM framework shall support the capability to collect up-to-date telemetry data (such as performance data, KPIs, and alarms).

Req-2: ZSM framework shall support the capability of common access to the collected up-to-date telemetry data, both inside a domain and cross-domain.

Req-3: ZSM framework shall support the capability of enforcing a data governance scheme for the common access to telemetry data.

Req-4: ZSM framework shall support the capability to store telemetry data (or to steer their appropriate storage).

Req-5: ZSM framework shall support the capability to (pre-)process and filter the telemetry data, and to perform cross-domain data aggregation.

NOTE: Filtering can be applied at the source or the destination of the data, or in intermediate entities.

Req-6: ZSM framework shall support the capability to check/validate the integrity of telemetry data, in particular in case of distributed data stores/replication.

Req-7: ZSM framework shall support the capability to manage the distribution of telemetry data, and keep distributed data consistent.

Req-8: ZSM framework shall support the capability to provide telemetry data to the data consumer according to the data consumer's requirements concerning but not limited to relevant data, relevant time, relevant form.

6.4.2 Machine learning for network & service automation

6.4.2.1 Description

Machine Learning encompasses different algorithms that can "learn" from data and improve the ability of executing a specific task. The learning process involves very little or no human intervention and has shown good performance in solving different computational tasks that mainly improve algorithmic ways of recognizing patterns in data (e.g. handwriting, voice and patterns recognition, anomaly detection, inference/prediction from data, etc.). The self-learning nature of these algorithms, together with the intensive use of data, makes them powerful tools that can leverage the zero-touch automation of telecommunications services and networks.

It is important to recall from ZSM ISG White Paper that machine learning is one of the tools/methods to be considered to "achieve the target of full automation". As such, requirements to support machine learning algorithms need to be addressed by the ZSM framework.

6.4.2.2 Rationale and challenges

Machine learning is a subfield of artificial intelligence that aims at developing algorithms that can reason on data and make decisions. The overall process of machine learning algorithms consists of:

i) receiving input data;

ii) learning from that data and creating models to solve a specific task; and

iii) applying the model to decide the outcome when new data is received.

These algorithms are employed mainly in problems that are too hard or infeasible to be modeled and solved by traditional (non-statistical) algorithms, such as pattern recognitions, anomaly detection, computer vision, etc. ML algorithms are broadly classified into three categories:

i) supervised learning, where the learning process is done based on labeled datasets;

ii) unsupervised learning, where data input is not labeled; and

iii) reinforcement learning, where the learning process maximizes a reward function based on a closed-loop structure.

As such, ML algorithms are heuristics that do not guarantee optimal solutions, but can be applied to solve specific problems where it has been proved to obtain good results. Each of the three categories pointed above are best at solving different kinds of problems. Also, there are many algorithms that can be classified as ML-based; each of them with different learning processes, computational complexity, and data requirements. Despite the various specificities of each algorithms, usually ML can be seen as a "black-box" that will receive input data and provide output decisions, whether it is a classification, clustering, or a function maximization problem. Furthermore, there are currently projects, e.g. Acumos AI and Algorithmia, that provide many ready-to-use ML-based algorithms that have been implemented and tested. Such platforms provide ML-as-a-Service (MLaaS) and can be easily integrated into larger systems to support decision making and/or optimization on different fields.

ML-based algorithms are already used to solve specific problems in telecommunication networks, e.g. customer service, predictive maintenance, fraud detection, network churn reduction, etc. With the fast growth of ML, more complex tasks that are related to the process of network and services automation should also be tackled by this type of algorithms. One needs to consider how to better support the use and integration of ML algorithms for enabling zero-touch automation within the ZSM framework.

The use of ML-based algorithms in network and services automation requires that many challenges be tackled, especially due to the criticality of the processes and different actors involved in the business. One critical problem faced is how to explain mathematically and/or intuitively the decisions taken by ML algorithms. Especially for operators since they will have their operations driven by the decisions taken by these algorithms. In network automation, there may be a need to have analogies/comparison between decisions taken by ML algorithms and the ones taken by humans. This can be easily done by algorithms such as decision trees, but impossible for others, such as neural networks.

The details of the algorithms are hard to be understood by subject matter experts, who will likely be the ones in charge of testing and deploying these algorithms. There is a clear necessity of translating statistical metrics into network KPIs that can be more easily understood by operators and users and can be used to compare ML with other types of algorithms.

The training phase is very critical and time-consuming, usually requiring human intervention and ML specialists to decide upon the best models to be used. Even after operation starts, the performance of ML models tends to suffer degradation over time and need to be retrained periodically. This creates the necessity of ways for monitoring the performance of the algorithms, possibly with human supervision, both in the training and the operation phases. Evaluating the performance of the ML algorithms and comparing with legacy (non-statistical) algorithms is essential for gaining trust from the stakeholders. This may be a big challenge for the adoption of ML algorithms as many of them require large amount of data and some time to start to get good results. Hence, operators will need to trust and provide data before they see the best results coming out of ML algorithms. The adoption may occur in phases, and probably both ML-based and legacy algorithms may run in parallel for some time to guarantee continuity of service.

6.4.2.3 ZSM scenario details

One way of packaging ML features into a system is through microservices-based approach.

In microservices-based approach, the training can be split from the optimization/operation. Both can work independently in virtualized/containerized environment. The training service may access the dataset repositories through REST interface, where historical data, alarms, logs and other useful data is stored. The result from training service are exported to model repositories, where "knowledge" from past experiences is stored. The optimization/operation services access the model repositories through REST interfaces and apply the retrieved models to current data. Eventually new up-to-date (labeled) data can be fed back into the dataset repositories as result out optimization/operation service outcomes.

Splitting training and operation as microservices easies the combination of different third-party platforms (e.g. Acumus AI, Algorithmia) and integration with other software. Decoupling data science from operations also facilitates comparisons of different ML-based and non-statistical algorithms, and enables incremental adoption of ML.

6.4.2.4 Related requirements for ZSM

Req-1: ZSM framework shall support the management of composite services.

Req-2: ZSM framework shall support interfaces that facilitate the integration of Machine Learning-as-a-Service frameworks into a zero-touch automation environment.

Req-3: ZSM framework shall allow for ways of measuring KPIs.

NOTE: The exact types of KPIs and their evolution could be considered in the next version of the present document.

Req-4: ZSM framework should support stepwise introduction of ML based management, allowing a mixed environment of traditional and ML algorithms while the maturity of and confidence in ML assets increase.

6.4.3 Predictive analytics

6.4.3.1 Description

In the automated network and service management environment, it is better to prevent the problem before it occur. Ideally, problems can be detected and solved before it impacts the end users. Passive processing should be evolved to proactive prevention via identifying predictions and key network issues.

6.4.3.2 Rationale and challenges

In the traditional network and service management, the network reports the problem and network management system solves the problem artificially, which takes long time to recover the service.

In 5G network, large amount of real time and high-reliable services are introduced. The increasing network complexity will bring large numbers of problems, which will give large challenges to the network management system, even though some problems can be solved automatically.

Most of the operations are troubleshooting, rather than preventing it before failure occurs. In this scenario, the Key Performance Indicators (KPI) can be predicted, and the problem can be prevented

6.4.3.3 ZSM scenario details

Prediction means to know what will happen next. In the process of data analysis, KPI prediction of future time based on existing data is often used to deal with possible risks and failures in advance. For example, using the prediction of resource capability, the network can be scaled out in advance to avoid network congestion, which can improve the user experience.

The prediction can be used in the following aspects:

- Prediction of resource usage to avoid congestion.
- Prediction of service KPIs to optimize service.
- Prediction of service health state to ensure reliability.
- Others.

Artificial intelligence and policy models may be utilized in the prediction of network conditions. In the process of KPI prediction, the existing history data and experience will be used to predict the trace of KPIs, e.g. by detecting changes of patterns in history. Other related data, like the topology, and the relying infrastructure data can also be used in the KPI prediction.

6.4.3.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to store historical data that is needed for the prediction and make it accessible to the analytics.

Req-2: ZSM framework shall support the capability to introduce data analytics for predicting KPI changes and failure conditions.

6.4.4 Real time monitoring and analysis

6.4.4.1 Description

In an automated network and service management environment, the network conditions (like the key performance indicator monitoring or some conditions that will trigger the policies), of the managed system should be monitored in real time, that is without unnecessary delay. Once an unexpected behaviour is detected, the management system should analyse the collected data and derive the root cause to solve the problem as quickly as possible.

NOTE: The term real time is not defined here; in this context, it is used for immediate and parallel actions and to distinguish from an offline processing that can be performed independently from the normal execution at a later time.

6.4.4.2 Rationale and challenges

Traditionally, the network problems are usually processed by humans based on experience. In 5G networks, the increasing complexity brings large challenge to the network fault diagnosis. In this scenario, real time monitoring and analysis is defined as a capability of automation to the ZSM framework. With this capability, the network state can be monitored and the root cause can be derived quickly and automatically, which ensures an improved operation efficiency and reduces cost.

While, the multi-levels of network increase the difficulty of data analysis and the existing approaches used in this field is insufficient.

6.4.4.3 ZSM scenario details

The purpose of monitoring is to know the up to date status of the managed system to ensure its stability and reliability.

Monitoring is done to detect something is happening. A notification will be generated when certain network conditions are satisfied, to which the system might or might not act. Traditionally, monitoring is done by human. In this scenario, it refers to monitoring permanently and automatically done by the ZSM framework. This can be possible by defining conditions (expected KPI values or policy conditions) as well as actions to be triggered.

In addition, analysis, means to derive why did something happen. When an unexpected behaviour occurs (e.g. deviation from KPI expectations), the insights of the situation describing the root cause of the event should be derived by the data analytics to be able to trigger the right action. The ZSM framework can solve the problem, escalate it, or delegate it.

Monitoring and analysis applications can be simple ones from a single source of data, such as computing usage, latency, etc. And it can be very complex ones that detect specific conditions based on data collected from various sources, such as root cause analysis.

6.4.4.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to set conditions (KPIs or policy conditions) that need to be monitored.

Req-2: ZSM framework shall support the capability to monitor the state of the managed resources.

Req-3: ZSM framework shall support the capability to detect undesired conditions and trigger appropriate actions.

Req-4: ZSM framework should support the capability to analyse conditions to detect root causes.

6.4.5 Proposal for analytics domains and concepts for interaction

6.4.5.1 Description

ZSM shall provide mechanisms to allow for small or large atomic functions to perform tasks in a process to enable full zero-touch automation. This should be possible independently from the network or service nodes.

6.4.5.2 Rationale and challenges

In order to optimize the life cycle process of any network and service it is understood that the concept of DevOps and NetOps is likely to be an important enabling working model. In order to be able to achieve the agility required it is required that the operator has access to a wide range of tools and capabilities that can be adopted in both very well organized and well considered timing and in more urgent scenarios. This agility needs to be possible at the same time as service continuity is maintained and thus it has to be possible in a very agile manner to introduce new functionality and concepts independent on the network or service function.

6.4.5.3 ZSM scenario details

One example of a scenario that needs to be managed in an agile manner might be the following. A service is relying on the use of a range of vSwitches (VNF), as new traffic patterns are introduced by a new service this triggers certain bugs and issues of the switching VNF and it silently go off-line. The ability to understand that the node is malfunctioning is not possible from the normal O&M interfaces of the node but it is possible to understand from looking at the end2end traffic that is normally traversing the node as this is significantly interrupted. While the vSwitch vendor is resolving the underlying problem, the operator needs a mitigation strategy that minimize the service impact during these outages.

The operator develops a strategy using NetOps that can identify the fault (passive QoS monitoring of the service), Identify the failing node (active root cause analysis) and a policy to replace the VNF with a new instance in the affected location in the service topology. At the end of the incident the operator evaluates the impact to any subscriber by passive QoE analysis and feeds this data into a CEM process. If the service restoration time is short enough then the QoE impact is likely minimized and this metric can be used as an indicator of how effective this closed-loop assurance NetOps deployment is. As it is likely that the whole scenario has to be developed and commissioned within days if not hours it is unlikely that it is possible to extract new capabilities from a node provider for the affected End2End Services and thus this needs to be setup with individual components outside of the network or service nodes.

In order for this scenario to be possible a number of inherent capabilities needs to be present in the ZSM framework.

6.4.5.4 Related requirements for ZSM

Req-1: ZSM framework should support passive access to continuous up to date traffic in the network or service topology for an authorized consumer within the ZSM framework via relevant streaming APIs.

Req-2: ZSM framework shall support means to provide the current logical and physical topology of a network and service for an authorized consumer within the ZSM framework.

Req-3: ZSM framework shall support the ability for the authorized consumer within a management domain to relay a specific request for telemetry, trace or traffic to another management domain. Responding management domain shall be able to decline requests for telemetry, trace or traffic based on policy, security, operational or other considerations.

Req-4: ZSM framework shall support capabilities to evaluate and report the QoS of a network or a service, over either a specific duration of time or continuously over the service usage in near-realtime.

Req-5: ZSM framework shall support capabilities to identify the root cause of a network or service degradation. The root cause provided should be deterministic.

Req-6: ZSM framework shall support capabilities to evaluate and report the QoE of a service or a network service over either a specific duration of time or continuously over the service usage.

6.4.6 AI for network and service automation

6.4.6.1 Description

To address the issues of handling enormous amount of management data and shortage of network and service management personnel, Artificial Intelligence (AI) is becoming and effective mean for processing large amount of data and taking failure proof management decision. This'll help operators making their network management and service delivery much more cost efficient.

The functionalities of AI include "identification", "prediction" and "execution":

- "Identify" the current situation (characteristic) from the large amount of data.
- Analyse the characteristics of the data and "predict" the future tendencies.
- Make and "execute" the optimal plan which is based on the "identified"/"predicted" data.

6.4.6.2 Rationale and challenges

According to the introduction of 5G and network virtualization, the challenges on network and service are as follows:

1) Accelerate the network operation cycle and provide the services in early stage.
2) Establish the operation method to adapt advanced and complicated network.

The specific problems along with the two challenges above are assumed as follows:

- In the maintenance process, with the complex network topology which is due to the popularization of network virtualisation and network slicing, it is difficult to analyze the influence on customer service from a variety of data, recover the service according to the impact, and identify the failed device through alarm information, and implement the recovery.
- In the planning process, it will be complicated to predict the traffic volume of each network/hardware in a short time.

6.4.6.3 ZSM scenario details

The following scenario is expected when adopting AI to the maintenance process:

1) Collect and analyse a variety of data (alarm, log, packet data, etc.), identify the questionable part, and derive solutions from the history data with AI model.
2) Collect and analyse a variety of data (alarm, log, packet data, etc.), predict and detect the influence on network and service automatically, identify the questionable part, and derive solutions from the history data with AI model.
3) In case of the service influence detected by monitoring, it should be possible to take actions to recover the service automatically and confirm the service status after the action by utilizing the model generated by AI and a variety of data (alarm, log, packet data, recover information, etc.).

The following scenario is expected when adopting AI to the planning process:

1) Collect and analyze the status of traffic data and resources status, derive the expansion plan of virtual resources/network resources by AI, and control automatically.
2) Collect and analyze the event information and history data, and take actions automatically by AI to prevent the incidents occurrence or situation deterioration in the case of events such as concert.

There could be variety of AI algorithms available to a ZSM framework owner. However, interfaces/APIs necessary to feed such AI algorithms with appropriate data needs to be investigated and defined.

6.4.6.4 Related requirements for ZSM

To achieve network and service automation by using AI, the following are the requirements extracted from the above scenario:

Req-1: ZSM framework shall support collection of data from all managed entities within the ZSM framework that are necessary to perform automated network and service management based on AI.

NOTE: Data here refer to but not limited to configuration data, history data, operational data, topological data, inventory data.

Req-2: ZSM framework shall ensure that data is available not only inside management domains but also outside them so that such data can be available to any authorized consumer within the ZSM framework belonging to one operator.

6.4.7 CI/CD for ZSM framework functional components

6.4.7.1 Description

The agility is needed not only in network and services, but also in ZSM framework. This scenario focuses on the CI/CD of ZSM framework functional components.

6.4.7.2 Rationale and challenges

ZSM framework is a set of functional components that together provide capabilities for the automated network and service. For the ZSM framework functional components, it is necessary to improve ZSM services in a very agile way. CI/CD will help also for the framework component itself to link development, test, deployment and operation phases in ZSM functional component lifecycle. ZSM functional components should be reused, which is developed and deployed in an automatic way.

6.4.7.3 ZSM scenario details

A ZSM framework functional component should be a kind of managed entity that is self-contained and possible to integrate with other ZSM framework functional components to expose ZSM services. As defined in the scenario of "ZSM framework as entity in an ecosystem", a ZSM service is a management capability exposed by one or more functional components of the ZSM framework:

- ZSM framework functional components can be developed in a lot of ways. It can be developed from scratch, inhouse, or integrated using functional components from third party vendors.
- ZSM framework functional components will be integrated and deployed in the infrastructure. ZSM framework functional components should be reusable and interchangeable.
- Once in operation, ZSM framework functional components should have their own lifecycle. The possibility to replace and even improve ZSM framework in operation is an important quality of the ZSM framework, made possible with automated tests and verifications.

CI/CD pipeline can be used in the all the phases of ZSM framework functional components.

6.4.7.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to make ZSM framework functional components as managed entities that can be deployed independently.

Req-2: ZSM framework shall support the capability to change and upgrade functional components of ZSM framework without impacting other functional components and ZSM services.

Req-3: ZSM framework shall support the capability for automated lifecycle management of ZSM framework functional components.

NOTE: Examples are deploy, delete, upgrade, etc.

Req-4: ZSM framework shall enable interoperation between DevOps and operator CI/CD systems, in a way that does not require changes to the CI/CD systems themselves.

Req-5: Functional components of ZSM framework should be reusable and interchangeable.

6.4.8 Zero-touch self-optimizing network

6.4.8.1 Description

Network management is to a large degree about dynamic decision-making where human and artificial decision agents control different aspects of a complex dynamic system through feedback loops. As the state of the network and the usage of it change over time, different decisions have to be made to maximize the benefit of the investments in radio spectrum, equipment, and software.

Many decision loops are needed with different characteristics for different purposes. One of the most important parameters is time. The time scale of a decision loop is largely determined by the time needed to evaluate operating data in time to take good decisions and validate them, and the time it takes to execute any resulting change.

Figure 6.4.8.1-1: Distributed use of decision loops. By deploying a multitude of distributed autonomous decision loops with different characteristics the benefits of the investments in the network can be maximized

6.4.8.2 Rationale and challenges

As the networks enter the 5G and IoT era, network growth and complexity continue to accelerate. The network itself will be several magnitudes larger in terms of number of elements that have to be managed. Network Function Virtualization promises flexibility and network adaptation at a speed of change that is far beyond what a human can manage. With Internet of Things, traffic from safety critical applications, high volume data streams, and data with other characteristics and requirements, will be mixed in the network. Because of this, optimization of traffic towards a diversity of different network KPIs and SLAs becomes vital.

As operators also expect reductions in costs for managing their networks, the resulting requirement is that zero effort is spent on managing each network element.

Zero touch decision loops: An important zero touch principle is to maintain the separation of concern and time perspectives between different decision loops to ensure stable conditions for decision-making whether it is manual or automatic. To further emphasize the stability and to reduce the work efforts it is important to maintain consistent configurations across the network. These decision loops should represent all major activities needed for network management. Hence by reducing the effort in each of them to a minimum, the total effort will be close to zero.

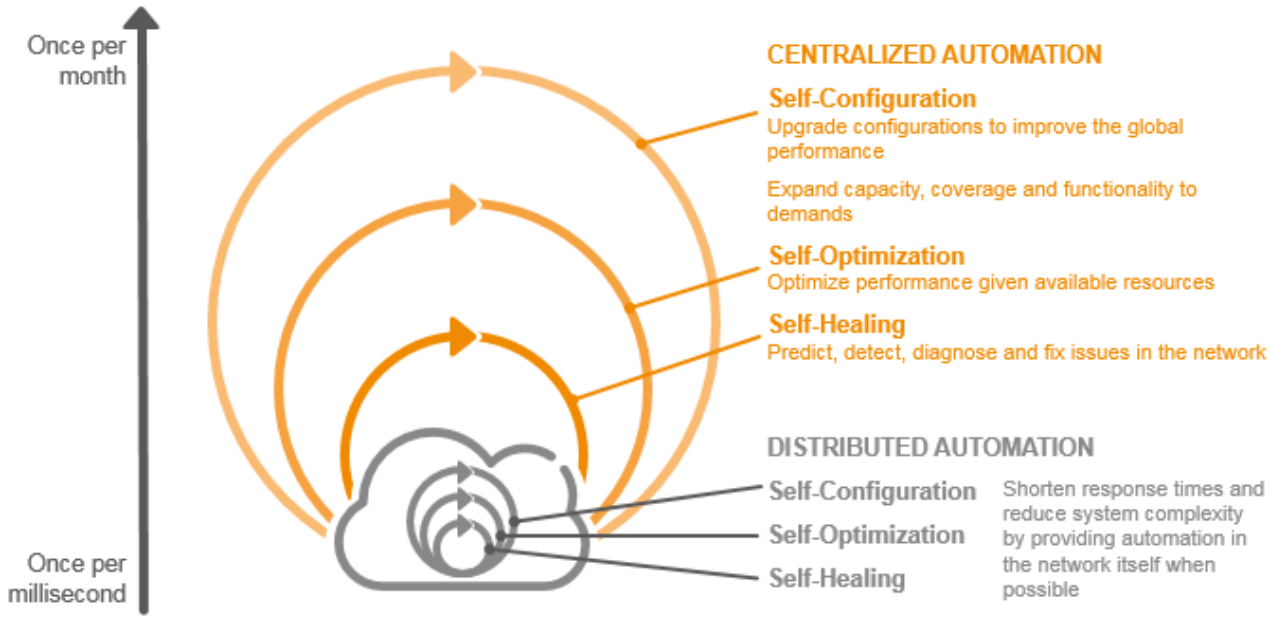

Figure 6.4.8.2-1: Examples of zero touch decision loops for different purposes. The terminology is only indicative

Use of machine intelligence: Automation strives at eliminating all frequent tasks. However, by introducing automation the risk of decreasing the degree of freedom could lead to a static solution. Instead of deploying many hand-crafted rules network management should be enhanced by machine-intelligence, including machine-learning and machine-reasoning, the automation functions will become self-learning and adaptive and will thus support the desired dynamical behaviour.

Analytics and policy instead of human interaction: Many of the existing network decision loops involve a human link. A set of reports has to be analyzed and a decision has to be made by a member of the NOC. To reach zero-touch, advanced analytics and dynamic policy have to replace these human qualities.

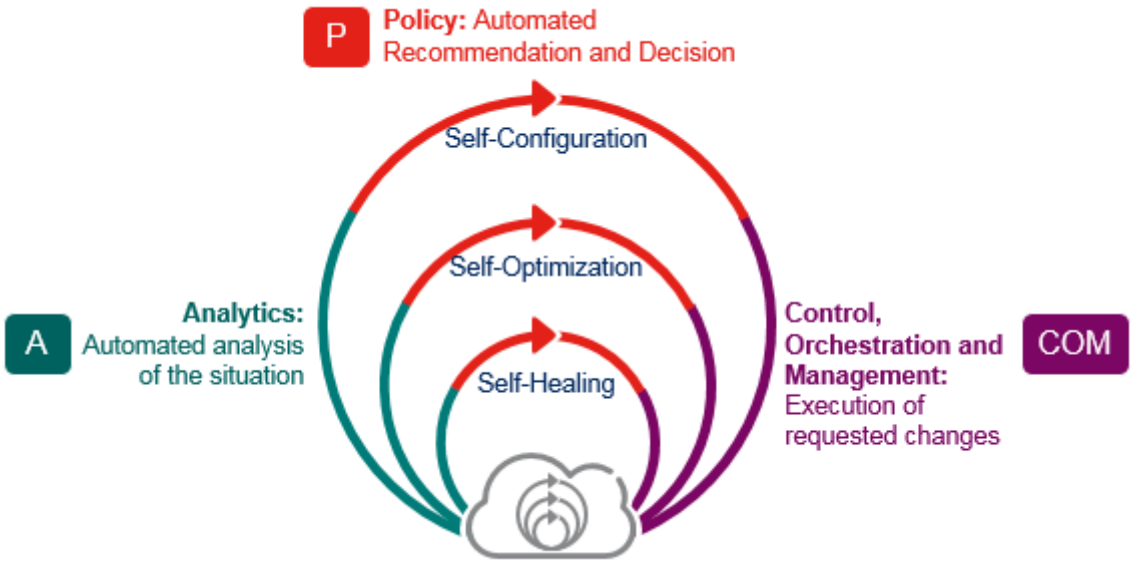

Figure 6.4.8.2-2: An example of how analytics and policy technologies could be deployed in decision loops to obtain a dynamic behaviour

Easy to use - easy to trust: The remaining tasks that have to be handled manually could gradually be replaced by policy-based decision making. This includes tuning of the overall network performance rather than tuning of each individual network element. Also, manual work would change from being reactive to being proactive. This is expert's work and requires significant knowledge and competence. To support this work, visualization and analytics tools

provide valuable insights and recommendations. Once a decision has been made, the actual execution would be straight forward by means of changes in policies. Monitoring the performance, proving the effects of automation functions, and keeping an audit trail of all changes is essential for trust-building. Scientific methods may be applied to try out a change in a small sample of the network before rolling out network wide.

Programmable and flexible: Each operator is expected to have their own flavor. E2E flows of tasks would have to be adapted to each operator's specific work processes and the network management system needs be able to interact with other systems in the operator's environment. To facilitate these adaptations models, software development kits, and APIs could be provided to support programming of the automation capabilities that have been included in the solution.

6.4.8.3 ZSM scenario details

To avoid instability in the network, deteriorating performance and increasing workload, the complexity could be kept under control by means of some principles:

Global parameter settings: The complexity in configuration of the network could be largely reduced by establishing a limited set of site types and assigning global parameter settings for each site type. Apply automated tuning of the remaining parameters that depend on local conditions.

Separation in time: An agent controlling the context for another agent has to be significantly slower. Input data rates and filtering times should correspond to the decisions at hand.

Separation of concern: Different agents should not be responsible for maintaining the same KPIs.

Separation of control: Different agents should not control the same set of parameters.

Distributed automation: Decisions should be made as close to the source as possible to reduce system complexity and to increase speed.

The fastest decision loops will be present in VNFs, even in the VNF components, to provide optimal characteristics for the benefit of the supported services in a dynamic environment. These are typically specific and not part of the network management, but they need to be in close connection with network-based functions in order to request extended support when the VNF specific resources are inadequate for providing the needed resources, e.g. computing power or data storage capacity.

Whereas the traditional network nodes are distinctly separated from the network management the need for flexibility and dynamicity in SDN/NFV based solutions force the demarcation lines to wither.

Furthermore, the principles would, in some cases, need to translate across multiple operator domains.

6.4.8.4 Related requirements for ZSM

Req-1: ZSM framework shall support the use of automated decision loops, with different characteristics and scope, as a means to perform network and service management.

Req-2: ZSM framework shall provide an interface for the purpose of bringing decision criteria to the decision loops, i.e. triggers, policies.

Req-3: ZSM framework shall provide means to hinder an overarching loop from infringing on a more local loop's responsibility. Exceptions from this rule shall be possible based on operator preferences.

Req-4: ZSM framework shall enable the collection of all relevant and available data, and the corresponding context information, needed by a specific decision loop.

NOTE 1: Care has to be taken not to overload the ZSM framework resources.

Req-5: ZSM framework shall be able to evaluate the network resources needed to enable the collection of data for each decision loop.

NOTE 2: The purpose is to perform a cost/benefit analysis.

Req-6: ZSM framework shall enable monitoring of the effects of automation functions to build trust in every stage of increased automation towards a fully automated solution.

Req-7: ZSM framework shall enable the network owner to disable any automation function in case of malfunction.

6.4.9 Self-learning based on reinforcement learning

6.4.9.1 Description

Reinforcement Learning (RL) is a type of machine learning algorithm that interacts with an unknown environment and tries to find an optimal policy to perform a given task. Some key ideas behind reinforcement learning algorithms come from behavioural psychology, and how these algorithms work resembles the general process of a child learning new tasks. RL has been investigated as a tool for creating distributed self-learning algorithms in telecommunications systems that are able to learn the network behaviour and optimize tasks, such as VNF self-scaling, self-healing, life-cycle management, etc.

6.4.9.2 Rationale and challenges

With the advent of virtualization, many network functions have become virtualized (e.g. vMME, vEPG, vSGSN, vPGW). Virtual network functions (NFVs) allow functionalities such as self-configuration, self-optimization and self-healing to be performed more quickly and in an automated way. Such functionalities enable the realization of parameter-free and zero-touch systems that assure SLA (Service Level Agreements) and reduce TCO (Total Cost of Ownership). Reinforcement learning is a promising technology to solve such an optimization problem.

Reinforcement learning is an ML technique that can be used to develop self-learning algorithms. The goal is to learn an optimal policy that will maximize a (long-term) value function. The self-learning algorithms interact with a given unknown environment by means of actions. Actions lead to the observation of limited and delayed rewards. The learning process and the environment to be learned are usually modeled as a markovian decision process. At each state the self-learning algorithms decide the next transition based on the action taken and the reward received. Considering the expected future rewards, a value function can be calculated at each state and an optimal policy that maximizes such function can be derived.

Since the self-learning algorithms work with a model-free environment, it needs to balance out exploitation and exploration. When exploiting, the self-learning algorithm selects the best policy learned so far based on previous experiences. On the other hand, when exploring, the self-learning algorithm searches for better policies using decisions not yet tried. Exploration creates opportunities to learn better policies, but also risks the degradation of the value function. In service-critical telecom systems, exploration can have an impact on the service quality and may risk the compliance with SLA.

The employment of self-learning algorithms is particularly challenging due to the operator's live production networks strict requirements on availability, stability, robustness, predictability/explanation, controllability, as well as operation efficiency and effectiveness. The main questions that need to be answered in this regard are related to the pre-training phase, the learning phase, and the interval of policy updates, as well as the question of human intervention.

There are some deployment options for the self-learning algorithm that need to be evaluated together with the operator, to find out the best way for stepwise adoption of RL in operational networks. To train a RL model, extensive exploration needs to take place to find the optimum action policy. A live system is either too slow or too sensitive to provide sufficient training data. A solution is to use a simulator to train the self-learning algorithm, and the trained policy is transferred to a live environment to take actions. The use of a simulated environment or sand-box to learn the policies and store the experience/knowledge in a repository to be used later in live deployments is still a research topic, but it will be crucial for the success to create self-learning algorithms that can rapidly be used in different environments and can safely be applied in live networks.

Lastly, the reward function is a quality measurement inherently dependent on operational expertise. Hence, it has to be designed with data scientists and subject matter experts. A good reward function should be able to capture instantaneous serious performance degradation and avoid significant negative impact on system performance or SLA fulfilment. Whenever human intervention is present during the adoption of RL, the actions manually taken, or the rejection of the self-learning algorithm ´s actions, should also be considered in the reward measurement.

6.4.9.3 ZSM scenario details

RL, as a special type of ML, inherently includes actuation as part of learning, hence becomes an attractive technique in network configuration and optimization. As discussed in previous sections, the operators are reluctant to allow a self-learning algorithm to enforce the actions without a human sanity layer. Besides, live networks may be too slow to provide insightful information for the self-learning algorithm to derive the optimal policy.

There are two main solutions to tackle both issues and enable an easy to use, easy to trust self-learning algorithm. One solution is to provide simulators and/or sand-boxes where self-learning algorithms could stress out exploration and speed up learning phase. Secondly, there is a need for a knowledge memory that would allow different learned policies to be stored and shared to speed up the self-learning algorithm´s learning process. The key idea of a shared knowledge memory is to stabilize the learning process and make full use of the diversity of different environments.

6.4.9.4 Related requirements for ZSM

Req-1: ZSM framework shall provide access to operational and historical data to authorized consumers.

Req-2: ZSM framework shall allow the creation and execution of ML sand-box environments where self-learning algorithms can get access and use data.

Req-3: ZSM framework shall provide means to store self-learning software´s knowledge in a persistent manner.

6.4.10 Optimization of supervised/unsupervised learning used in management services for closed loop

6.4.10.1 Description

To achieve zero touch automation in operation and management of 5G networks and network slicing, AI and ML are expected to support management services for closed loop such as predictive detection, root cause analysis and decision making etc. ML is mainly divided into three types of learning; supervised learning, unsupervised learning and reinforcement learning. In case of supervised/unsupervised learning, their accuracy depends on the quantity and quality of the training data, hence it is essential to enrich the predictive model using the data set obtained in both training phase before deployment and operation phase after deployment to enhance the accuracy of supervised/unsupervised learning used in management services.

6.4.10.2 Rationale and challenges

In manual operation, operators follow the procedures documented before starting operation to take actions such as isolating trouble and restoring it. The document is updated if something wrong or unknown events are found in daily operation. In case of zero touch operation leveraging supervised/unsupervised learning, it is required to keep optimizing ML used in management services for closed loop to assure the quality of service without human intervention as much as possible.

The challenges in optimizing supervised/unsupervised learning used in management services are as follows:

- The accuracy of ML is not so high in the beginning of operation due to lack of training data. It is necessary to use the data set (e.g. performance, log, topology, trouble information, etc.) obtained from non-production network during training phase before starting operation.
- The accuracy of ML needs to be improved continuously in operation phase using the data set (e.g. performance, alarm, topology, trouble information, etc.) obtained from production networks.

6.4.10.3 ZSM scenario details

The following scenario is expected to address the above challenges:

1) A new service is deployed on non-production environment.
2) A variety of trouble cases such as link down and traffic congestion etc. are made occur to collect and store data such as performance, log, topology and trouble information, etc.

3) ML used in management services leverages the stored data set to optimize ML.

4) The new service is deployed on production environment.

5) Data obtained during operation such as performance, alarm, topology and trouble information, etc. are collected and stored.

6) ML used in management services leverages the stored data set to improve the accuracy of ML.

6.4.10.4 Related requirements for ZSM

To achieve optimizing supervised/unsupervised learning used in management services for closed loop, the following requirements need to be considered:

Req-1: ZSM framework shall support the capability of collecting and storing data obtained in both training phase and operation phase such as performance, log, alarm, topology, trouble information, etc.

Req-2: ZSM framework shall support the capability of exposing the stored data set obtained in training/operation phase to ML used in management services to enhance the accuracy of ML based on these data.

6.5 Collaborative/federated service management

6.5.1 Communication services hosted across multiple operators

6.5.1.1 Description

An operator A may create a communication service across multiple operator networks, for example operator A and operator B. Operator A is responsible for the overall management of this communication service. This communication service across multiple operators is composed of other communication services or network resources from operator A and from operator B.

Operator A's ZSM compliant management system performs the following actions for the creation of such a communication service across multiple operators:

- Operator A receives a communication service request. Operator A determines to use its own and operator B's network to create the communication service, decomposes the communication service request for operator A's and operator B's network, and requests the creation of the composing partial communication services to each operator's management system.
- Both operators' management system may either create a new partial communication service or use an existing one to satisfy the request.
- When requested, operator B's management system provides management data (e.g. performance data) and appropriate management interfaces to operator A's management system for the part of the communication service hosted by operator B.

NOTE: Operator A may determine to use more than two operators to support the communication service. Operator A remains responsible for the management of the complete communication service.

6.5.1.2 Rationale and Challenges

This scenario brings a level of automation to this communication service creation and management, where, given the initial legal agreements are in place, on operator can create a communication service partially hosted by other operators in an automated way.

For realizing complete automation of such communication services there are a number of challenges to consider:

1) Automated business agreements such as automated pricing of the partial communication services requested.

2) Appropriate communication service catalogues exposed across operators, possibly at varying levels of abstraction.

3) Ability of an operator's management system to split communication service request to partial communication services based on this abstraction.

4) Automated inter operator interfaces to request such partial communication service.

5) Appropriate interface exposure between operators to support automated management of the partial communication services.

6) Appropriate security and access control to appropriately restrict the interface exposure.

7) Telemetry data collection across the operators that respects the abstraction levels.

6.5.1.3 ZSM scenario details

A communication service customer requests a communication service to operator A. Based on the communication services offered by multiple other operators, the operator A may host and manage the communication service over multiple operator networks. The following scenarios are possible.

Scenario 1: A communication service composed of multiple communication services:

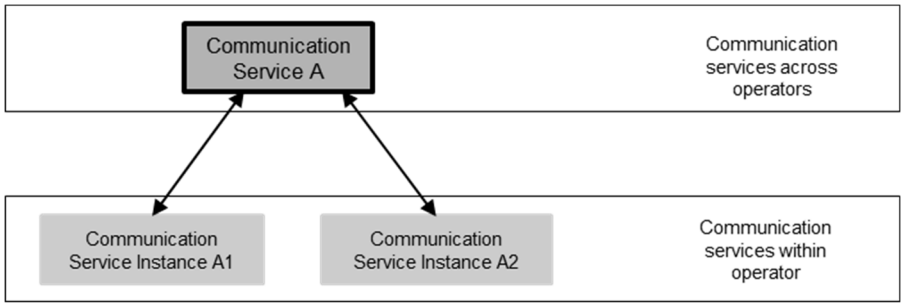

Figure 6.5.1.3-1: A communication service composed of two communication service instances across operators

- The operator A decomposes a communication service to multiple communication services and determines to host these multiple communication services in other operator networks.
- The operator A sends a request to host a part of the communication service to other multiple operators (operator B) with the required parameters. The parameters include but are not limited to the communication service identifier, the communication service requirements of the composed communication service, suitable APIs (e.g. PM/FM exposure), etc.
- After receiving the request, each of the other operators (operator B) creates a new partial communication service or use an existing one to satisfy the request.
- The operator A may receive the acknowledgement from each of the multiple other communication service provider (operator B) after a successful deployment of the communication service, the acknowledgement may include the appropriate information to identify the partial communication service.
- The operator A can provide the E2E management of the communication service to the customer.

Scenario 2: A communication service composed of multiple network slice instances:

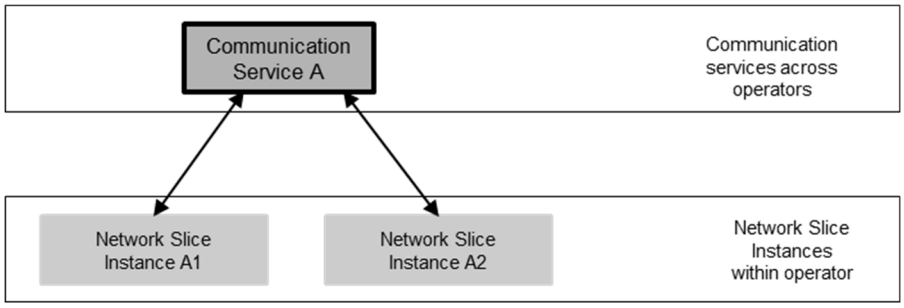

Figure 6.5.1.3-2: A communication service hosted over two network slice instances across operators

- The operator A creates a communication service and decomposes the communication service with multiple network slice instances and determines to host the multiple network slice instances in multiple other operator networks.
- The operator A sends a request to host a network slice instance to each of multiple other network operators with the required parameters. The parameters include but are not limited to respective identifiers, the network slice requirements of the composed network slice instance, suitable APIs (e.g. PM/FM exposure), etc.
- After receiving the request, each of multiple other network operators create a new network slice instance or use an existing one to satisfy the request.
- The operator A may receive the acknowledgement from each of the multiple other network slice providers after a successful deployment of the network slice instance, the acknowledgement may include the appropriate information to identify the instantiated NSI.
- The operator A can provide the E2E management of the communication service to the customer.

Scenario 3: A communication service with a network slice instance composed of multiple network slice subnet instances:

NOTE: A Network Slice Subnet Instance (NSSI) is defined within ETSI TS 128 530 [i.3].

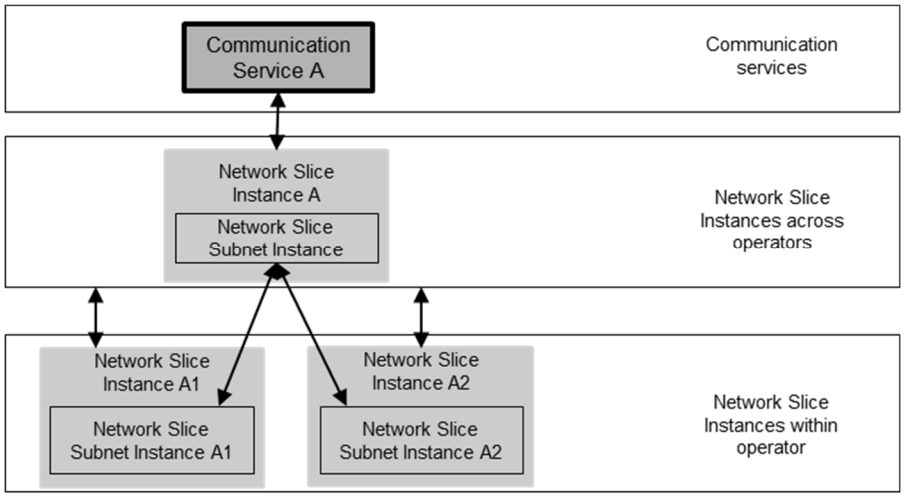

Figure 6.5.1.3-3: A communication service hosted over a network slice instance composed from two network slice subnet instances across operators

- The operator A creates a communication service with a network slice instance. The operator A decomposes the network slice instance with multiple network slice subnet instances and determines to host the multiple network slice subnet instances in multiple other operator networks.

- The operator A sends a request to host a network slice subnet instance to each of multiple other network operators with the required parameters. The parameters include but are not limited to respective identifiers, the network slice subnet requirements of the composed network slice subnet instance, suitable APIs (e.g. PM/FM exposure), etc.
- After receiving the request, each of multiple other network operators create a new network slice subnet instance or use an existing one to satisfy the request.
- The operator A may receive the acknowledgement from each of the multiple other network slice subnet providers after a successful deployment of the network slice subnet instance, the acknowledgement may include the appropriate information to identify the instantiated NSSI.
- The operator A can provide the E2E management of the communication service to the customer.

6.5.1.4 Related requirements for ZSM

The following requirements need to be fulfilled by the ZSM framework to enable the described scenario:

Req-1: ZSM framework shall support the capability of the automated creation and management of communication services and network slice instances hosted across multiple operators.

Req-2: ZSM framework shall support the capability of the automated service advertisement to and discovery from other operators' management domains.

Req-3: ZSM framework shall support the capability of the communication service decomposition and the automated communication service requests to multiple other network operators.

Req-4: ZSM framework shall support the capability to provide the interfaces' exposures for the automated management of the services.

NOTE: The supported level of automation is outside the scope of the present document.

6.5.2 Private communication services hosted by an operator

6.5.2.1 Description

In 5G network, enterprises in vertical industries will have private communication services for their business in conjunction with the 5G operators' networks. To do this, enterprises will request to an operator by using APIs exposed by the operator's management system to create and maintain the communication services on the operator's network as well as the enterprises' premise.

6.5.2.2 Rationale and Challenges

This scenario requires to bring a level of automation to the communication service management.

For realizing complete automation here, there are a number of challenges to consider:

1) Appropriate communication service templates exposed to enterprises and used by them for requests to an operator. Those templates require:
   a) To use expressions easily understood by IT engineers of enterprises who have sufficient knowledge of de facto cloud environment.
   b) To be flexible enough to be adjusted to various environments (e.g. hardware conditions of on premises equipment).
   c) To allow descriptions at various abstraction levels.
   d) To yield declarative requests in a sense that an operator keeps the network status as defined in the templates.

2) Appropriate interactions during operation between an operator and enterprises. This requires:

   a) To allow enterprises to supervise the network management.

   b) To allow enterprises to manage UE's subscription specific to the private communication services provided by the enterprise.

3) Appropriate access control and security protection for the interface allowing interactions between an operator and enterprises.

6.5.2.3 ZSM scenario details

Creation/modification/termination of a private communication service is executed quickly. Even a temporary (e.g. different time frames such as short-lived or long-lived services) usage of this service is expected.

Precondition: An operator A provides suitable APIs, so that enterprises in vertical industries can request creation/modification/termination of a private communication service with required parameters:

Step 1: Upon request from enterprise B, operator A creates such a service for enterprise B, targeting at UEs belonging to enterprise B.

Step 2: Operator A offers this service with a network slice instance, decomposing it to a network slice subnet instance instantiated on network equipment residing on enterprise B's premise and a network slice subnet instance on operator A's network.

Step 3: While the service is in operation, operator A provides the E2E management under the name of enterprise B and exposes information necessary for enterprise B to supervise this management.

6.5.2.4 Related requirements for ZSM

The following requirements need to be fulfilled by the ZSM framework to enable the described scenario:

Req-1: ZSM framework shall support the capability of managing the private communication services based on requests coming from enterprises via APIs with minimal manual interaction.

Req-2: ZSM framework shall support the capability to allow the network operator to instantiate the network slice subnet instance over the enterprise premises (networks).

Req-3: ZSM framework shall support the capability of managing the private communication service with a network slice instantiated on the enterprise's network and the operator's network.

Req-4: ZSM framework shall support the capability to offer APIs that allow enterprises to operate the private communication services according to their needs.

6.5.3 Automation in multi-stakeholder ecosystems

6.5.3.1 Description

Envisioned 5G applications and services (e.g. Industry 4.0, tactile internet, remote control of drones, e-health, etc.) pose new challenges on the underlying networks and clouds. The success of future 5G systems and applications highly depends on the novel methods addressing the integration and joint virtualization of cloud and network resources. Furthermore, there will be need for a novel coordination and orchestration of diverse set of cloud and network resources, controlled in different ways and owned by one or many providers.

6.5.3.2 Rationale and Challenges

New 5G use cases will require a diverse set of cloud and network resources:

i) controlled in different ways; and

ii) owned and managed by cooperating or competing providers.

These resources should be coordinated and orchestrated in a novel way to jointly control cloud and network resources instead of traditional approaches following separate control.

In addition, the technological basis has to be elaborated which enables future business models and cooperation among the stakeholders of the ecosystem. In the 5G ecosystem, operators have several options for providing services from simpler NFVIaaS (NFV Infrastructure as a Service) and NaaS towards fully fledged VNFaaS (Virtual Network Function as a Service) or any types of SaaS (Software as a Service).

In order to resolve the above-mentioned challenges, a novel cross domain orchestration system is necessary, which provides E2E NW as a service over multiple administrative and technology domains. It is important that ZSM framework supports such novel systems that will emerge in the future by means of appropriate services and interfaces definitions.

6.5.3.3 ZSM scenario details

Cross domain orchestration requires appropriate resource control interfaces and information models, together with the corresponding workflows realizing the joint virtualization and control of cloud and network resources in a flexible and programmable way in a multi-operator environment. It is necessary to support automated operations over multilayer orchestration hierarchies created on demand and spanning across multiple infrastructure domains, which can be under different administration.

In this ecosystem, multiple 5G operators with different roles, capabilities, hardware/software resources and service portfolios are cooperating in creation, deployment and provisioning of services. This federation of providers would make 5G a global platform and enables service provisioning over the aggregated resource set of the whole federation. Extending the geographic footprint to a global coverage could be an important incentive for operators to participate in this coopetitive ecosystem, where multiple players compete while cooperating for the delivery of the E2E global service.

Multi-operator collaboration has been considered by different ISGs and open source implementations. ETSI MANO has been extended to support multiple administrative domains for NFVIaaS and NS across different administrative domains. MEF defines the third network concept for agile and assured global connectivity services that will be orchestrated E2E across all network domains, which may be owned and orchestrated by different network operators. Furthermore, ONAP does not support hierarchical orchestration, so it does not enable the federation of providers (it does not let the 3rd party providers enter the 5G ecosystem).

6.5.3.4 Related requirements for ZSM

Req-1: ZSM framework shall support hierarchical and federated orchestration.

NOTE 1: Hierarchical and federated orchestration are not the only way of orchestration that ZSM framework supports. Others can be addressed by other requirements.

Req-2: ZSM framework shall support orchestration across management domains that belong to different administrative entities.

Req-3: ZSM framework shall support capabilities for abstracted exposure of resources and topology between different network providers.

Req-4: ZSM framework shall support automated composition of services based on service components provided by multiple stakeholders.

NOTE 2: Examples of components that can be used to compose services are VNF components.

Req-5: ZSM framework shall support automated onboarding of service and services components provided by 3rd parties.

NOTE 3: Examples of 3rd parties are verticals or other operators.

6.6 Security

6.6.1 Troubleshooting of encrypted traffic in ZSM framework

6.6.1.1 Description

It is assumed that the ZSM framework will provide secure and authenticated communication between network entities in the ZSM framework.

During the lifecycle of any network or service it is most likely that during several instances it is required to in detail troubleshoot the communication to and from the network entities in the ZSM framework and between the ZSM frameworks and between ZSM framework and the controlled network entities. In the case that the communication is encrypted between the network entities involved it needs to be possible to decrypt this by the authorized party. Information extracted from/after the encryption is used within the operator.

NOTE: It is out of scope of this scenario to deal with traffic within a network entity without any externally exposed interfaces.

6.6.1.2 Rationale and challenges

In the process of troubleshooting various issues it has been learned over historic events that one cannot disconnect the traffic processing and the security processing of the traffic (e.g. encryption). It has been shown that in the event of troubleshooting it is not possible to expect a deterministic behaviour between security switched on versus off.

3GPP has historically indirectly provided capabilities to perform key recovery and perform independent decryption of the relevant traffic. Many networks today provide E2E encryption for network entity to network entity security via IPsec and this today limits the visibility and ability to troubleshoot the network and service that relates to the traffic between the network entities.

For the purpose of security, the owner of the ZSM framework notifies the owner of the network entities involved in the communication of the possibility to decrypt the traffic during the troubleshooting period.

The authorized party in this context is appointed and approved by the relevant means chosen by the owner of the ZSM framework. The authorized party is a troubleshooting function used to identify and rectify temporary problems and issues related to the ZSM framework.

The authorized party receiving the traffic and being able to decrypt it needs to manage the decrypted data and the means for decryption at the same or at a higher security domain compared to the original security domain the traffic and the means of decryption was part of.

NOTE 1: The ability to decrypt the traffic does not provide the opportunity to perform a replay-attack on the network entities.

NOTE 2: This relates to the communication between the ZSM framework components and not the management of underlying infrastructure (NFVI, etc.).

6.6.1.3 ZSM scenario details

It is understood that it is not possible to rely on the decryption of the traffic from the traffic network entity in the case that the network entity is malfunctioning or underperforming in certain scenarios.

6.6.1.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability of decryption of management traffic.

NOTE: This is for troubleshooting purposes by an authorized consumer within the ZSM framework.

Req-2: ZSM framework shall support the capability of decryption of traffic without support from the network entity involved in the communication.

Req-3: ZSM framework shall not impact the network entity performance while decryption is supported.

Req-4: ZSM framework shall inform the owner of the ZSM framework that decryption is possible by the authorized consumer for the traffic sent during the duration of the troubleshooting process.

Req-5: ZSM framework shall inform the owner of the network entity/network entities involved that decryption is possible by the authorized consumer for the traffic sent during the troubleshooting process on demand.

6.7 Testing

6.7.1 Automated system test in production network

6.7.1.1 Description

In software verification, unit test, integration test, system test, etc. are necessary. These tests are done in development environment, laboratory environment, or production environment, depending on the testing purpose. This scenario describes about system tests of a network service in the production environment.

6.7.1.2 Rationale and challenges

System tests for a network service are generally performed in laboratory environments, which simulate production environments with smaller scale. Even if system tests were successful in the laboratory environments, the network service may fail in the production environments. Thus, it is indispensable to perform system tests in the production environments. However, if the tests are performed in manual manner, it will be more time consuming and error-prone compared to laboratory environments, because of the scale and complexity. Therefore, it is also important to perform system tests in fully automated manner in production environments.

Following key challenges need to be considered for this scenario (non-exhaustive lists):

- Perform system tests in cross domains.
- Perform system tests without interfering to other services which are in operation.

6.7.1.3 ZSM scenario details

As a network operator, she/he wants to perform the following items in fully automated manner in his/her network, eliminating any human intervention:

Pre-condition: A network service to be launched is deployable in the production network.

Step 1: The network service is deployed and configured for testing.

Step 2: Optionally, additional testing functions (e.g. test traffic generator/receiver, live traffic mirroring) are deployed as needed and configured for testing.

Step 3: Prepared test scenarios are executed.

Step 4: Once all the test scenarios are successful, the testing functions are removed.

Step 5: The network service is configured for starting live operation.

Post-condition: The network service starts providing its service.

6.7.1.4 Related requirements for ZSM

To achieve an automated system test in production network, the following requirements need to be met:

Req-1: ZSM framework shall support the capability to perform automated system tests of a network service deployed in multiple network domains including but not limited to access, transport, core, and cloud.

Req-2: ZSM framework shall support the capability to automatically deploy and configure necessary testing functions for automated system tests across multiple network domains including but not limited to access, transport, core and cloud.

Req-3: ZSM framework shall support the capability to perform system tests of a network service without interfering other unrelated services.

6.7.2 CI/CD for network services

6.7.2.1 Description

CI/CD has been widely used in IT industry, which greatly promotes the software iteration and rapid provisioning of network services. Similar needs also exist in telecommunication industry. E2E, developer-to-provider CI/CD lifecycle enables dynamic additions and changes of network services, which helps to achieve the development and operational agility in 5G networks.

This scenario focuses on the CI/CD for network service. The CI/CD pipeline for the managed entities is outside the ZSM framework. But the ZSM framework may be aware of some actions of the CI/CD pipeline or needs to support the automated actions triggered by the CI/CD pipeline.

6.7.2.2 Rationale and challenges

CI/CD will become a necessary part of the network life cycle management to achieve automation and agility, ensuring carrier-grade stability and improving operational efficiency. These goals can be met with CI/CD:

- Accelerate the software release, and achieve frequently delivery of small changes.
- Ensure the latest version, and improve the error correction.
- Reduce the failure rate and operational costs.

Challenges:

- How organizations and teams work together, e.g. CI/CD teams of supplier of the managed entities and the user (CI/CD teams with service provider organizations).
- Joint CI/CD pipeline of integrated development, testing, deployment in productive environments; definition of a touchpoint between CI/CD pipeline of developers (in vendor environment) and the CI/CD pipeline of the operators/service provider.
- CI/CD pipeline will trigger some lifecycle management actions of network services, which should be executed by ZSM framework automatically.
- Multiple stages of the test results in both the CI/CD pipeline and ZSM framework should feedback to the developers before the network service enters the productive environment to improve it.
- CI/CD pipeline needs to interact with the ZSM framework for organizing the deployment and test in life networks or in shared deployment of testing and life deployments.

6.7.2.3 ZSM scenario details

CI/CD is an automated process of development, testing, and deployment for each network service, which is implemented as a joint CI/CD pipeline.

The existing phases of the CI/CD pipelines need to run in a ZSM controlled deployment. But the ZSM framework will not control the CI/CD pipeline, just enable it. The following phases should be considered in the CI/CD pipeline:

- Software of the network service is developed and integrated:
  - This step means the developer keeps their work-in-progress continually integrated with every other developer, which is the meaning of continuous integration (CI). CI is the first step of CI/CD pipeline, which may be implemented by vendors. In this phase, the new capability is tested to ensure the new software can run in ZSM framework.

- The newly integrated software of network service is deployed as an instance to the running environment using ZSM framework LCM operations:
  - After testing, CI/CD pipeline will trigger the network service deployment functionality using the interface exposed by ZSM framework. Then, ZSM framework will deploy the new network service software to the running environment as a network service instance, which is controlled by ZSM framework.
- The instance is maintained and upgraded:
  - In a CI/CD environment, the network services are always running the latest version of software, which also leads to a faster implementation of the software bug corrections. Frequent service upgrade is also triggered by the CI/CD pipeline, and executed by the ZSM framework.

The pipeline should enable collaboration between the various groups involved in delivering software and provide everyone visibility about the flow of changes in the system, together with a thorough audit trail.

In all the phases of the CI/CD pipeline, zero touch automation is a key to accelerate CI/CD cycle, like automated testing and automated deployment. There will be a need for multiple testing environment to allow for multiple stage of testing in the whole life of deployment of network service, both in the CI/CD pipeline and ZSM framework. ZSM framework will provide a testing environment for different types of testing, and the testing functionalities can be deployed as needed in the ZSM testing environment, which is intended for use by operators/service provider, vendors and the CI/CD team. The general testing functionalities can be deployed into the ZSM framework as a testing scenario, which can be reusable and be triggered by the CI/CD pipeline. In addition, the specific testing can only be done by the developers in the CI/CD pipeline, but not deployed to the ZSM framework testing environment.

6.7.2.4 Related requirements for ZSM

Req-1: While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability to treat network services as standalone units that can be deployed independently from other unrelated services.

Req-2: While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability to change and upgrade the services without any impact on other unrelated network services.

Req-3: While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability to expose the interfaces of network service testing, deployment and upgrade, so that these actions can be triggered by a CI/CD pipeline.

Req-4: While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability to make use of the existing CI/CD toolchains.

Req-5: While network services are upgraded and tested in CI/CD pipeline, ZSM framework shall support the capability of additional automated tests of network services.

NOTE: See the detailed testing requirements in scenario "Automated system test in production network".

Req-6: ZSM framework shall support the capability of enabling interoperation between CI/CD pipeline in vendor environment and service provider CI/CD pipeline for the managed entities, in a manner that does not require changes to the tools of the CI/CD pipelines.

6.7.3 Automated test capabilities concerning ZSM

6.7.3.1 Description

The management and orchestration of 5G networks and services have to cope with several challenges caused by different reasons such as expected and unexpected events and failure situations, e.g. management functionality, service, and system integration, trouble shooting, optimization concerning infrastructure and services, and network congestion cases.

Therefore testing capabilities, especially automated capabilities are important in the ZSM field.

The tests can be carried out in different test environments for example within dedicated test networks and/or production/live networks.

The tests will be realized based on several information, e.g. policies, rules, profiles, configuration data as well as performance data and will be connected with for example AI functionalities for analysis, decision making and triggering of follow-up actions.

6.7.3.2 Rationale and challenges

Tests are crucial after and before several expected and unexpected events and actions to identify whether services/applications, functionalities, and components especially in the management context are working as requested.

In addition, it is also important that these tests will be triggered and carried out automatically to avoid e.g. manual failures and to be faster to solve them without human intervention.

Furthermore, testing in production/live networks is necessary as well to have the appropriate environment depending on the test scenarios.

Following key challenges have to be considered in this context, for example (non-exhaustive enumeration):

- Automated E2E management and orchestration of testing concerning 5G networks, services and applications.
- Automated testing as well as management of the 5G networks, services and applications via several administrative and/or technical domains.
- Automated testing as well as to recommend and to trigger respectively the appropriate follow-up actions in this context.
- Considering of several data sources, e.g. policies, rules, profiles, and SLAs and to trigger automatically the appropriate tests.
- Automated handling of conflict resolution within a single or between several administrative and/or technical domains.
- Automated testing within production/live networks after for example automated failure corrections without impacting the current requested behaviour of the running services.

6.7.3.3 ZSM scenario details

To fulfil the challenges and requirements on this field, there are several steps necessary (not a complete list/description):

- The test network(s) and/or the production network as well as the ZSM framework are deployed to support functionality that enables the realization of automated testing capabilities.
- The services, components and functionalities, which shall be tested are deployed.
- The test scenarios are prepared.
- The tests will be executed.
- Afterwards the appropriate follow-up actions will be automated recommended and/or triggered.
- After a successful handling the services, components and functionalities, which have been tested and possibly modified, etc. are working in a requested manner.
- Otherwise, additional actions have to be carried out.

6.7.3.4 Related requirements for ZSM

This is a listing of related requirements (not a complete list):

Req-01: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for service tests within test networks.

Req-02: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for service tests within production/live networks via single and/or several administrative and technical domains.

Req-03: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for active and passive testing of E2E services and/or only parts of them.

Req-04: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for active and passive testing of management functionalities/capabilities.

Req-05: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities based on several information such as rules, policies, profiles, models, configuration data, performance data, and SLAs/OLAs.

Req-06: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities in connection with the automated conflict resolution handling within a single or between several administrative and/or technical domains.

Req-07: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities in connection with AI and machine learning functionalities and applications.

Req-08: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for service tests after the modification/update of this service.

Req-09: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities for service tests to support the finding of the root cause.

Req-10: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing capabilities to identify the failure segment within an E2E service chain.

Req-11: ZSM framework shall support the capability of enabling the provisioning and the support of automated testing and management capabilities to recommend and/or to trigger appropriate follow-up actions.

Req-12: ZSM framework shall support the capability of enabling the provisioning and the support of automated management and orchestration capabilities for the automated testing capabilities including their follow-up actions triggered by them.

6.8 Tracing

6.8.1 Automated tracing capabilities

6.8.1.1 Description

Automated tracing capabilities will become more and more important. The tracing capabilities will be used e.g. for trouble shooting, root cause analysis, optimization of infrastructure and services, support of testing activities, support of prevention and mitigation of cyber attacks, to deliver data for automated decision handling in the connection with AI and ML functionalities. In addition, with the tracing an automated decision can be tracked and explained for an authorized consumer on demand in the context of automated decision making from AI and ML algorithms.

The tracing will be seen here based on the description in [i.4].
The tracing can be realized in test environments as well as in production and live networks.
The tracing could be executed based on for example configuration and performance data, profiles, rules and policies.

6.8.1.2 Rationale and challenges

Tracing is relevant for the monitoring of infrastructure and SW, especially services.
The tracing capability can be a crucial factor in the case of unexpected events and in connection with predictions. In addition, it is also important for the testing area.

Following key challenges have to be considered in this context, for example (non-exhaustive enumeration):

- Automated E2E management and orchestration of tracing for 5G networks, services and applications.
- Automated tracing concerning 5G networks, services and applications via several administrative and/or technical domains.
- Automated tracing and to trigger automatically the appropriate follow-up actions.
- Considering of several data sources, e.g. policies, rules, profiles, and to realize automatically the appropriate tracing procedures.
- Automated tracing within production/live networks without impacting the current requested behaviour of the running services.
- Automated handling of several trace levels based on several conditions.

6.8.1.3 ZSM scenario details

To fulfil the challenges and requirements on this field, there are several steps necessary (not a complete list/description):

- The test network(s) and/or the production network as well as the ZSM framework are deployed to support functionality that enables the realization of automated tracing capabilities.
- The services, components and functionalities, which shall be traced are deployed automatically.
- The trace procedures are prepared automatically.
- The traces will be executed automatically.
- Afterwards the appropriate follow-up actions will be automatically triggered.
- After a successful automatic handling the services, components and functionalities, which have been traced and possibly modified automatically, etc. are working in a requested manner.
- Otherwise, additional actions have to be carried out automatically.

6.8.1.4 Related requirements for ZSM

This is a listing of related requirements (not a complete list):

Req-01: ZSM framework shall support the capability of enabling the automated management of automated tracing capabilities.

Req-02: ZSM framework shall support the capability of enabling several tracing levels on demand in an automated way.

Req-03: ZSM framework shall support the capability of enabling automated tracing capabilities in production/live networks without any impairment of the running E2E services.

Req-04: ZSM framework shall support the capability of enabling automated tracing capabilities based on several information e.g. rules, policies, profiles, information and data models, configuration and performance data.

Req-05: ZSM framework shall support the capability of enabling automated tracing capabilities with the use of AI and machine learning functionalities and applications.

6.9 Integration/interoperation

6.9.1 ZSM framework as entity in an ecosystem

6.9.1.1 Description

A commercial telecommunications service provider (a network and/or service operator) wants to use a ZSM framework to provide (telecommunication) services "zero-touch". The ZSM framework enables automatic network and service management and exposes ZSM services to consumers.

6.9.1.2 Rationale and challenges

As a business entity, the commercial telecommunications service provider (network and/or service operator) strives to prosper within the commercial ecosystem and to be of high value for its stakeholders. This can only be achieved if providing services that are useful for and needed by customers, at minimum cost and within a time as short as possible to enable.

Rationale:

- Increase dynamicity and speed to create and deliver services; accelerate processes.
- Cope with increasing complexity and amounts of data.
- Efficient use of resources reduce cost and improve return on investments.
- Reduce delays and issues caused by manual, time-intensive steps in processes; free humans for other tasks.

Challenges:

- Interaction and, to some extent, cooperation with other entities in the ecosystem around the ZSM framework will be necessary:
  - Interactions with humans:
    - e.g. to steer the ZSM framework (e.g. parameters, configuration, constraints, adding new HW or SW components); or
    - during new service development.
  - Interactions with non-human entities (commercial, technical):
    - ZSM framework is unlikely to cover and produce every part of its services by itself.
- Evolution of the ZSM framework itself (incl. migration to ZSM from non-automated systems).

6.9.1.3 ZSM scenario details

As an entity, the ZSM framework is embedded in a wider ecosystem, and has relationships and interfaces with its owner, consumers of ZSM services and providers (see also figure 6.9.1.3-1).

The owner is a (business) entity that owns the ZSM framework; e.g. operators. As entity, the owner is non-human, but it "employs" humans for different tasks.

Consumers of ZSM services use one or several of the management capabilities exposed by the ZSM framework. Consumers are non-human entities or human users. Human users may fall into different categories; like e.g. "end user", enterprise or operator customer, administrator (employee of the owner). ZSM services offer machine-consumable interfaces. For interfacing with human users they require the use of e.g. a GUI, web portal or application.

Providers are entities that the ZSM framework uses to manage networks and (telecommunication) services. These entities are non-human, but may "employ" or require humans for different tasks:

- Examples for providers in the business domain: Vendors, other operators.

- Examples for providers in the technology domain: RAN, 3GPP/5G Core, Optical, Ethernet, VNFs, HW components.

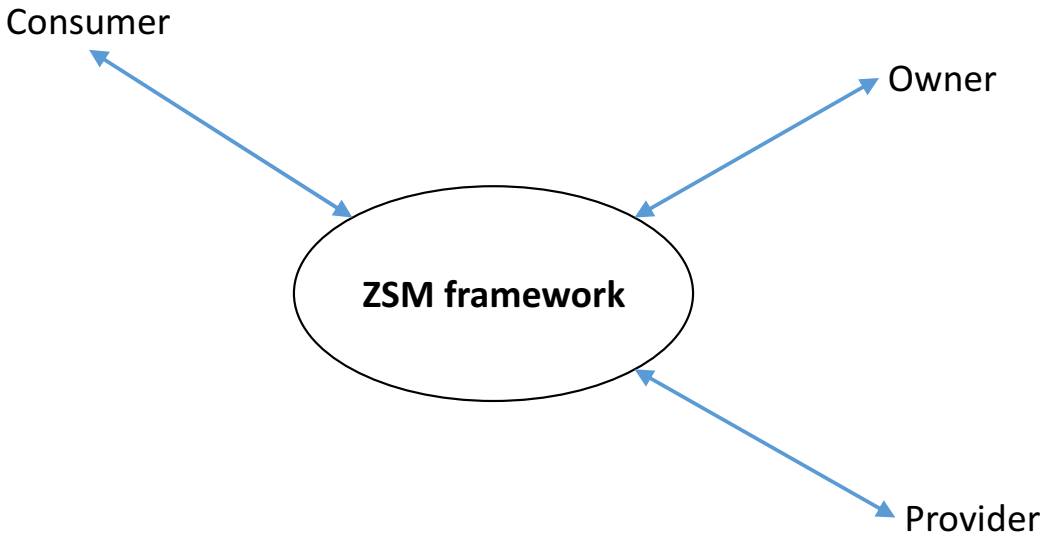

Figure 6.9.1.3-1: ZSM framework is embedded in a wider ecosystem

Assumptions:

- ZSM services enable consumers to interact with the ZSM framework and to manage (telecommunication) services.
- The number of (telecommunication) services may vary over time.
- The number of ZSM services may vary over time.
- (Telecommunication) services are instantiated for use (service delivery).
- The ZSM framework manages the (telecommunication) service lifecycle automatically, including progressing from phase to phase and step to step within phases.
- At certain points in the (telecommunication) service lifecycle input and/or triggers may be required to progress to or activate a next step or phase. Such inputs or triggers may come from humans or non-human entities in the wider ecosystem.

The lifecycle of (telecommunication) services is handled by the ZSM framework and comprises the following three stages:

1) Creation:
   a) Design
   b) Preparation for utilization
2) Utilization (0..n times; in parallel and/or sequentially):
   a) Instantiation and Initialization
   b) Service Delivery by the service instance (usage)
   c) Modification/Adjustment of service instance (may include deactivation & reactivation)
   d) Instance termination (incl. deactivation)

3) Elimination:

   a) Disposal

NOTE: The detailed lifecycle stages and processes are beyond of the scope of the present document.

Examples for inputs or triggers required to come from humans:

- Initiation of service creation based on customer request.
- Utilization of service instance based on customer purchase.
- Escalation of error situation or decision to be taken that the ZSM framework cannot handle.

6.9.1.4 Related requirements for ZSM

Req-1: ZSM framework shall have the capability of managing the lifecycle of customer-facing services.

Req-2: ZSM framework shall have the capability of managing the lifecycle of resource-facing services.

Req-3: ZSM framework shall be able to interact with entities outside of itself (owner, consumer, provider).

Req-4: ZSM framework shall support the capability to interact with humans and to adjust to conditions where human intervention/reaction is required, e.g. using a GUI, web portal or application.

Req-5: ZSM services shall offer machine-consumable interfaces.

Req-6: ZSM services may provide means for interfacing with human users.

Annex A (informative): Change History

Date	Version	Information about changes
March 2018	0.0.1	Skeleton proposal
April 2018	0.0.2	Skeleton modified, Title modified, Disclaimer adapted, Scope adapted, Editor's note in clause 4.2 "Requirements" adapted. The term "use cases" has been removed. Clause 6 "Use cases" removed. The entry in the "Document history" removed.
May 2018	0.1.0	Editor's note in clause 5.1 "Introduction" incorporated. Following contributions have been incorporated: - ZSM(18)000089r2 Other Proposal of ZSM scenario: Slice Life Cycle Management - ZSM(18)000090r5 Other Proposal of ZSM scenario: Slice Isolation - ZSM(18)000092r4 Other Proposal of ZSM scenario: ZSM System as Entity in an Ecosystem - ZSM(18)000093r4 Other Zero-touch Full Automation of 5G network and Service Management - ZSM(18)000107r4 Other Scenario for management and orchestration of network slicing - ZSM(18)000108r3 Other Proposal on Scenario for exposure of management interface to support management and orchestration of NSaaS - ZSM(18)000109r2 Other Scenario for network slice monitoring - ZSM(18)000111r2 Other Scenario for automated network bandwidth management - ZSM(18)000112r1 Other ZSM scenario Proposal: Automated Healing - ZSM(18)000116r1 Other Proposal_for_ZSM_scenarios_Automatic E2E Network Topology Management - ZSM(18)000128r3 Other NaaS lifecycle and exposure with an IoT network slicing use case Editorial Changes: - Formatting changes - Orthographical corrections - Names of contributors included in annex C.
August 2018	0.2.0	Following contributions have been incorporated (1): - ZSM(18)000015r3 - ZSM(18)000115r5 - ZSM(18)000175r3 - ZSM(18)000194r2 - ZSM(18)000168r3 - ZSM(18)000013r6 - ZSM(18)000202r1 - ZSM(18)000206r4 - ZSM(18)000208r3 -> Please see the following page for further information

Date	Version	Information about changes
August 2018	0.2.0	Following contributions have been incorporated (2): - ZSM(18)000212r8 - ZSM(18)000213r3 - ZSM(18)000215r1 - ZSM(18)000216r1 - ZSM(18)000255r2 - ZSM(18)000262 - ZSM(18)000266r2 - ZSM(18)000284r1 - ZSM(18)000285r2 - ZSM(18)000286r2 - ZSM(18)000290r2 - ZSM(18)000295r2 - ZSM(18)000305 The normative reference for [2] "DGS/ZSM-00007ed111_Terminology" in clause 2.1 "Normative references" included The following informative references in clause 2.2 "Informative references" included: "ETSI GR ZSM 005 " "ETSI GR NFV IFA 023" ETSI TS 128 530 V15.1.0 3rd Generation Partnership Project; Technical Specification Group" Some Editor's note deleted and incorporated Some Notes incorporated In clause 3.1 "Definitions" one definition included. This definition will be shifted later to the ZSM Terminology document [2] In clause 3.3 "Abbreviations" abbreviations added Additional names of contributors included in annex C Editorial Changes: - Formatting changes - Orthographical corrections
October 2018	0.3.0	- Categorization of the scenarios based on the contribution ZSM(18)000368r3 "Proposal on grouping of scenarios and way forward working methodology" realized Following contributions have been incorporated and assigned to the appropriate categories: - ZSM(18)000195r8 Scenario for a Zero-Touch Self-Optimizing Network - ZSM(18)000288r7 CI/CD for network services - ZSM(18)000291r5 Self-learning based on reinforcement learning - ZSM(18)000312r3 ZSM001 Scenario about automated test capabilities - ZSM(18)000364r2 Automated discovery of services offered by a management domain - Contribution ZSM(18)000216r1 "Use Case for multi-operator service deployment" has been removed because this content is already captured in ZSM(18)000295r2 "Add ZSM Scenario details in Use Case for multi-operator communication service deployment" - Numbering of the figures partly adapted Editorial Changes: - Formatting changes - Orthographical corrections

Date	Version	Information about changes
November 2018	0.4.0	Following contribution has been incorporated and assigned to the appropriate category: - ZSM(18)000475r2 Scenario on Optimization of supervised/unsupervised Learning used in Management Services for Closed Loop The corresponding requirements have been included in the requirement clause 4. Additional names of contributors included in annex C Editorial Changes: - Formatting changes - Orthographical corrections
November 2018	0.5.0	Following contribution has been incorporated: - ZSM(18)000535r1 ZSM001 propose to update and restructure requirements Editor's notes concerning requirements 1 and 2 in clause 5.4.9.4 removed because these Editor's notes have been solved by appropriate contributions regarding ZSM007. Editorial Changes: - Formatting changes - Orthographical corrections
December 2018	0.6.0	Following contributions have been incorporated: - ZSM(18)000566r2 ZSM001 scenario on Network service management by multiple levels of service - ZSM(18)000574r2 ZSM Scenario: Private communication services hosted by an operator - ZSM(18)000617 ZSM001 propose to re-categorize scenario - ZSM(18)000618r3 ZSM001 propose to reword requirements - part 1 - ZSM(18)000620r3 ZSM001 propose to update requirements - part 3 - ZSM(18)000621 ZSM001 propose to update requirements - part 6 - ZSM(18)000627r2 ZSM001 propose to update requirements - part 8 - ZSM(18)000628r1 ZSM001 propose to update requirements - part 5 - ZSM(18)000629r2 ZSM001 propose to update requirements - part 7 - ZSM(18)000632 ZSM001 propose to reword requirements - part 4 Editorial Changes: - Clause numbering updated - Numbering of the figures partly adapted - Formatting changes - Orthographical corrections
January 2019	0.7.0	Following contribution has been incorporated: - ZSM(18)000647r1 ZSM001 propose to update requirements - part 2.2
March 2019	0.8.0	Following contributions have been incorporated: - ZSM(18)000648r2 ZSM001 propose to update requirements - part 2.3 - ZSM(18)000649r3 ZSM001 propose to update requirements - part 2.4 - ZSM(18)000650r1 ZSM001 propose to update requirements - part 2.5 - ZSM(18)000651r3 ZSM001 propose to update requirements - part 2.1- ZSM(18)000029 ZSM001 2.2 Informative references; Adding a reference - ZSM(18)000606r2 ZSM001 5.x Tracing - ZSM(18)000526r4 Automation in Multi-stakeholder Ecosystems Editorial Changes: - Clause numbering updated - Numbering of the figures partly adapted - Formatting changes - Orthographical corrections
March 2019	0.8.1	GS declared as a stable draft.

Date	Version	Information about changes
May 2019	0.9.0	Changes have been made based on the contribution ZSM(19)000252 Deletion of Annex F. That means listed authors & contributors removed from the present document. Editorial Changes: - Annex numbering updated.
August 2019	0.10.0	Status: Proposed Final draft. This draft will be sent to editHelp! for clean-up. Following contributions have been incorporated: - ZSM(19)000279r3 ZSM001: Changing ZSM framework user to ZSM framework consumer - ZSM(19)000286r2 ZSM001: Removal of Editor's note, etc. in the ZSM001 GS - ZSM(19)000287r1 ZSM001: Modification proposals concerning clause 5.6.1 "Scenario for Troubleshooting of encrypted traffic in ZSM" - ZSM(19)000355r2 ZSM007: Definition of hierarchical orchestration and federated orchestration - Only the definitions for "hierarchical orchestration" and "federated orchestration" have been incorporated in the ZSM001 draft GS from the contribution ZSM(19)000355r2. - ZSM(19)000373 ZSM001: Editorial Changes - ZSM(19)000384 ZSM001: Explanation for the term "day two operation" concerning the LCM operations - ZSM(19)000409r1 ZSM001: remove EN in 5.2.3.12.4 - ZSM(19)000417r1 ZSM001: Additions and modifications of normative references within the clause "Normative references" of the ZSM001 draft GS - ZSM(19)000422 ZSM001: Addition and modification of references in the clause "1 Scope" of the ZSM001 GS - ZSM(19)000423r2 ZSM001: Addition of a new clause "4 Introduction" in the ZSM001 GS - ZSM(19)000441r1 ZSM001: Content for clause 4.1 "Introduction" and related modifications in clause 4.2 "Requirements" - ZSM(19)000443r1 ZSM001: Incorporation of additional abbreviations in clause 3.3 "Abbreviations" of the draft ZSM001 GS - Requirements in the scenario descriptions synchronized with the modified requirements in the requirement table - Requirement table updated concerning the modification of requirements based on approved contributions, requirement numbering, clause headings, clause references, etc. Editorial Changes: - clause numbering, clause headings, and the corresponding references within the present document updated - Additional references included - References partly modified - Additional figure captions incorporated - Numbering of the figures adapted - Table header for the requirement table updated - Table caption respectively table reference incorporated - Additional abbreviations in the "Abbreviations" clause included - Corrections concerning the term "must" which is not allowed in ETSI deliverables - Adaption of the text concerning abbreviations, etc. - Annex headings updated - Formatting changes - Orthographical corrections

Date	Version	Information about changes
August 8th, 2019	0.11.0	Status: Final Draft Editorial Changes: - ETSI editHelp! cleanup - References partly modified - Formatting changes - Orthographical corrections - A few abbreviations in the "Abbreviations" clause removed - Additional abbreviations in the "Abbreviations" clause included

History

Document history		
V1.1.1	October 2019	Publication