ETSI GR ZSM 021 V1.1.1 (2026-05)

GROUP REPORT

Zero-touch network and Service Management (ZSM); Study of ZSM Framework from Automation to Autonomy

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
DGR/ZSM-021_GRAutom2Auton

Keywords
artificial intelligence, automation, autonomous, levels

ETSI

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

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

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

Contents

Intellectual Property Rights 4
Foreword 4
Modal verbs terminology 4
1 Scope 5
2 References 5
2.1 Normative references 5
2.2 Informative references 5
3 Definition of terms, symbols and abbreviations 6
3.1 Terms 6
3.2 Symbols 6
3.3 Abbreviations 6
4 ZSM target to autonomy 7
4.1 Concept of autonomy 7
4.2 Differences between automation and autonomy 8
4.3 High-Level Description of autonomous system 8
4.4 The progress of Network Automation 9
4.4.1 Review of ZSM work 9
4.4.2 Review of industry work 10
4.4.2.1 Introduction 10
4.4.2.2 Standardization of the Network Automation and Autonomy 10
4.4.3 Review Summary 11
5 Scenarios that benefit from autonomy 11
5.1 Scenario 1 Fault Self-Healing with Autonomy Capabilities 11
5.2 Scenario 2 Fault Management - Signalling Storm Prevention 11
6 ZSM architecture for autonomy 12
6.1 Overview 12
6.2 Architecture design objectives and principles 12
6.3 Reference Architecture evolution 12
6.3.1 Function View 12
6.3.2 Deployment and interactions in ZSM 14
6.3.2.1 Description 14
6.3.2.2 Example of procedure flows 15
7 Potential new ZSM Capabilities fulfil autonomy 16
8 Potential future work based on the present document 17
Annex A: Change history 18
History 19

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document examines the ZSM framework capabilities required to support autonomy. It highlights the differences between automation and autonomy, and the differences among levels of autonomy, through a review of published ZSM work and other industry work.

The study work is driven by scenarios that would benefit from autonomy, it includes an activity aimed at identifying the ZSM framework capabilities to fulfil autonomy.

Additionally, possible service gaps are addressed. Collaboration with and reference to other SDOs (e.g. in TM Forum, IRTF NMRG, 3GPP SA5) are recommended when appropriate.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR ZSM 005: "Zero-touch network and Service Management (ZSM); Means of Automation".

[i.2] ETSI GR ZSM 011: "Zero-touch network and Service Management (ZSM); Intent-driven autonomous networks; Generic aspects".

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

[i.4] TM Forum IG1258: "Autonomous Networks Glossary v1.2.0".

[i.5] ETSI GS ZSM 002: "Zero-touch network and Service Management (ZSM); Reference Architecture".

[i.6] ETSI GS ZSM 009-1: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 1: Enablers".

[i.7] ETSI GS ZSM 016: "Zero-touch network and Service Management (ZSM); Intent-driven Closed Loops".

[i.8] Joseph Sifakis: "Autonomous Systems - An Architectural Characterization", 2018.

[i.9] TM Forum IG1218: "Autonomous Networks Business Requirements and Framework v3.0.0".

[i.10] TM Forum IG1251A: "Autonomous Networks Reference Architecture Realizations v1.0.0".

[i.11] TM Forum IG1253: "Intent in Autonomous Networks v1.3.0".

[i.12] ETSI TS 128 312: "LTE; 5G; Management and orchestration; Intent driven management services for mobile networks (3GPP TS 28.312 Release 19)".

[i.13] ETSI TS 128 104: "5G; Management and orchestration; Management Data Analytics (MDA) (3GPP TS 28.104 version 18.4.0 Release 18)".

[i.14] ETSI TS 128 105: "5G; Management and orchestration; Artificial Intelligence/ Machine Learning (AI/ML) management (3GPP TS 28.105 version 18.4.0 Release 18)".

[i.15] ETSI TS 128 561: "5G; Management and orchestration; Management aspects of Network Digital Twins (3GPP TS 28.561 version 19.0.0 Release 19)".

[i.16] ETSI TS 123 288: "5G; Architecture enhancements for 5G System (5GS) to support network data analytics services (3GPP TS 23.288 version 18.7.0 Release 18)".

[i.17] IETF RFC 9315: "Intent-Based Networking - Concepts and Definitions".

[i.18] IETF RFC 8969: "A Framework for Automating Service and Network Management with YANG".

[i.19] IETF draft-ietf-nmop-network-incident-yang-08: "A YANG Data Model for Network Incident Management".

[i.20] ETSI GR ZSM 020: "Zero-touch network and Service Management (ZSM); Study on the Utilization of Agents in Autonomous Networks".

[i.21] ETSI GS ZSM 007: "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

autonomous networks: network and software platforms that are capable of sensing their environment, learning from it and adapting their behaviours accordingly, with little or no human input

single domain: logically bounded management scope that can fulfil closed-loop automation of specific network operations

NOTE: Within the ZSM framework, a Single Domain is defined as a Management Domain instance with autonomous capabilities.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ZSM 007 [i.21] and the following apply:

5GS	5G System
AN	Autonomous Networks
AN Levels	Autonomous Network Levels
AN L4	Autonomous Network Level 4
CCSA	China Communications Standards Association
CN	Core Network
IBN	Intent-Based Networking
IDMS	Intent-Driven Management Services
MDA	Management Data Analytics
NDT	Network Digital Twin
NWDAF	Network Data Analytics Function

OAM	Operations, Administration and Maintenance
SMF	Session Management Function
ToR	Terms of Reference
UPF	User Plane Function
YANG	Yet Another Next Generation

4 ZSM target to autonomy

4.1 Concept of autonomy

"*Automation is the action of making a task executable without human intervention. It is realized by introducing new automatic functions or by replacing, modifying or augmenting manual functions with automation artifacts (e.g. a script executing a series of commands)*" (ETSI GR ZSM 005 [i.1]). A comprehensive automation provides an approach for combining function automation (e.g. combination or chaining of the functions that collectively achieve the closed loop automation) with process automation (e.g. operational processes such as service creation, assurance and optimization, etc.).

Automation refers to "*the use of machines and computers that can operate without needing human control*", on the other hand, autonomy implies "*the capability to make decisions free from human control*" (TM Forum IG1258 [i.4]).

In [i.8], autonomous agent is defined as "*the capacity of an agent to achieve a set of coordinated goals by its own means (without human intervention) adapting to environment variations*".

The ZSM framework of course supports automation of network operations. Closed loops, in their most basic form, achieve automation by linking perception to analysis, decision making and action. However, when perception, analytical and decision-making processes are fixed, the closed loop is only able to operate within that range of contexts and circumstances for which those fixed processes generate effective outcomes. If context or circumstances change sufficiently, then elements of the closed loop should be redesigned in order that the closed loop can function effectively. Such redesign may include changing elements and means of perception, of methods of analysis, of methods and bases for decision making, or of actuation of decisions taken.

Fundamentally, the ability of systems flexibly to adapt to new, changing or unforeseen problems, contexts and circumstances, without human intervention, lies at the heart of the distinction between autonomy and "mere" automation. This view is widely held across the inter-linked fields of cognitive science, philosophy of mind, and AI. Somewhat more generally, the gap between automation and autonomy is linked to cognition, a capability which is imperfectly described across these fields, but broadly held to encompass at least two others: reasoning and learning. Reasoning is, itself, somewhat imperfectly defined as - in essence - those capacities needed to find or design effective solutions to new or evolving problems. Learning refers to improving reasoning outcomes through acquisition and use of new knowledge.

Aspects of these concepts - for example, the inclusion and utility of knowledge within closed loop structures, and the complementing of operational (automation) closed loops with cognitive closed loops supporting adaptation - have been developed within ZSM work. However, the role and use of reasoning and learning have not been fully developed or described within ZSM work to date, in significant part because technology supporting these capabilities - specifically and first, generative AI - was not available and broadly understood until relatively recently. Conceptually, autonomy is now generally linked - for good reason - to such technologies.

To summarize, within the ZSM frameworks, autonomy refers to the system's capability to achieve goals by its own means - encompassing decision-making, service orchestration, and service lifecycle management, etc. - without human intervention, while adapting to variations of network and its environment.

4.2 Differences between automation and autonomy

In the context of network and service management, there are various interpretations regarding the distinction between automation and autonomy. For instance, automation + intelligence (as the cognitive closed loop defined in ETSI GR ZSM 009-3 [i.3], clause 5.1) may be considered as autonomy. To facilitate clearer differentiation, it is recommended to list some of the distinctions along several dimensions, such as:

- Operator experience: automation is predictable and reliable, with clearly defined and expected outcomes. While autonomy is adaptive but less predictable, it dynamically adjusts behaviour.
- Decision-making mechanism: automation generally is rule-based, or at least, is designed to work properly only within a constrained set of circumstances. Those circumstances should be anticipated and reflected at the point of design. Whereas autonomy can enable dynamic decision-making through self-learning and goal management capabilities (herein referred to as Choice-Making).
- Environmental adaption: automated processes may be expected to perform within constrained environmental circumstances. Autonomous systems, on the other hand, can cope with environmental change, uncertainty or unpredictability.

4.3 High-Level Description of autonomous system

ZSM has been actively working on reducing the human intervention of network and service management automation, and progressing toward the full automation. While the ultimate objective is to achieve autonomy, the ZSM framework can be considered as an autonomous system, which should be designed to enhance operational capabilities by self-awareness, autonomous decision-making and self-learning mechanisms to handle the complexity and dynamics of networks, while minimizing the need of human intervention.

Intent management, closed-loop automation, knowledge serve as the fundamental functions in the ZSM framework. The closed-loop mechanism is designed to fulfil individual intents and resolve issues detected from environment automatically. ETSI GR ZSM 011 [i.2] further explores various potential intent conflicts and resolution approaches (e.g. set priorities, set utility-goals,), however, managing multi-intent conflicts remains an ongoing challenge. Additionally, automation system often struggles to detect sub-threshold deterioration before it escalates into faults.

Autonomy is considered to address these challenges and the dual closed-loop mechanism (shown in Figure 4.3-1) can be a potential explanation to explore a way forward to autonomy, in which, the closed-loop (Monitor-Analysis-Decision-Execution) automation plus knowledge reflects responses to inputs such as intents and incoming events (ETSI GS ZSM 009-1 [i.6]), this is referred to as a Reactive Closed-loop. Meanwhile, self-awareness is used to recognize potential risks and threats, and choice-making selects the most suitable goal. These functions enable learning and adaptation capabilities - by leveraging and continuously updating knowledge - thereby forming a Proactive Closed-loop.

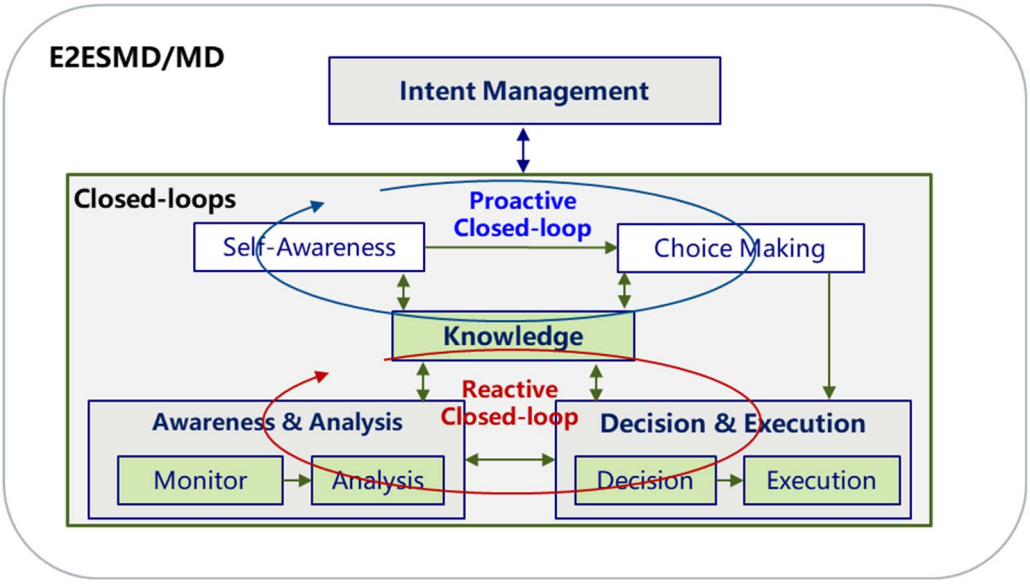

Figure 4.3-1: Closed-loops for autonomy

A designed reactive closed loop serves as the foundational mechanism for operation automation, whereas the proactive closed loop is triggered by changes in knowledge - beginning with new knowledge of some inadequacy of the reactive closed loop. This drives a redesign of the reactive closed loop. For example, when a known issue "a user reports video stuttering and performance anomalies are detected in a specific path" is detected by a violation of implemented KPIs, the reactive CL accommodates using established designed reactions. In this case, the root cause analysis and linked decision-making are within design bounds. However, when facing a new issue such as "a user reports video stuttering while all KPIs appear normal", the designed reactive closed loop cannot resolve the problem. In this case, the proactive CL would activate its reasoning capabilities to infer potential causes and subsequently update the decision-making and action outcomes: in effect, re-designing the reactive closed loop.

4.4 The progress of Network Automation

4.4.1 Review of ZSM work

This clause reviews existing ZSM work for network and service management automation, based on which a gap analysis between the existing automation work and target autonomy capabilities will be conducted.

As defined in ZSM ToR, the goal of ZSM is to have all operational processes (e.g. delivery, deployment, orchestration, configuration, assurance, and optimization) executed automatically, ideally with fully automated.

ETSI GS ZSM 002 [i.5] defines the ZSM framework which is versatile and built on service-based principles offering scalability, modularity, extensibility, and flexibility, provides capabilities to integrate AI-based functionalities and enable closed-loop automation.

ETSI GS ZSM 009-1 [i.6] introduces a structured feedback loop between data monitoring, data analytics, decision-making and actions, which aims to reach and preserve a set of objectives without external intervention, and within which the automated decision-making mechanisms can be bounded by rules and policies.

ZSM framework also takes advantage of emerging technologies to increase network and services management automation and efficiency. For example, AI/ML, Network Digital Twin can enhance analytics and decision-making to empower the closed-loop operation. In addition, the closed-loop automation is governed by policies, rules, intents and/or other forms of inputs that guide its behaviour.

Figure 4.4-1 shows the concepts related to service and network automation, in which intent (ETSI GR ZSM 011 [i.2], intent-driven autonomous networks) allows human network operators to convey requirements of network (i.e. SLA). Intent management can translate intents into internal goals, which are the inputs of service life cycle management automation and closed loop automation, AI technology may be able to increase the "intelligence" regarding learning based, adaptiveness of automated systems. Some stages of service life cycle management automation or closed loop automation depend on Network Digital Twin to determine the expected outcomes, impacts and effects.

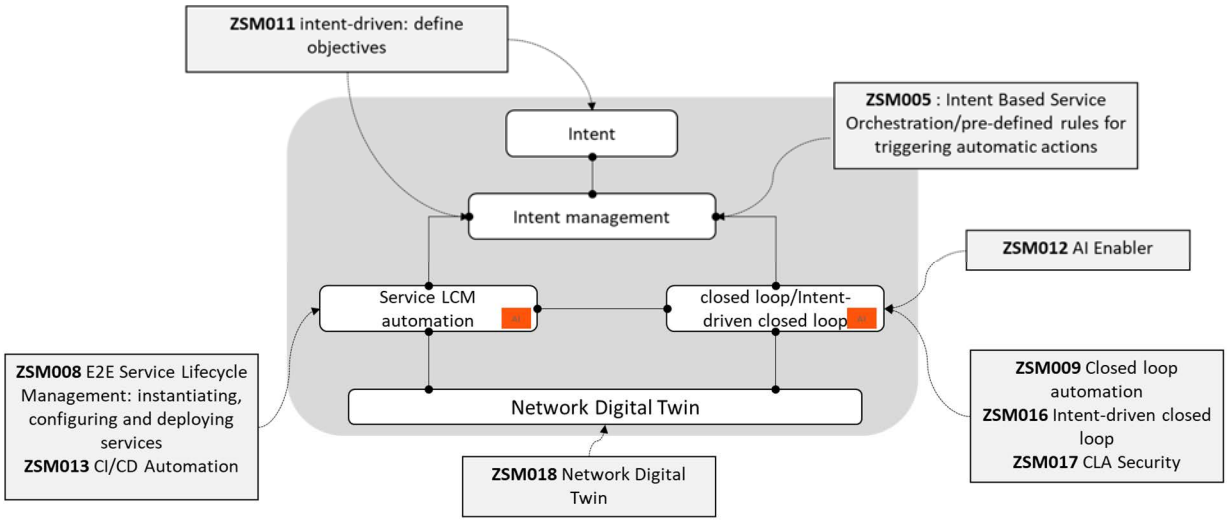

Figure 4.4-1: Concepts of ZSM automation

4.4.2 Review of industry work

4.4.2.1 Introduction

The evolution of automation in communication networks aims to address the complexity of operation networks through closed-loop automation, intent-driven management, and AI/ML technologies. Following are analyses of some standards developments and industry practices in this field.

4.4.2.2 Standardization of the Network Automation and Autonomy

TMF defines the Autonomous Networks (AN) vision (TM Forum IG1218 [i.9]), which describes the evolution from "automation" to "autonomous" through the Autonomous Network Levels (AN Levels), transitioning from rule-based process automation to intelligent, closed-loop autonomy:

- AN Reference Architecture (TM Forum IG1251A [i.10]): Defining a three-layer architecture (Business, Service, Resource Operations) for Autonomous Networks. Each layer contains closed-loop automation capabilities, interacts via intent-driven APIs, implements Awareness-Analysis-Decision-Execution cycles within multiple Autonomous (self-governing) Domains, supported by AI/ML technologies.

- Intent In AN (TM Forum IG1253 [i.11]): Defining an architecture for intent management, intent modelling, and intent APIs.

3GPP SA5&SA2 have advanced Mobile Network Automation through specifications such as:

- Intent-Driven Management Services (IDMS) (ETSI TS 128 312 [i.12]): Defining a framework for intent-driven management, which can translate high-level business or operational intents into automated network configurations and actions, to enhance network efficiency and user experiences.

- Management Data Analytics (MDA) (ETSI TS 128 104 [i.13]): Defining a framework to process and analyse diverse network management data (e.g. performance metrics, alarms, and configuration data) to generate actionable insights like predictions, root cause analysis, and operational recommendations, enables operators to predict network operations. MDA can also enhance network efficiency by supporting cross-domain coordination between RAN, CN, and NWDAF, facilitating closed-loop automation.

- AI/ML Management (ETSI TS 128 105 [i.14]): Defining a framework for ML model lifecycle management in 5GS (including 5GC, NG-RAN, and management system), which enables and facilitates the AI/ML capabilities with the suitable AI/ML techniques in 5GS, addressing management challenges during ML model training, ML model testing, AI/ML inference emulation, ML model deployment and AI/ML inference.

- Network Digital Twin (NDT) (ETSI TS 128 561 [i.15]): Defining a framework to enable network simulation/emulation, support prediction of network failure and risk, and generate ML training data for ML models.

- Network Data Analytics Function (NWDAF) (ETSI TS 123 288 [i.16]): Defining a functional component to collect, process, and analyse network data from various sources (e.g. AMF, SMF, UPF, OAM) to generate analytics and support AI/ML-based decision-making.

IETF also has network automation specifications such as:

- Intent-Based Networking (IBN) (IETF RFC 9315 [i.17]): Defining a framework for intent-based networking, which defines "intent" as high-level declarative operational goals, differentiates it from policy and service models, and specifies core principles (e.g. Single Source of Truth, learning capability) and functionalities (fulfilment and assurance) to enable automated network management focused on achieving desired outcomes with minimal human intervention.

- A Framework for Automating Service and Network Management with YANG (IETF RFC 8969 [i.18]): Defining a framework for service and network management automation that leverages YANG data modelling technologies and SDN techniques to address challenges like the lack of standard data models and limited network visibility in legacy OSS/BSS systems, enabling vendor-agnostic integration, dynamic resource allocation, policy enforcement, and multi-layer model interaction for efficient service delivery and fulfilment.

China Communications Standards Association (CCSA), Technical Committee 7 also has a working group working on the standardization of advancing autonomous network architectures, as well as emerging technologies, for instance, intent, foundation model, which aligns with global trends while addressing China's unique industry demands, with ongoing standardization efforts aimed at achieving AN L4.

4.4.3 Review Summary

As investigated in the present document, several SDOs working on Network and Service Management primarily focus on closed-loop automation, with the aim of minimizing human intervention to achieve single objective within a constrained set of circumstances. When it comes to complex systems, however, the specification of even a simple single objective presents significant challenges. Consider, for example, an employer wants to replace a cleaning staff with a robot. What kinds of the objective specifications should be? Should it be action-oriented (e.g. where and how to sweep), object-oriented (e.g. what kinds of dirt, dust and hair, etc., should be removed), or result-oriented (e.g. what should the floors and shelves look like once the job is done)?

In operational environments, the telecommunications network system has to deal with multiple objectives, beyond the difficulty of specifying each objective separately, it is still very difficult to specify how the system should balance, prioritize, or weigh the competing objectives under dynamic changeable circumstances.

Regarding these challenges, the standardization work of exploring a transition from closed-loop automation to autonomous systems is essential. Such as, adopting and harmonizing specifications from different SDOs for extracting objectives through right intents, establishing weight allocation, prioritization, and mutual constraints across multiple objectives, and enhancing system capabilities of reacting to and handling negative conditions directly related to the system's own decisions and actions, etc.

5 Scenarios that benefit from autonomy

5.1 Scenario 1 Fault Self-Healing with Autonomy Capabilities

Network autonomy introduces a substantial enhancement to the self-healing capabilities of AN systems.

In autonomous networks, intelligence applications based on AI models are evolving from the role of supporting tools to that of core executors, particularly with the integration of generative AI models.

When applied to fault self-healing, these intelligence applications exhibit proactive intelligence: in fault analysis phase, different domain intelligence applications can autonomously orchestrate single/multi-domain collaboration to isolate and locate faults; and in fault resolution phase, they can generate repair strategies, execute corrections through multi-round analytical reasoning communications with each other, and continuously self-learning from outcomes.

This end-to-end autonomy enables highly efficient, human-free fault self-healing, resulting in a paradigm shift from reactive maintenance to proactive, self-optimizing network resilience.

NOTE: The intelligence applications mentioned in this scenario can correspond to Agents in ETSI GR ZSM 020 [i.20].

5.2 Scenario 2 Fault Management - Signalling Storm Prevention

When a mobile service disruption occurs, massive repeated reconnection attempts from User Equipment (UE) may be triggered, potentially causing a signalling storm. If the signalling storm induces network equipment anomalies, the impact may propagate, resulting in large-scale user complaints.

At the stage of receiving an issue, the Closed-loop automation of management domain (e.g. core network domain) initiates fault analysis and mitigation actions in response to the issue, the typical fault mitigation approaches involve controlling the flow of upstream network equipment in accordance with preconfigured rules, switching service to predefined standby or disaster recovery paths, etc.

Leveraging autonomous capabilities in the management domain, potential risks caused by mobile service interruption will be recognized in advance through identifying deviations between predicted and actual traffic (capability of Self-Awareness as defined in clause 4.3). This enables the system to recognize "something wrong has happened" before the user complaints arise, thereby demonstrating predictive functionality. Rather than initiating, the Choice-Making function (part of Proactive Closed-loop as defined in clause 4.3) employs predictive modelling for evaluation and recommendation, prior to conducting immediate Root Cause Analysis (RCA) to determine the underlying issue. This process involves evaluating the potential impacts, followed by generating prioritized recommendations to either repair the risks or mitigate the impacts. Based on the priority, the decision may be made as applying flow control with an optimal parameter to mitigate potential signalling storms, in alignment with the meta-goal of "maintaining network stability".

NOTE: In the present document, a meta-goal refers to an abstract representation of the fundamental intent guiding network and service management to achieve desired operational outcomes, e.g. ensure service continuity.

6 ZSM architecture for autonomy

6.1 Overview

In the context of network and service management, the transition from automation to autonomy means enabling operational processes with minimal or no human intervention under new, changing, or unanticipated circumstances. Exploring ZSM architecture evolution for autonomy aims to guide human operators to focus on strategic objectives, goal definition, intent refinement, and knowledge provisioning. Furthermore, the architecture may facilitate the evolution of development methodologies from traditional model-based approaches toward more adaptive paradigms.

6.2 Architecture design objectives and principles

ETSI GS ZSM 002 [i.5], clause 4 introduced a set of architecture principles, aiming to guide the way of designing the ZSM architecture to allow fully automated network and service management. To enable autonomous network and service management in the ZSM framework, these principles can be extended to guide an agentic autonomy on development, implementation, and functional behaviour aspects:

1) Hierarchical autonomy: the architecture can be instantiated as agents at different network hierarchical layers (based on ETSI GS ZSM 002 [i.5], clause 4.2.8, Principle 08: Separation of concerns in management). Every agent can perform closed-loop operations as needed.

2) Adaptive Learning: continuously improve behaviour based on feedback.

3) Technology agnostic solution: clause 4.2.8 of ETSI GS ZSM 002 [i.5] defined model-driven and open interfaces in principle 04, the autonomy is no restrictions on implementations, which can range from monolithic AI-based architectures to hybrid architectures integrating model- and data-driven components.

4) Collaboration by interoperability: the interaction between agents and other agents serves collaboration on fulfilling operational and management intents autonomously.

6.3 Reference Architecture evolution

6.3.1 Function View

This clause aims to propose a reference architecture in which the incremental functions - applicable to the evolution towards autonomy - can be identifiable and implementable.

Clause 4.2 introduced self-awareness and choice-making functions, enhancing the ZSM framework with learning, adaptation and interaction, etc. capabilities. These functions combined with ZSM architectural components that are necessary for realizing Closed Loops (as defined in ETSI GS ZSM 009-1 [i.6]), can be illustrated as an Autonomous Agent (as defined in ETSI GR ZSM 020 [i.20]), as shown in Figure 6.3-1.

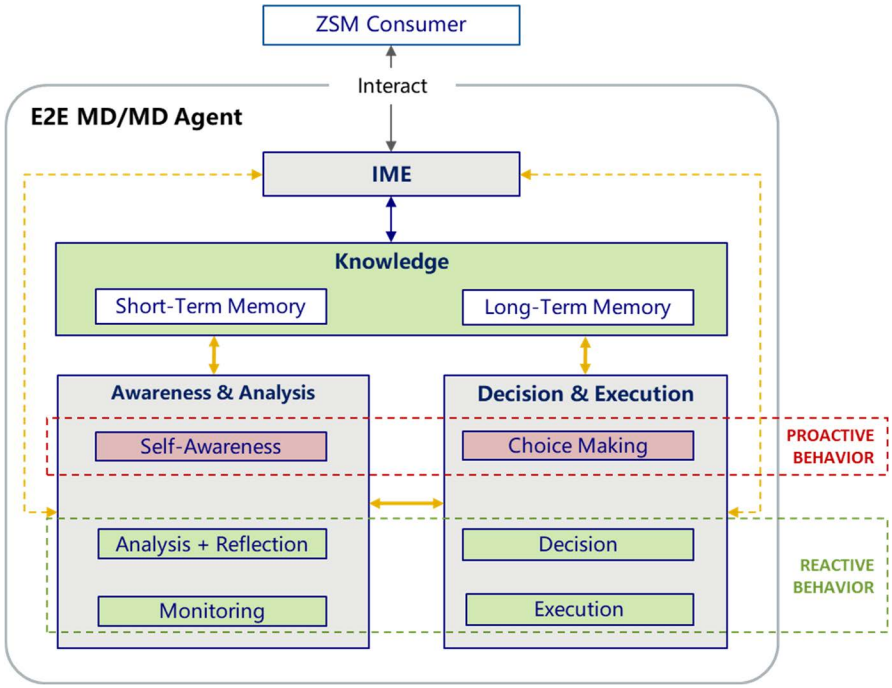

Figure 6.3-1: Function View of Core Functional Components for Autonomous Architecture

Closed-Loop Automation (Monitoring, Analysis, Decision, Execution, Knowledge) is the fundamental mechanism in the ZSM framework.

This functional view presents the key features for expanding the Closed-Loop Automation:

1) Separation of Reactive and Proactive Behaviours:

   - Reactive Behaviour (Green): immediate responses to environmental input, enabled through monitoring, analysis, reflection, decision and execution. Reflection queries the knowledge to interpret monitoring and analysis data with a broader context, updating predictive models (e.g. Network Digital Twin models).

   - Proactive Behaviour (Red): higher-level reasoning processes, including also self-awareness and choice-making to drive long-term strategy. Self-Awareness refers to the self-assessment mechanisms which enable the learning-based adaptation. Choice-Making chooses the most suitable goal among a set of goals based on the comprehensive evaluation, for example, cost-benefit analysis, priority evaluation, etc.

2) Integrated Self-Awareness Module:

   - Previous architectures lacked structured self-assessment mechanisms, meaning adaptability was limited to predefined scenarios. This model introduces the capability of comparing the operational state with the desired state continuously to evaluate intent fulfilment, enabling system to reason about its own objectives dynamically.

3) Expanded Knowledge Module:

   - Knowledge refers to the comprehensive collection of information, facts, rules, and heuristics that facilitate analysis, decision-making etc., it can be expanded to Short-Term Memory and Long-Term Memory:

     - Short-Term Memory: maintains active and readily available information as symbolic variables for the current decision cycle. This includes perceptual inputs, active knowledge (generated by reasoning or retrieved from long-term memory), and other core information carried over from the previous decision cycle (e.g. agent's active goals, intents, etc.).

     - Long-Term Memory: it is persisted in order to last longer than the agent's lifetime, and it contains different types of knowledge both specific to an agent or more generally shared between multiple agents.

- ZSM architecture historically relied on real-time analytics, this model allows for experience-driven decision-making, enabling more sophisticated learning-based adaptation.

4) Explicit Differentiation of Reflection and Decision-Making:

- The analysis extends with reflection to incorporate predictive modelling, allowing system to anticipate environmental changes rather than simply reacting to them.

- Previous architectures often merged reflection with decision loops, making it difficult to establish long-term adaptation strategies. This model separates immediate reactions from strategic planning, supporting both real-time control and long-term evolution.

6.3.2 Deployment and interactions in ZSM

6.3.2.1 Description

The ZSM framework should support the separation of concerns in autonomy in management domain and end-to-end management. Figure 6.3-2 below illustrates a typical deployment and interaction relationships in terms of hierarchical autonomy.

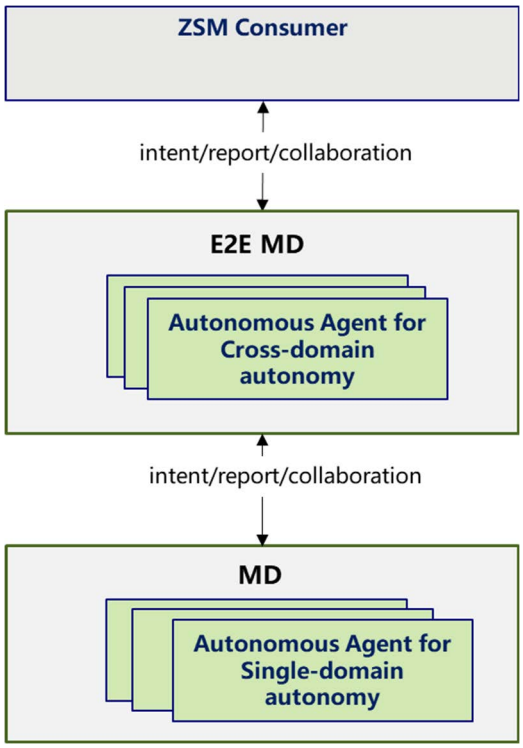

Figure 6.3-2: Deployment view of Autonomous Agents in ZSM framework

A Management Domain (MD) is responsible for the single-domain autonomy, while the End-to-End Service Management Domain (E2ES MD) is responsible for cross-domain autonomy. Domains and the end-to-end service management domain may collaborate to achieve collective objectives. Agents implemented in MDs or the E2ES MD may work together to handle complex tasks that are beyond the scope or capabilities of individual agents.

It should be noted that the intent concept, as described in ETSI GR ZSM 011 [i.2] and ETSI GS ZSM 016 [i.7], in effect treats entire MDs, as agents capable of and responsible for autonomous fulfilment of network service objectives given to them via an interface. This is reflected in the fact that the intent fulfilment structure given in ETSI GS ZSM 016 [i.7], there mapped to the ZSM architecture and other ZSM constructs, is identical to the agent structure given in the present document and in ETSI GR ZSM 020 [i.20]. Intent mechanisms supporting communication and negotiation of objectives, and reporting of their fulfilment status, therefore represent one basis and mechanism for inter-agent collaboration. Other inter-agent collaboration mechanisms might map, in effect, to less functionally comprehensive management functions and services or their equivalents, for example, comprising data services, or data and analytical services.

6.3.2.2 Example of procedure flows

As shown in Figure 6.3-3, an example illustrates how intent and collaboration can be used to interact between different domains in a network and service assurance scenario. The steps shown in Figure 6.3-3 are as follows:

Steps 1-2: Single-domain agent continuously detects the anomaly or deterioration (e.g. performance degradation, traffic anomaly) based on the analysis of collected data, including detect the deviation of real collected data and predicted data.

Steps 3-4a/4b: The single-domain agent attempts recovery with autonomous workflow orchestration, if successful, it notifies the Cross-domain agent via step 4a. If not, the Cross-domain agent will be notified with adequate information via step 4b. The interface used in steps 4a/4b may employ intent report (as defined in ETSI GS ZSM 016 [i.7]) or incident (as defined in IETF draft-ietf-nmop-network-incident-yang-08 [i.19]).

Steps 5-6: Leveraging cross-domain knowledge, the cross-domain agent performs comprehensive analysis and coordinates with relevant single-domain agents, including identifying suitable agent, negotiating task objectives, and distributing task accordingly.

Steps 7-8: The single-domain agent performs using comprehensive information from both the cross-domain agent and other domain agents.

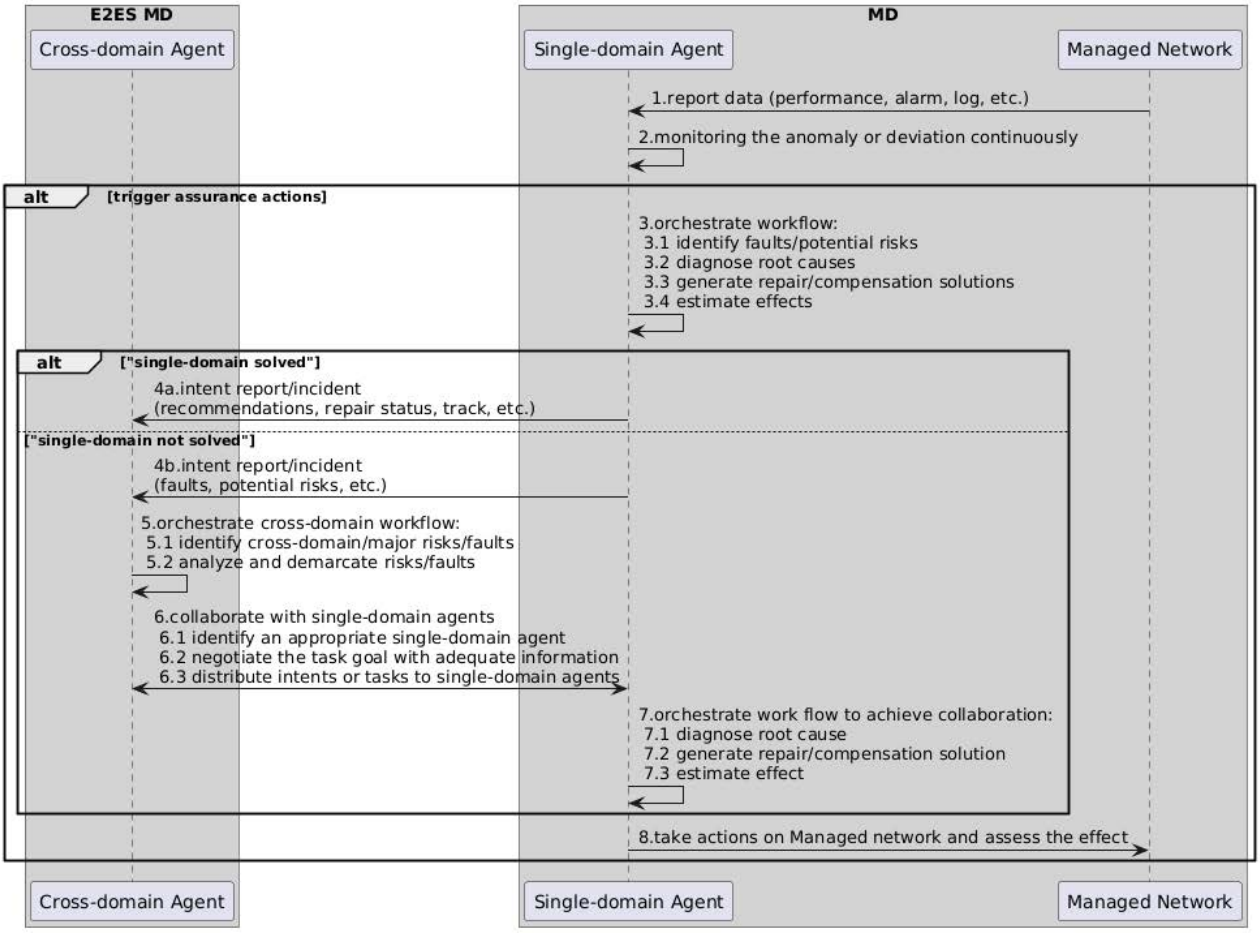

Figure 6.3-3: Example of interaction with autonomy in ZSM framework

7 Potential new ZSM Capabilities fulfil autonomy

As previously stated, the evolution of the ZSM framework from automation towards autonomy necessitates the capability for autonomous decision-making and action based on self-awareness and choice-making capabilities. This autonomy requires ZSM framework can cope with environmental change, uncertainty or unpredictability, thereby enhancing the overall operational efficiency and stability of the system. Furthermore, the achievement of more complex tasks necessitates collective intelligence, which emerges from the collaboration and interaction among multiple autonomous agents.

The following requirements have been extracted from the scenarios described in clause 5.

In clause 6.5.5 and clause 6.6.5 in ETSI GS ZSM 002 [i.5], orchestration services can "allow authorized consumers to instantiate and maintain domain-level network services, including creation, modification and termination of the services, and allows the automation of corresponding workflows". Such services can be extended to meet the autonomous networks requirements.

Capability-7.1: It is recommended that the ZSM framework provides the capability of autonomous orchestration for services (including RFS and CFS) exposed from management domains and CFS across multiple management domains.

As defined in clause 6.5.3 and clause 6.6.3 in ETSI GS ZSM 002 [i.5], analytics services are responsible for providing insights and generating predictions, which are critical capabilities for closed-loop automation. Furthermore, self-awareness should constitute an essential functional component within the ZSM framework to enable proactive autonomous operations to transcend mere reactive responses based on the analysis of environmental inputs.

Capability-7.2: It is recommended that the ZSM framework provides the capability to implement the proactive behaviour by utilizing self-awareness functionality.

NOTE 1: Self-awareness refers to awareness of the internal state of the agent and the perceived state of the network, thus it is the agent current understanding of the environment. This allows the agent to forecast potential risks and plan remediation actions to mitigate such risks.

Based on the scenario defined in clause 5.2, signal storms can be prevented through proactive handling.

Capability-7.3: ZSM Framework should support the capability to report the potential risks and to provide mitigation recommendations for impact reduction.

NOTE 2: "Potential risk" refers to future events or conditions possessing a specific probability of occurrence that can cause the network state to deviate from its management intent or Service Level Agreements (SLAs).

As defined in clause 4.1, autonomy of ZSM frameworks refers to the system's capability to achieve goals by its own means. The ZSM framework needs to establish robust "guardrail" mechanisms, these include: defining strict policies to limit dangerous agent actions (e.g. "set a maximum cost ceiling for the scaling operations of each service"), real-time monitoring of anomalous deviations in agent decisions, and implementing an "emergency stop" function.

Capability-7.4: It is recommended that the ZSM framework provides the capability to define safety policies and "guardrail" mechanisms to enforce operational boundaries for autonomous agents.

In clause 6.5.4 and clause 6.6.4 in ETSI GS ZSM 002 [i.5], intelligence services are responsible for driving intelligent closed-loop automation in the E2ES MD or MD by supporting multiple levels of automated decision-making and human oversight with fully autonomous management being the final stage. Autonomous systems are expected to achieve fully autonomous management without human supervision across multiple intent-driven closed loops in the E2ES MD or MD by leveraging knowledge and reasoning, even in unanticipated operational circumstances.

Capability-7.5: It is recommended that the ZSM framework provides the capability to update knowledge through feedback and learning, and to use reasoning to make knowledge-based decisions, interpretations, new designs and new plans.

Capability-7.6: It is recommended that the ZSM framework provides the capability to explain and trace the origins and basis of autonomous knowledge-based decisions, interpretations, re-designs and new plans.

8 Potential future work based on the present document

The ZSM framework needs to support an evolution from siloed automation towards autonomous network systems. This autonomy is agent-based and collaborative: each agent fulfils specific objectives and goals, and through coordination with other agents, it contributes to realization of the provided intents. Therefore, the correctness of an agent's behaviour also depends on its ability to coordinate with other agents in such a way that its actions not only do not prevent other agents from achieving their goals, but also create the synergies needed to satisfy global objectives:

- The present document describes capability requirements supporting autonomous orchestration of exposed services and resources. Further investigation is required to specify the orchestration processes and functional behaviours in greater detail.
- The standardization of collaboration and interaction among multiple autonomous agents, to achieve collaborative intelligence within an MD or across MDs, can be explored.
- Addressing the combination of the ZSM framework integration mechanism with agent autonomous orchestration to facilitate an evolutionary development path towards a dynamic architecture of the ZSM framework may be explored. This evolution may lead to a dynamic architecture, for example:
  - Temporal dynamism: the number of agents and their interactions can change over time, for example when agents and their interactions are created or deleted.
  - Spatial dynamism: agents' behaviour changes according to their position in space. This is the case with mobile agents.
  - Organizational dynamism: agents change their behaviour according to their position in the organization of the system.
- Exploring the integration of declarative intent, network digital twin, AI and emerging protocols with or within autonomous agents to facilitate system cognition, adaptive decision-making and efficient collaboration.
- Exploring ways to achieve high efficiency in interactions between autonomous agent and their surroundings, including agent-to-user, agent-to-agent, agent-to-tool interactions and observability/security, etc.
- Exploring the value creation potential of, and implementation paradigms for, higher autonomy, which is expected to redefine telecommunications and to significantly enhance the experience of network subscribers, vertical industries, and telecom operators.

Annex A:
Change history

Date	Version	Information about changes
21 May 2025	V0.0.2	ZSM(25)000049r3 ZSM021_4.1 Concept ZSM(25)000050r3 ZSM021_Clause 4.4.1 Review of ZSM work ZSM(25)000051r2 ZSM021_Clause 2 References ZSM(25)000064r3 ZSM021_Clause 4.3 High level description
15 July 2025	V0.1.0	ZSM(25)000052r1 ZSM021_Clause 4.2 Difference ZSM(25)000078r3 ZSM021 Review of industry work for automation ZSM(25)000079r2 ZSM021 Wireless Network Fault Handling Scenario for Autonomy ZSM(25)000093r3 ZSM021_Clause_5_Signaling storm prediction ZSM(25)000100 ZSM021_Clause 4 Gap analysis ZSM(25)000103r1 ZSM021_Clause 6.1 Architecture principles ZSM(25)000104r1 ZSM021 Review of industry work for automation ZSM(25)000113r2 ZSM021_Clause_6.2_Architecture function view ZSM(25)000119r1 ZSM021_Autonomy_terms ZSM(25)000120r1 ZSM021_Clause 6 Architecture Overview ZSM(25)000122r1 ZSM21_Clause_6.2 Deployment and interactions ZSM(25)000124r1 ZSM021_Clause_6.2_interactions example ZSM(25)000126r1 CR for ZSM021 Wireless Network Fault Handling Scenario for Autonomy
26 Nov 2025	V0.1.1	ZSM(25)000186 ZSM021 Change to 4.4 Review of industry work for automation ZSM(25)000187r2 ZSM021_Clause_7_capability of orchestration ZSM(25)000189r2 ZSM021_Clause_7_capability of choice making ZSM(25)000121r1 ZSM021_Clause 7 Potential ZSM Capabilities to support autonomy ZSM(25)000188r2 ZSM021_Clause_7_capability of assess risk ZSM(25)000249r1 ZSM021_Clause_4_3_example_of_reactive_and_proactive_CLZSM(25)000245r1 ZSM021_Clause_7_capability of autonomous decision-making
23 March 2026	V0.1.2	ZSM(25)000191r5_ZSM021_Clause_8_future_work ZSM(26)000025r1_ZSM_021_Automation_versus_Autonomy
9 April 2026	V0.1.3	Editorial changes
13 April 2026	V0.1.4	Editorial changes, update abbreviations

History

Version	Date	Status
V1.1.1	May 2026	Publication