ETSI GR ENI 007 V1.1.1 (2019-11)

GROUP REPORT

Experiential Networked Intelligence (ENI);
ENI Definition of Categories for AI Application to Networks

Disclaimer

The present document has been produced and approved by the Experiential Networked Intelligence (ENI) 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/ENI-0011

Keywords

artificial intelligence, categorization, category,
network

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 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 Overview 6
4.1 Background on AI integration and network autonomicity 6
4.2 Examples of application in specific areas..8
4.2.1 Automation applied to vehicle driving...8
4.2.2 Autonomicity applied to home broadband services 9

5 Categories of Network Autonomicity 10
5.1 Introduction 10
5.2 Factors determining the network autonomicity level 11
5.2.1 Technical factors...11
5.2.2 Market factors 12
5.3 Network autonomicity categories description 12
5.4 Tabular representation of Network Autonomicity categories..13
5.5 Scenario Examples of Network Autonomicity categories 16
5.5.1 Introduction...16
5.5.2 Autonomicity categories of network traffic classification 16
5.5.3 Autonomicity categories of IDC energy management...19
5.5.4 Autonomicity categories for network fault recovery 21
5.5.5 Autonomicity categories of DCN service and resource design...24
5.5.6 Autonomicity categories of DCN service quality optimization 27
5.5.7 Autonomicity categories of End-to-End service quality assurance in bearer network.......................30

6 Relation of the Autonomicity Categories to ENI system architecture and other architectures 33
6.1 Introduction 33
6.2 Mapping of Assisted System Classes into Network Autonomicity Categories 33

7 Conclusions 35

Annex A: **Related work published by other SDOs..36**

History 37

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 Report (GR) has been produced by ETSI Industry Specification Group (ISG) Experiential Networked Intelligence (ENI).

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 defines various categories for the level of application of Artificial Intelligence (AI) techniques to the management of the network, going from basic limited aspects, to the full use of AI techniques for performing network management.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] ETSI GS NFV 003 (V1.3.1): "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.2] MEF PDO CfC (V0.8): "Policy-Driven Orchestration", September 2019.

[i.3] ETSI GS ENI 001 (V2.1.1): "Experiential Networked Intelligence (ENI); ENI use cases".

[i.4] MEF 55: "Lifecycle Service Orchestration (LSO): Reference Architecture and Framework", March 2016.

[i.5] MEF MCM 78: "MEF Core Model", September 2019.

[i.6] Gamma E., Helm R., Johnson R. and Vlissides J.: "Design Patterns: Elements of Reusable Object-Oriented Software", Addison-Wesley, November 1994. ISBN 978-0201633610.

[i.7] ISO/IEC 2382-28: "Information technology -- Vocabulary".

[i.8] ISO/IEC/IEEE 42010: "Systems and software engineering -- Architecture description".

[i.9] ETSI GR ENI 004: "Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI".

[i.10] ETSI GS ENI 005 (V1.1.1): "Experiential Networked Intelligence (ENI); System Architecture".

[i.11] ETSI GS ENI 002 (V2.1.1): "Experiential Networked Intelligence (ENI); ENI requirements", September 2019.

[i.12] ETSI GR ENI 003 (V1.1.1): "Experiential Networked Intelligence (ENI); Context-Aware Policy Management Gap Analysis", May 2018.

[i.13] TM Forum whitepaper of Autonomous Networks: "Empowering Digital Transformation For The Telecoms Industry".

NOTE: Available at https://www.tmforum.org/wp-content/uploads/2019/05/22553-Autonomous-Networks-whitepaper.pdf.

[i.14] 5G-PPP White Paper: "5G Automotive Vision", October 20, 2015.
SAE document J3016: 'Taxonomy and Definitions for Terms Related to On-Road Automated Vehicles", January 16, 2014.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR ENI 004 [i.9] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR ENI 004 [i.9] apply.

4 Overview

4.1 Background on AI integration and network autonomicity

ETSI ISG ENI defines how Artificial Intelligence (AI) can be usefully applied in telecommunication networks to support the management objectives of operators. These include making management faster, more efficient and providing higher resilience and reliability of the infrastructure and of the services delivered to end-users.

AI can make Operation and Maintenance (O&M) of a traditional network much more efficient with significant cost savings. AI application for early fault discovery and location, for instance, can enhance the performance of the network as perceived by end-users as well as by the operator, and reduce fault detection and recovery costs for the operator; this will in turn reduce loss of income due to service unavailability and from the reduction of maintenance costs thanks to early fault discovery and location.

The transition to virtual networks will further enhance the benefits of AI application. AI can support network entities as orchestrators and provide different ranges of management, from assisting and recommending changes (but not actually performing changes), to performing only those changes that are trusted by the operator, to performing changes without human intervention. AI can enable the dynamic adaptation of resources to changing traffic conditions and business goals, and even enable trusted changes without human intervention; this produces a fully self-managed network in normal conditions. If extraordinary conditions (e.g. when the network exhibits complex faults or is under attack), external (manual) intervention is required (though the AI can provide recommendations for fixing problems).

Figure 1 illustrates the expected step-by-step evolution of networks as AI is integrated into them as well as trusted by operators.

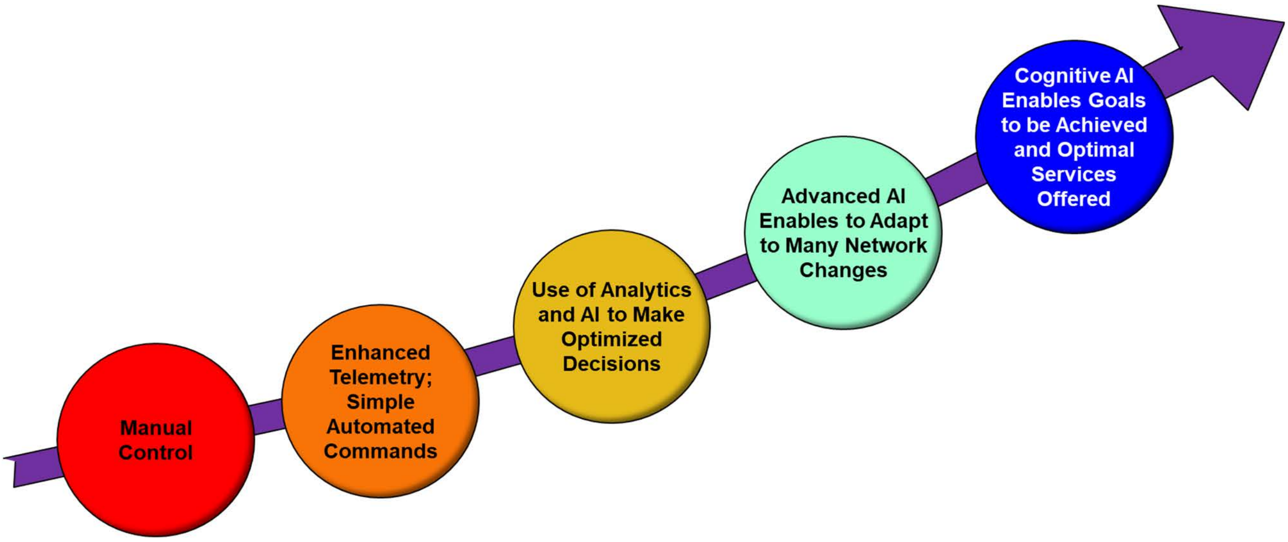

Manual Control
Enhanced Telemetry; Simple Automated Commands
Use of Analytics and AI to Make Optimized Decisions
Advanced AI Enables to Adapt to Many Network Changes
Cognitive AI Enables Goals to be Achieved and Optimal Services Offered

Figure 1: Scenarios of network evolution with the integration of AI

Figure 1 shows how the gradual introduction of increased AI functionality enables more management and control decisions to be enhanced and made with increasingly less human intervention. Most importantly, the use of AI enables many other functionalities to operate with increased accuracy and effectiveness.

- The traditional implementation of network control and management, with no AI and essentially no automation is not shown in the figure.

- Manual control requires complete human intervention. Even if AI is present, it is up to the human to make all decisions and issue all commands. This is sometimes called reactive processing (see clause 4.5.4.2 of ETSI GS ENI 005 [i.10]).

- The first step of using AI has two notable effects. First, it enhances existing telemetry by interacting with the network and ensuring that the most applicable telemetry is provided for a given context. Second, it enables the human to trust its recommendations, and gradually take over some of the management duties. Both of these are based on the ability of the AI to understand cause-and-effect relationships between monitored data and issued commands, and more importantly, for the AI to explain its reasoning so that humans trust its conclusions. This is also called deterministic management (see clause 4.5.4.3 of ETSI GS ENI 005 [i.10]).

- The next step of using AI builds on the previous level, and provides tighter integration with analytics. This enables the system to move from deterministic to predictive management. Predictive management uses different processes to calculate probable future events, states, and/or behaviours. Predictive processing also typically allows probability and/or risk assessment. The prediction is based on analysing current and historical operation, and applying patterns found to identify possible problems as well as opportunities for improving operation (see clause 4.5.4.4 of ETSI GS ENI 005 [i.10]).

- The next step of using AI builds on the previous level, and adds elementary goal-directed behavior. Predictions are now made that are directly related to business goals, which enables the network to provide optimized end-user services. For example, as user needs, business goals, or network conditions change, the system can dynamically change the network configuration to adapt to these changes.

- The final step of using AI builds on the previous level, and creates a cognitive management system. While the previous level is able to make decisions based on stated goals, a cognitive system is able to create new goals in order to optimize system operation. Cognitive processing enables the system to understand what has happened and plan a corrective set of actions to achieve system goals and optimize operations (see clause 4.5.4.5 of ETSI GS ENI 005 [i.10]).

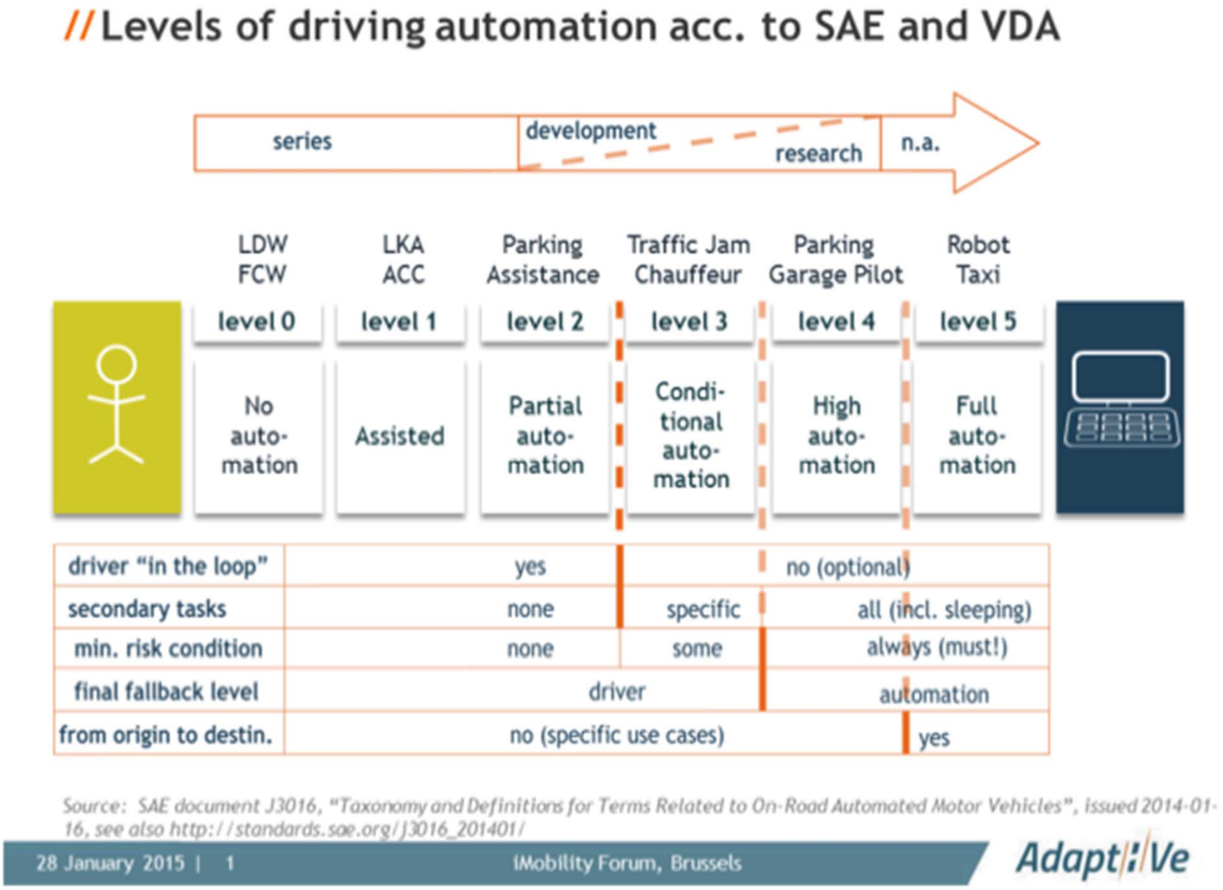
It is recommended that the system uses policy-based management to issue commands, regardless of the level of AI being used. This is because it provides consistent and auditable behavior. This is critical for enabling adaptive and flexible service offerings that respond to changing business goals, user needs, and environmental constraints.

It is therefore possible to speak of different categories, of implementation of AI in telecommunications networks, according to how much the AI system will be able to influence the adaptation of the network and to what extent the diverse parts of the network are controlled using AI assistance.

4.2 Examples of application in specific areas

4.2.1 Automation applied to vehicle driving

The concept of automation categories is already used in specific fields, such as the automotive industry [i.14], for which the aspects considered to define the categories involve the level of intervention required by the human driver of a vehicle, versus the level of control delegated to networked, onboard, and environmental AI assisted agents. The categories of vehicle driving automation have been defined by the Society of Automotive Engineers (SAE), USA and by the German Association of the Automotive Industry (Verband der Automobilindustrie (VDA)). The levels of automation defined by the SAE/VDA for automotive applications are illustrated in Figure 2, where the description of the level of control the driver has over the car for each category is also given.



//Levels of driving automation acc. to SAE and VDA

LDW FCW	LKA ACC	Parking Assistance	Traffic Jam Chauffeur	Parking Garage Pilot	Robot Taxi
level 0	level 1	level 2	level 3	level 4	level 5
No auto-mation	Assisted	Partial auto-mation	Condi-tional auto-mation	High auto-mation	Full auto-mation

	level 0	level 1	level 2	level 3	level 4	level 5
driver "in the loop"	yes				no (optional)	
secondary tasks	none			specific	all (incl. sleeping)	
min. risk condition	none			some	always (must!)	
final fallback level	driver				automation	
from origin to destin.	no (specific use cases)					yes

Source: SAE document J3016, "Taxonomy and Definitions for Terms Related to On-Road Automated Motor Vehicles", issued 2014-01-16, see also http://standards.sae.org/j3016_201401/

28 January 2015 | 1 iMobility Forum, Brussels AdaptIVe

NOTE: Reproduced with the permission of the 5G-PPP www.5g-ppp.eu.

Figure 2: Levels of automation defined by the SAE/VDA for automotive applications [i.14]

NOTE 1: The content of the figure refers to the terminology used by SAE/VDA in the context of automotive applications, e.g. the term automation may often be found. Therefore, Figure 2 is provided just as a conceptual example and the used terminology is not relevant to the present document.

Analysing the categories defined in the figure, and the associated documents [i.1] and [i.2], one can easily understand how categories can also be defined for an autonomic network, if the role of the car driver is replaced by that of the human operator of a network. With reference to Figure 2, instead of 'driver in the loop', one could speak of 'operator in the loop'. Moreover, increasing categories will have an increasing role of autonomic management based on AI application, with the subsequent reduction of required intervention of the operator. ETSI ISG ENI already provides the fundamentals for defining different categories of AI based network autonomicity in the "Use Cases" [i.3], "Requirements" [i.11] and in the "Context-aware policy management Gap Analysis" [i.12] documents. It is therefore straightforward to define AI-based network-autonomicity categories, in analogy to what has been just described in the different area of automotive application for AI. However, as it has been pointed out in note 1, the car automation example is not strictly and directly mapped to any network autonomicity use cases.

NOTE 2: An autonomic system is a ***self-governing system*** that can manage itself in accordance with high-level objectives.

NOTE 3: Self-governance is performed using cognition. The term "manage itself" means that the autonomic system can *sense* changes in itself and its environment, *analyse* changes to ensure that business goals are being met, and *execute* changes to protect ***business goals.***

4.2.2 Autonomicity applied to home broadband services

The example in this clause is the application of the concepts discussed above to a specific and limited set of network resources; this is the home network scenario, which is similar to an operator's network on a much smaller scale and with a much simpler architecture.

Figure 3 illustrates the definition of categories for autonomicity of broadband home services.

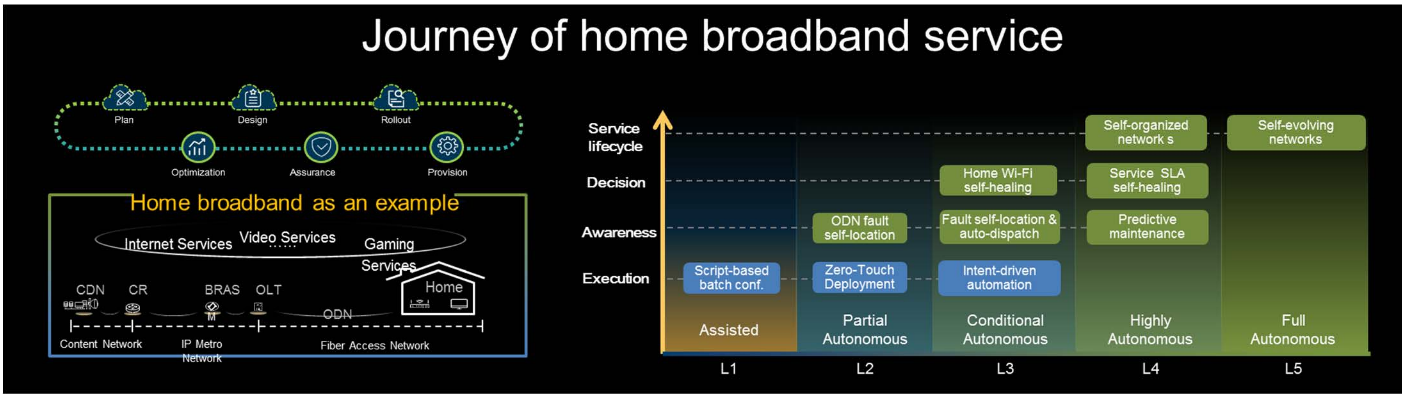


Figure 3: Example of definition of categories for autonomicity of home broadband services

NOTE 1: Figure 3 was originally made for different purposes, and is provided in the present document as an example; the terms used in it do not match necessarily the terminology used in ENI.

- The L0 category, fully manual, does not appear in figure 3.
- In the L1 category, where the Network Management System (NMS) is used to deliver device configuration scripts in batches, the efficiency is improved.
- In the L2 category, the Optical Network Terminal (ONT) box supports plug and play (PnP) for home terminals and implements partial autonomicity of the home network and services management. An example of this category is the implementation of intelligent fault location for the access network, at the level of the Optical Distribution Network (ODN).

NOTE 2: In addition, zero touch deployment, where devices are provisioned and configured automatically, also avoids the use of manual operation.

- In L3 category, conditional autonomicity, the system is autonomic in some phases of the service life cycle. For example, the service provisioning, driven by the intent 'broadband service', could configure 100 Mbit/s of fixed bandwidth based on the type of the house (villa, apartment), or could even define the bandwidth to be allocated based on user preferences (such as degree of game enthusiasm and video enthusiasm). This implementation completely replaces manual service deployment and greatly improves the O&M efficiency in service deployment.

NOTE 3: Home Wi-Fi self-healing and fault self-location and dispatch may also be utilized.

- The L4 category is highly autonomic, where service awareness and decision-making based on service provisioning are implemented. For example, with this increase on the degree of autonomicity, proactive maintenance, SLA-based self-healing, and service driven self-organizing networks can be implemented. This could represent a solution in support of those scenarios for which continuously accelerating service innovation creates revenue, while planning and design are not required.

- In the L5 category, full autonomic management is implemented in all scenarios, which can be seen as a long term goal.

The concepts provided in the examples will have to be extended in order to define general categories for the AI based networks autonomicity. This will be done in the following clauses.

5 Categories of Network Autonomicity

5.1 Introduction

Establishing suitable network autonomicity categories is helpful to guide users in choosing a specific implementation of AI assisted network, and understanding the self-adaptation capabilities to, i.e. changed service conditions, faults, deployment of new services and the autonomicity of operation and overall management.

It is important to note that the categories are focusing on the level of autonomicity the network is characterized by as a consequence of AI tools deployment. In other words, the different categories are providing a classification in terms of the advantages automation and autonomicity bring into the network management and operation processes thanks to the capabilities of adaptation and optimization acquired. Different categories will therefore correspond to different approaches and perspectives in network management and operation. The lowest category corresponds to the absence of automation and autonomicity, and their presence and influence increase in higher categories up to the full AI based autonomicity of network management and operation, thanks to cognition capabilities and closed loop implementation.

In the present clause, the characteristics that an AI assisted network needs are discussed with respect to:

1) match the requirements imposed by the services that the provider wants to implement; and

2) offer the needed level of autonomicity (which includes the many aspects mentioned above in clause 4).

Categories of network autonomicity are detailed below with a clear indication of what services and applications and what management approach the network is suited to support.

5.2 Factors determining the network autonomicity level

5.2.1 Technical factors

A number of technical factors need to be taken into account to determine the degree of AI based autonomicity in a network, and thus, the category that the system can be associated with. The increasing autonomicity of the network with the support of the ENI system open different market perspectives for its use in terms of supported services. Therefore, both technical and market factors will be taken into account for the different categories of network autonomicity, offering separate views. In this clause the technical factors will be considered, while market factors are considered in clause 5.2.2. The technical factors that influence the AI assisted network autonomicity are:

- Man-machine interface and level of required manual interaction/configuration with:
  - Imperative based mode, requiring to specify how a change in the network configuration is implemented (e.g. all manual, CLI by-device configuration, NETCONF multi-device collaboration management)
  - Declarative/intent based mode, requiring to specify what should be configured, without specifying how this configuration is realized
- Data collection and awareness parameters that define the attainable level of awareness:
  - Single device and shallow awareness (e.g. based on SNMP events and alarms)
  - Local awareness (e.g. based on SNMP events, alarms, KPIs, and logs)
  - Comprehensive awareness (based on basic telemetry data)
  - Comprehensive and adaptive sensing (such as compatible with data compression and optimization technologies)
  - Adaptive posture awareness (edge collection plus judgment)
  - Adaptive optimization upon deterioration (edge closed-loop, including collection, judgment, and optimization)
- Decision making participation (human operator in the loop or not): relevance of human decision versus machine decision
- Degree of intelligence and level of knowledge, analysis and understanding:
  - Lack of understanding (manual analysis)
  - Limited autonomous analysis
  - Deep autonomous analysis
  - Comprehensive knowledge based short-term forecast
  - Comprehensive knowledge based long-term forecast
  - Self-adaptation and knowledge-based reasoning
- Adaptation of the configuration to changes in the environment:
  - Static if no autonomic adaptation is supported
  - Limited adaptability to changes
  - Adaptability to significant changes
  - Any change when any autonomic adaptation is supported

- Supported scenarios including complexity and type of domain, use cases and architecture:
  - Single scenario
  - Selected scenarios
  - Multiple scenarios
  - Any scenario

5.2.2 Market factors

The factors that impact the market relevance of network autonomicity involve the possibility to adapt the system and create service offers in different scenarios and involving, according to the 5G network concept, different stakeholders covering a part of or the whole service chain. The market relevance is determined by aspects as the level of simplicity of the AI assisted Network management, the resulting flexibility of the supported services, the required effort and staffing to operate and manage the network, the usage of resources and energy, the level of customer experience.

There are several factors that impact the simplicity of management and control of the AI assisted network and therefore the market relevance that an AI system (enabling the given level of simplicity) can have. An example can be the service creation and configuration interface, which is based on basic command line and complex procedures or an intent based automated one; another is that of a Network Management System (NMS) that, when combined with a controller, is able to realize the full automation in a single domain and/or cross-domain. Examples of such factors include (but are not limited to):

- Scheduling execution: implemented by a person (i.e. manually executed), person and system (i.e. semi-automated), or system (i.e. fully automated).
- Network perceptual monitoring: performed by a person, person and system, or system.
- Analysis and decision-making: done by a person, person and system, or system.
- Service recovery: operated by a person, person and system, or system.
- Customer experience evaluation: by a person, person and system, or system.
- Service coverage capability: coverage of some service scenarios or all service scenarios.

It is challenging to provide a comprehensive list of all the relevant factors. Some of the most relevant are used in Table 2 of clause 5.4 to provide an example of the application of the concept, which is not considered exhaustive.

5.3 Network autonomicity categories description

From totally operator controlled up to the full autonomicity of network management and control based on AI, the categories of AI-based network automation are defined in the following in terms of the factors and the features discussed previously:

- Category 0. **Manual O&M:** O&M operators manually control the network through traditional interfaces and check network alarms and logs in order to understand the presence of anomalous behaviours. SNMP events trigger simple adaptive actions in network devices and alarms provide information about network anomalies and trigger an action from the operator to solve the problem. The operator is therefore always in the loop. There is no intelligence in the network though there is some automation needed to activate the single alarms and the logs triggering the operator's actions.
- Category 1. **Assisted O&M:** Automated scripts are used in service provisioning, network function deployment, configuration and maintenance. There is a shallow perception of the network status, limited to a part of the network or of services, and machines provide limited suggestions for decision making to the operator. There is local awareness based on alarms, SNMP events and logs, KPI measurement. There is a very low level of self-adaptation.

- Category 2. **Partial automation:** Most of the service provisioning is automated, as well as network deployment and maintenance. The AI system has a comprehensive perception of the network status and local machine decision making is implemented; the AI system provides multiple options for service provisioning and can make limited decisions. For example, in cloud computing scenarios with Category 2 network autonomicity, the data center hosted virtualized part of the network provides the API interface for overlay network configuration and automatic network configuration operations are performed according to the scheduling requirements of the cloud platform, such as OpenStack.

- Category 3. **Conditional automation:** Building on Category 2 capabilities, the AI system can sense real-time environmental changes, and in certain domains, optimize and adjust the network configuration thanks to the implementation of closed-loop management. The key characteristic of a Category 3 network is the ability to perform a dynamic autonomic control of operation and maintain a predefined performance level when operating in a single domain. In particular, for Category 3, under predefined conditions and in a given domain, e.g. OSS, BSS, mobile application, transport network, etc., the system can continuously execute control tasks to assure the target performance. This could be done with the system aggregating alarms and identifying fault conditions based on AI, triggering the fault location module to quickly locate the fault and automatically dispatching the trouble ticket. In a Category 3 optical network scenario, for instance, the E2E delay for the supported services is dynamically measured, traced, optimized and maintained.

- Category 4. **High automation:** Building on Category 3 capabilities, the AI system enables, in a cross-domain environment, customer experience-driven predictive or pro-active closed-loop management of networks and services. This allows operators to resolve network faults prior to receiving customer complaints, reduce service outages and, ultimately, improve customer satisfaction. The key characteristic of Category 4 automation is the ability to control and manage the network based on customer experience verification in complex cross-domain service scenarios. For example, in the home broadband service scenario, in a Category 4 network, there are autonomic:

    - measurement and analysis of customer experience in real time

    - continuous identification of dynamic network exceptions with respect to the planned behaviour, and proactive remediation and improvement to meet or exceed contracted service goals

    - rectification of faults and self-recovery

    - trouble reporting based on service experience deterioration and network anomalies detection, enabling predictive operation and maintenance

    - resolution of incidents before they escalate (e.g. Event Handling, Self-Healing, Automatic Re-routing, Resource Reallocation)

    - reduction of the service interruption rate and of the related impact on customer experience

- Category 5. **Fully autonomic system:** This category is the ultimate goal for telecom network evolution. The system is implemented with full closed-loop automation across multiple services, multiple domains, and the entire lifecycle, achieving the full autonomicity of the network.

5.4 Tabular representation of Network Autonomicity categories

Table 1 shows how the factors specified in clause 5.2 impact each of the 6 categories of network autonomicity described in clause 5.3 from a technical point of view. Table 2, instead, analyses the categories in terms of market perception and impact.

Table 1: Categories of network autonomicity from a technical point of view

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of intelligence	Environment adaptability	Supported scenarios
Category 0	Manual O&M	O&M operators manually control the network and obtain network alarms and logs	How (command)	All-manual	Single and shallow awareness (SNMP events and alarms)	Lack of AI based understanding (manual management and control)	Fixed	Single scenario
Category 1	Assisted O&M	Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status and machine suggestions for decision making	How (command)	Provide suggestions for machines or humans and help decision making	Local awareness (SNMP events, alarms, KPIs, and logs)	Limited analysis capability	Limited adaptability to changes	Selected scenarios
Category 2	Partial automation	Automation of most service provisioning, network deployment, and maintenance Comprehensive perception of network status and local machine decision making	How (declarative)	The machine provides multiple opinions, and the machine makes limited decisions	Comprehensive awareness (basic telemetry data)	Deep analysis capability	Limited adaptability to changes	Selected scenarios
Category 3	Conditional automation	In specific environmental and network conditions there is automatic network control and adaptation	How (declarative)	Most of the machines make decisions	Comprehensive and adaptive sensing (such as data compression and optimization technologies)	Comprehensive analysis and knowledge; Short-term forecast capability	Adaptability to significant changes	Multiple scenarios
Category 4	Partial autonomicity	Deep awareness of network status; in most cases the network performs autonomic decision-making and operation adjustment	What (intent)	Optional decision-making response	Adaptive posture awareness	Comprehensive analysis and knowledge Long-term forecast capability	Adaptability to significant changes	Multiple scenarios
Category 5	Full autonomicity	In all environmental and network conditions, the network can automatically adapt	What (intent)	Machine autonomous decision	Adaptive optimization as a consequence of quality of service deterioration	Autonomic evolution and knowledge reasoning	Adaptability to any change	Any scenario

Table 2 shows how the factors specified in clause 5.1 impact each of the 6 categories of network autonomicity from a market point of view.

Table 2: Categories of network autonomicity from a market point of view

Category	Name	Definition	Scheduling execution	Perception monitoring	Analysis and decision-making	Customer experience	System capability	Example of network generation
Category 0	Manual O&M	O&M operators manually control the network and obtain network alarms and logs	Operator	Operator	Operator	Operator	n/a	Command line
Category 1	Assisted O&M	Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status and machine suggestions for decision making	Operator and system	Operator	Operator	Operator	Selected service scenarios	NMS
Category 2	Partial automation	Automation of most service provisioning, network deployment, and maintenance Comprehensive perception of network status and local machine decision making	Operator and System	Operator	Operator	Operator	Selected service scenarios	NMS + controller
Category 3	Conditional automation	In specific environmental and network conditions there is automatic network control and adaptation	Mostly System	Operator and system	Operator	Operator	Multiple service scenarios	Single-domain: Automation + perception analysis + limited context-awareness trigger conditions drive closed-loop management
Category 4	Partial autonomicity	Deep awareness of network status; in most cases the network performs autonomic; decision-making and operation adjustment	Mostly System	Operator and System	Operator and System	Operator and System	Multiple service scenarios	Cross-domain (for some service scenarios): Automation + perception analysis + experience; context-awareness and simple cognitive processing closed-loop management
Category 5	Full autonomicity	In all environmental and network conditions, the network can automatically adapt	System	System	System	System	Any service scenario	Cross-domain and any service: Automation + perception analysis + experience; situation awareness and cognitive processing closed-loop management

5.5 Scenario Examples of Network Autonomicity categories

5.5.1 Introduction

In order to accelerate adoption of network autonomicity, operators are expected to focus on O&M approaches in the various scenarios.. This means that O&M process, especially in terms of decision making, data collection and analysis, changes directly relate to a particular goal and result defined by the operator, and with a business value. Progress of network autonomicity will be accelerated if autonomicity categories of a core set of scenarios is defined, which will be of value to all operators. Then, development of the related autonomous driving solutions for these scenarios can be prioritized accordingly. Clause 5.5 illustrates the autonomicity categories of several typical scenarios.

5.5.2 Autonomicity categories of network traffic classification

Network traffic classification works as a fundamental tool in network operation and management, e.g. to ensure QoS, perform traffic engineering, guarantee network security, etc. With the growth in the diversity of applications, traffic volume and the proportion of encapsulated traffic, traditional traffic classification methods e.g. the port-based method and the DPI-based method are inefficient. However applying AI algorithms to the statistic-based method becomes the main trend.

Table 3 shows the application of autonomicity categories to the network traffic classification scenario.

Table 3: Categories of network autonomicity for network traffic classification

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Supported Scenarios
Category 0	Manual O&M	O&M operators manually control the network and obtain network alarms and logs	How (command)	All-manual	Manually extracts ports	Manually using a port to determine application layer protocol	Non-encrypted traffic classification
Category 1	Assisted O&M	Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status and machine suggestions for decision making	How (command)	Manual analyse the classification results and make decisions such as Qos guarantee, traffic engineering and intrusion detection, etc. Then machines take actions.	Machines such as DPI devices uses automated scripts and inspects signatures in the packet payload to identify the traffic of a non-encrypted application	Manually discovering which signature strings match an application	Non-encrypted traffic classification
Category 2	Partial automation	Automation of most service provisioning, network deployment, and maintenance Comprehensive perception of network status and local machine decision making	HOW (declarative)	Manual analyse the classification results and make decisions such as Qos guarantee, traffic engineering and intrusion detection, etc. Then machines take actions.	Machines such as DPI devices uses automated scripts and inspects signatures in the packet payload to identify the traffic of a non-encrypted application or particular signatures	Manually discovering which signature strings match an application	Non-encrypted traffic and a small amount of encrypted traffic classification
Category 3	Conditional automation	In specific environmental and network conditions there is automatic network control and adaptation	HOW (declarative)	Based on the classification results, the machine provides multiple opinions and makes a limited decision. Operators make the final decision and trigger the machines action	Manually collect and label traffic data for model training. Machines implement a trained model and perform inference.	Manually choose an appropriate Deep Learning algorithm and adjust model parameters.	Non-encrypted traffic and a large amount of encrypted traffic classification
Category 4	Partial autonomicity	Deep awareness of network status; in most cases the network performs autonomic decision-making and operation adjustment	WHAT (intent)	Based on the classification results, the machine provides multiple opinions and even an optimization solution. Humans determine whether to implement it.	Automatically collect and label traffic data for model training and then perform inference based a trained model. When classification results get worse, manually determine whether to update the model and then automatically determine how to update.	Manually choose an appropriate deep reinforcement-learning algorithm to get an optimum model; automatically adjust parameters and learn an appropriate classification model based on pre-defined rules	Non-encrypted traffic and a large amount of encrypted traffic classification

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Supported Scenarios
Category 5	Full autonomicity	In all environmental and network conditions, the network can automatically adapt	WHAT (intent)	Machine self-decision	Automatically collect and label traffic data for model training and then perform inference based a trained model. Automatically decide whether to update the model and how to update.	Completely automatically train a model	Non-encrypted traffic and encrypted traffic classification

5.5.3 Autonomicity categories of IDC energy management

Energy management is always a key factor for large telecom operators. About 40 % - 60 % of operator's power consumption comes from IDCs. AI policy can be exploited in two ways to reduce power consumptions as well as reduce the PUE for IDCs.

1) Cooling system management to provide precise cooling policies matching IDC heat spots

2) Service optimization to improve the power efficiency of IDC services

Table 4 shows the 6 categories of network autonomicity for IDC energy management scenario.

Table 4: Categories of network autonomicity for IDC energy management

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 0	Manual O&M	O&M personnel manually control the cooling	How (command)	All-manual	manual measurement of room temperature	Lack of AI based understanding (manual management and control)	Fixed	Single scenario
Category 1	Assisted O&M	Partially automated temperature tuning based on environmental changes	How (command)	Temperature sensors can be used to assist	Local awareness (room temperature and rack temperature)	Limited analysis capability	Limited adaptability to changes	Selected scenarios
Category 2	Partial automation	Automation of local temperature and partial adjustments of services according to predefined rules	HOW (declarative)	The control module provides suggestions, and makes limited decisions such as changing the temperature	Comprehensive analysis (historical temperature curves and IDC services data)	Deep analysis capability	Limited adaptability to changes	Selected scenarios
Category 3	Conditional automation	Automatic control and adaptation of temperature and IDC services in specific conditions	HOW (declarative)	Most of the machines make decisions	Comprehensive and adaptive sensing (such as data compression and optimization technologies)	Comprehensive analysis and knowledge; forecast capability	Adaptability to significant changes	Multiple scenarios
Category 4	Partial autonomicity	Deep awareness of temperature status and IDC service demands; autonomic decision-making and operation adjustment in most cases	WHAT (intent)	Optional decision-making	Adaptive posture awareness	Comprehensive analysis and knowledge Forward forecast capability	Adaptability to significant changes	Multiple scenarios
Category 5	Full autonomicity	The IDC services and cooling system can automatically adapt to all environmental and network conditions	WHAT (intent)	Machine autonomic decision	Adaptive optimization upon quality of service deterioration	Autonomic based on knowledge reasoning	Adaptability to any change	Any scenario

5.5.4 Autonomicity categories for network fault recovery

At present, intelligent fault recovery includes the functions of alarm correlation, root cause analysis, partial alarm self-healing functionality, etc. Through alarms, filtering, compression and correlation, a procedure is initiated and executed to fix remotely the fault on the equipment. For fault that cannot be fixed remotely, accurate diagnosis or sufficient alarm information is generated to help network operators to locate the problem manually.

Table 5 shows the application of autonomicity categories to network fault recovery scenario. From Table 5, it is possible to assign the present network fault recovery to category 2, under evolution to Category 3.

Table 5: Categories of network autonomicity for network fault recovery

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 0	Manual O&M	O&M operators manually control the network and obtain network alarms and logs	How (command)	All-manual root-cause location and fault recovery	Single device shallow awareness (by manual collection of alarms and identifying the root-cause based on operator's experience)	Lack of AI based understanding (manual management and control)	Fixed	Single scenario
Category 1	Assisted O&MA	Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status and machine suggestions for decision making	How (command)	Manual and offline tool-assisted root-cause location; manual fault recovery	Local awareness (collecting alarms/performance/log automatically, and tool-assisted fault diagnosis)	Limited analysis capability	Limited adaptability to changes	Selected scenarios
Category 2	Partial automation	Automation of most service provisioning, network deployment, and maintenance Comprehensive perception of network status and local machine decision making	HOW (declarative)	Evaluate if fault(s) can be handled by self-recovery; visual tool of root-cause location ; provides multiple suggestions for fault recovery; manual fault recovery	Comprehensive awareness (prediction of potential failures based on operator's experience, offline-tool and what-if fault simulation； automatic inspection; fault found by alarm compression and correlation; dynamic baseline anomaly identification)	Deep analysis capability	Limited adaptability to changes	Selected scenarios
Category 3	Conditional automation	In specific environmental and network conditions there is automatic network control and adaptation	HOW (declarative)	Root-cause location; provides fault-recovery solutions； generate a procedure according to one fault	Comprehensive and adaptive sensing (slow degradation prediction e; worst-case simulation based on automatic inspection; accurate anomaly identification)	Comprehensive analysis, knowledge reasoning and forecast capability	Adaptability to significant changes	Multiple scenarios

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 4	Partial autonomicity	Deep awareness of network status; in most cases the network performs autonomic decision-making and operation adjustment	WHAT (intent)	Generate a procedure according to each fault; recovery according to root-cause location capability; the system provides fault-recovery solutions and simulation; optimal solution decision; automatic fault recovery	Adaptive posture awareness (prediction of slow degradation of performance; worst-case simulation; accurate anomaly identification)	Comprehensive analysis, knowledge reasoning and forecast capability	Adaptability to significant changes	Multiple scenarios
Category 5	Full autonomicity	In all environmental and network conditions, the network can automatically adapt	WHAT (intent)	Machine self-decision (automatic root-cause location and fault recovery)	Adaptive deterioration optimization (prediction of slow degradation of performance; worst-case simulation; accurate anomaly identification; solution optimization)	Autonomic evolution and knowledge reasoning capability	Adaptability to any change	Any scenario

5.5.5 Autonomicity categories of DCN service and resource design

With an increasing number of services with various characteristics hosted in Data Center Network (DCN) (e.g. E-bank system, etc.), autonomous network service and resource design in accordance with service requirements play an important role to increase service deployment efficiency, improve resource utilization and reduce human cost.

Table 6 shows the application of autonomicity categories to the DCN service and resource design.

Table 6: Categories of network autonomicity for DCN service and resource design

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 0	Manual O&M	O&M operators manually control the network and obtain network alarms and logs	How (command)	All-manual (manual service parameter generation; manual configuration delivery of logical and physical networks)	Single and shallow awareness (manual resource query; manual device design based on device model)	Lack of AI based understanding (manual management and control)	Fixed	Single scenario
Category 1	Assisted O&M	Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status, machine suggestions for decision making	How (command)	Provide suggestions to machines or humans and help decision making (operators manually generate service parameters through procedures; tool-assisted and manual configuration)	Local awareness (manual device design based on device model; manual service testing)	Limited analysis capability	Limited adaptability to changes	Selected scenarios
Category 2	Partial automation	Automation of most service provisioning, network deployment, and maintenance Comprehensive perception of network status and local machine decision making	HOW (declarative)	The machine provides multiple options, and makes limited decisions operators manually select the service automatic configuration of physical devices based on the logical network configuration	Comprehensive awareness (basic telemetry data) manual network design based on logical models, manual service testing	Deep analysis capability	Limited adaptability to changes	Selected scenarios

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 3	Conditional automation	In specific environmental and network conditions there is automatic network control and adaptation	HOW (declarative)	Most of the machines make decisions (automatic network parameters generation and configuration according to the characteristics of DCN services with manual adjustment and confirmation; status check of logical network configuration delivery (success or failure) through service pre-deployment simulation; configuration delivery of logical network with manual confirmation; automatic configuration delivery of physical network)	Comprehensive and adaptive sensing (such as data compression and optimization technologies) automatic design of the network recommendation of computing resources deployment with manual adjustment and confirmation; automatic validation of network configuration through testing	Comprehensive analysis, knowledge reasoning and forecast capability	Adaptability to significant changes	Multiple scenarios
Category 4	Partial autonomicity	Deep awareness of network status; in most cases the network performs autonomic decision-making and operation adjustment	WHAT (intent)	Optional decision-making (automatic generation and deployment of network configuration status check of network configuration by service simulation; partly with manual confirmation	Adaptive posture awareness automatic design of logical network and deployment of computing resources; automatic validation of network configuration through testing)	Comprehensive analysis, knowledge reasoning, forward forecast capability	Adaptability to significant changes	Multiple scenarios
Category 5	Full autonomicity	In all environmental and network conditions, the network can automatically adapt	WHAT (intent)	Machine autonomous decision	Adaptive optimization as a consequence of quality of service deterioration (autonomous DCN service and Intent based resource design)	Autonomic evolution and knowledge reasoning capability	Adaptability to any change	Any scenario

5.5.6 Autonomicity categories of DCN service quality optimization

According to the results and information about network performance, customer complaint, network fault alarm, network logs, etc., AL/ML-enabled DCN service quality optimization is the main trend to satisfy user's Quality of Experience (QoE), guarantee SLA and improve network resource utilization.

Table 7 shows the application of autonomicity categories to network performance optimization scenario.

Table 7: Categories of network autonomicity for DCN service quality optimization

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 0	Manual O&M	O&M operators manually control the network and obtain network alarms and logs	How (command)	All-manual	Single and shallow awareness (SNMP events and alarms)	Lack of AI based understanding (manual management and control)	Fixed	Single scenario
Category 1	Assisted O&M	Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status and machine suggestions for decision making	How (command)	Provide suggestions to machines or humans and help decision making tool-assisted manual adjustment of network parameters based on empirical values; manual service validation with tool-assisted testing)	Local awareness based on SNMP events, alarms, KPIs, and logs (offline tool-assisted network performance evaluation; SLA anomaly detection based on static rules; tool-assisted root-cause analysis and location)	Limited analysis capability	Limited adaptability to change	Selected scenarios
Category 2	Partial automation	Automation of most service provisioning, network deployment, and maintenance Comprehensive perception of network status and local machine decision making	HOW (declarative)	The machine provides multiple opinions, and the machine makes a small decision automatic adjustment of network devices and conditions through pre-defined template; tool-assisted Virtual Private Cloud (VPC) parameter adjustment; manual service validation with tool-assisted testing	Comprehensive awareness (basic telemetry data) online tool-assisted performance deterioration prediction based on empirical values; SLA anomaly detection; root-cause analysis, demarcation and location with visual tools	Deep analysis capability	Limited adaptability to changes	Selected scenarios

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 3	Conditional automation	In specific environmental and network conditions there is automatic network control and adaptation	HOW (declarative)	Most of the machines make decisions automatically adjust VPC (Virtual Private Cloud) parameters to adapt to real-time traffic machine recommendation and manual confirmation of virtual machines (VMs) relocation Service quality evaluation through simulation and testing;	Comprehensive and adaptive sensing for automatic traffic detection, system adaptability ;SLA monitoring; recommendation of ;configuration with manual confirmation; root-cause analysis, demarcation and location with visual tools;	Comprehensive analysis, knowledge reasoning and forecast capability	Adaptability to significant changes	Multiple scenarios
Category 4	Partial autonomicity	Deep awareness of network status; in most cases the network performs autonomic decision-making and operation adjustment	WHAT (intent)	Optional machine decision-making [automatically adjust VPC (Virtual Private Cloud)] parameters to adapt to real-time traffic Machine recommendation and manual confirmation of virtual machines (VMs) relocation with manual adjustment and confirmation; Service quality evaluation through simulation and testing)	Adaptive posture awareness (automatic traffic detection, adaptability of firewall strategies and SLA monitoring; automatic recommendation and delivery of candidate firewall strategies with updating logs; AI based fast root-cause analysis, demarcation, location and process; AI recommendation of solutions, optimal solution selection and deployment based on simulation results,dynamic adjustment of solution)	Comprehensive analysis and knowledge Forward forecast capability	Adaptability to significant changes	Multiple scenarios
Category 5	Full autonomicity	In all environmental and network conditions, the network can automatically adapt	WHAT (intent)	Machine autonomous decision	Adaptive optimization upon quality of service deterioration (DCN service quality optimization based on intent, including user experience guarantee, resource utilization improvement, etc.)	Autonomic evolution and knowledge reasoning capability	Adaptability to any change	Any scenario

5.5.7 Autonomicity categories of End-to-End service quality assurance in bearer network

With the rapid development of mobile communication technologies, B2C and B2B services are being paid more and more attention. Ultra-HD video plays the major role in 5G 2C services (e.g. mobile 4K Live, cloud VR/AR, vehicle-mounted 4K video, real-time high-precision map, etc.), which demands both wide coverage and large bandwidth. In addition, 5G 2B services (e.g. automatic driving, smart manufacturing, telemedicine, and smart grid), have higher requirements on the quality of the bearer network in terms of high bandwidth, low latency, and high reliability.

In the 5G era, carriers should pay attention to network service quality in addition to the overall network performance. Fast fault locating and proactive fault prevention based on service path and quality visibility are key techniques for E2E Service Quality Assurance (SQA) in the bearer network.

Table 8 shows the 6 categories of network autonomicity for End-to-End SQA scenario in bearer network.

Table 8: Categories of network autonomicity for End-to-End SQA in bearer network

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 0	Manual O&M	O&M operators manually control the network and obtain network alarms and logs	How (command)	manual fault root-cause location and service quality checking	collecting alarms manually; no information about E2E service quality; manually analysing fault root-cause;	Manual management and control	Fixed	Single scenario
Category 1	Assisted O&M	Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status and machine suggestions for decision making	How (command)	manual root-cause location; manually switching the active tunnel to its standby; manual and tool-assisted service quality checking;	receiving user complaint; collecting network alarms and fault report; manual and tool-assisted root-cause location;	Limited analysis capability	Limited adaptability to changes	Selected scenarios
Category 2	Partial automation	Automation of most service provisioning, network deployment, and maintenance Comprehensive perception of network status and local machine decision making	HOW (declarative)	rapid bidirectional forwarding detection (BFD) to detect fault; automatically switching the active tunnel to its backup; manual service quality checking; tool-assisted service quality testing;	receiving user complaint; collecting network alarms and fault report; manual and tool-assisted root-cause location;	Deep analysis capability	Limited adaptability to changes	Selected scenarios
Category 3	Conditional automation	In specific environmental and network conditions there is automatic network control and adaptation	HOW (declarative)	automatically switching active tunnel to its standby and assuring recovery of service quality; automatically service quality checking;	proactively detecting network fault and monitoring base station service quality; automatic fault root-cause location based on in-band detection solution, e.g. In-situ Flow Information Telemetry (iFIT), etc.; manual and tool-assisted root-cause location;	Comprehensive analysis, knowledge reasoning and forecast capability	Adaptability to significant changes	Multiple scenarios

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Data Collection and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenarios
Category 4	Partial autonomicity	Deep awareness of network status; in most cases the network performs autonomic decision-making and operation adjustment	WHAT (intent)	automatically switching active tunnel to its standby; limited manual confirmation of commands/operations; automatically assuring recovery of service quality; real-time SQA;	proactively detecting network fault and monitoring base station service quality; automatic fault area location and root-cause location	Comprehensive analysis, knowledge reasoning, forward forecast capability	Adaptability to significant changes	Multiple scenarios
Category 5	Full autonomicity	In all environmental and network conditions, the network can automatically adapt	WHAT (intent)	automatically switching active tunnel to its backup without manual confirmation of commands/operations; automatically monitoring service quality and assuring recovery of service quality; real-time SQA;	proactively detecting network fault; proactively monitoring service quality; automatic fault area location and automatic root-cause location;	Autonomic evolution and knowledge reasoning capability	Adaptability to any change	Any scenario

6 Relation of the Autonomicity Categories to ENI system architecture and other architectures

6.1 Introduction

This clause describes the relation between the Network Autonomicity Categories and the ENI system architecture as well as other architectures.

6.2 Mapping of Assisted System Classes into Network Autonomicity Categories

According to [i.9] the ENI system is defined as a set of entities, based on the "observe-orient-decide-act" control loop model that produces commands, recommendations, and knowledge to assist or direct the management of another system. Thanks to ENI implementation the system will acquire a degree of autonomicity that can be classified in one of the 6 Network Autonomicity Categories described in clause 5.3. The ENI system architecture analysis functions include Knowledge Management, Context Awareness, Cognition Management, and situation-aware, model-driven, Policy Management.

The ENI architecture document [i.9] provides another classification for the different assisted systems according to the fact that they can natively incorporate AI functional blocks or not and to the way they are interfacing with ENI, implementing a closed control loop or not. It is therefore very interesting to describe the relation between the Network Autonomicity Categories described in clause 5.3, and the Assisted System classes defined in [i.10], as also the latter take into account not only the intrinsic nature of the Assisted System but also in which way it interacts with ENI. This relation is shown in Table 9, where the Assisted System classes are mapped into categories of network autonomicity from a technical and market point of view.

Table 9: Mapping of Assisted System classes into network autonomicity categories from a technical and market point of view

Assisted System Class	Category from a technical/ market point of view	Level definition from a technical point of view	Category definition from a market point of view
Class 1 No AI	Category 0 manual O&M	This class of Assisted System has no AI capabilities. O&M personnel manually control the network and obtain network alarms and logs	With auxiliary tools, O&M personnel perform all dynamic tasks. All decisions are made manually; There is a single and shallow awareness. The management is made manually and there is lack of AI based understanding. Moreover, the environment adaptability is fixed.
Class 2 Internal AI is not part of the internal closed control loop	Category 1 Assisted O&M	This class of Assisted System uses some AI-based algorithms, but critically, does not use AI does not use AI within an internal closed control loop scheme. Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status and machine suggestions for decision making	Provide suggestions for machines or humans and help decision making. The Assisted System can help execute a subtask based on rules, while O&M personnel perform other dynamic tasks.
	Category 2 Partial automation	This class of Assisted System uses some AI-based algorithms, but critically, does not use AI within an internal closed control loop scheme. Automation of most service provisioning, network deployment, and maintenance Comprehensive perception of network status and local machine decision making	The Assisted System continuously completes via automation, most service provisioning, network deployment, and maintenance tasks. There is a comprehensive perception of network status and local machine decision making, however, it does not use AI within the internal control loop
	Category 3 Conditional automation	This class of Assisted System uses some AI-based algorithms, but critically, does not use AI does not use AI within an internal closed control loop scheme. In specific environmental and network conditions there is automatic network control and adaptation	The Assisted System can implement a complete closed-loop automation of single-domain scenarios. In specific environmental and network conditions, if a system failure occurs, then the Assisted System ensures that services provided to users are recovered in a timely manner.
	Category 4 Partial autonomicity	This class of Assisted System uses some AI-based algorithms, but critically, does not use AI within an internal closed control loop scheme Deep awareness of network status; in most cases the network performs autonomic decision-making and operation adjustment	The Assisted System can automatically execute the cross-domain and service close-loop automation.
Class 3 Internal AI in the closed control loop	Category 5 Full autonomicity	This type of Assisted System has AI-based decision-making capabilities as part of its internal control loop. In particular, this type of assisted system is applied in different network environments and network conditions, the network can automatically adapt to and adjust to meet people's intentions	The Assisted System can perform complete dynamic tasks and exception handling in all network environments. O&M personnel do not need to intervene.

7 Conclusions

The present document analyses the aspects that impact the autonomicity of a network (or more in general an assisted system) assisted by an ENI system, and the consequent possible different degrees of such autonomicity. This can be useful to classify systems making use of ENI assistance in different autonomicity categories. The indication of the category will therefore provide an indication of the effectiveness and the benefits of ENI implementation in a certain network and to a certain purpose (as optimization of energy consumption, management of networking resources and their dynamic instantiation in virtualized scenarios, etc.).

A similar approach has been applied in other areas, as for example the automotive industry, to favour an easier understanding of the characteristics of the systems consequent to introduction of automation, and it can be very useful also in the telecommunications industry because of the above mentioned large variety of applications that an ENI system can have.

Therefore, the present document, after considering the basic concepts and their use for the definition of general network autonomicity categories, has focused on the application of the same concepts to specific use cases of interest, to provide various examples of categorization of network autonomicity for specific aspects like energy management, traffic classification, virtual resource management.

Besides a pure technical perspective, a first analysis of the market aspects for the different categories has also been provided. This part of the present document could be further improved and extended by future releases, but anyway lays the first stone of the work to this end.

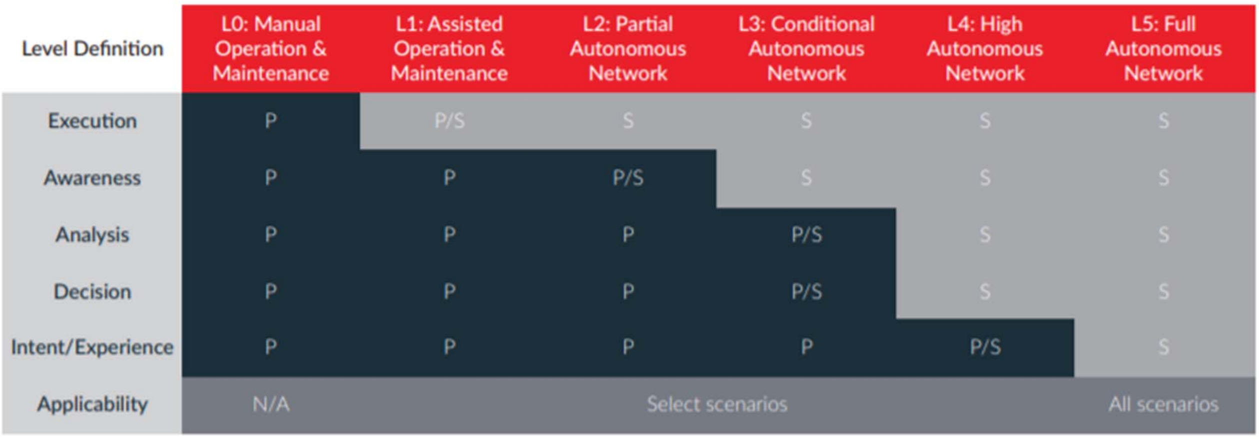
Finally, in clause 6, the present document offers an important view of the overall autonomicity (of the assisted system with ENI system support) mapping the different degrees of AI implementation in the original assisted system with the different ways in which it can interact with ENI (up to a full closed-loop-control).

In conclusion, the work summarized in the present document has provided a first careful definition of categories for network autonomicity based on technical characteristics. It can be further enriched with a more detailed and extended analysis of the market impact of network autonomicity and providing further examples of the application of categories to specific deployment scenarios or use cases, also in relation to ENI PoC activity.

Annex A: Related work published by other SDOs

This annex summarizes the state-of-art of related work.

In May 2019, TM Forum, published a whitepaper of Autonomous Networks: Empowering Digital Transformation For The Telecoms Industry [i.13], and a figure on Autonomous networks levels was shown in Figure A.1.



Level Definition	L0: Manual Operation & Maintenance	L1: Assisted Operation & Maintenance	L2: Partial Autonomous Network	L3: Conditional Autonomous Network	L4: High Autonomous Network	L5: Full Autonomous Network
Execution	P	P/S	S	S	S	S
Awareness	P	P	P/S	S	S	S
Analysis	P	P	P	P/S	S	S
Decision	P	P	P	P/S	S	S
Intent/Experience	P	P	P	P	P/S	S
Applicability	N/A	Select scenarios				All scenarios

P: Personnel, **S:** Systems

Figure A.1: Autonomous networks levels in TM Forum

In this white paper, Level 0 to Level 5 are defined as below:

- Level 0 - manual management: The system delivers assisted monitoring capabilities, which means all dynamic tasks have to be executed manually.
- Level 1 - assisted management: The system executes a certain repetitive sub-task based on pre-configured to increase execution efficiency.
- Level 2 - partial autonomous network: The system enables closed-loop O&M for certain units based on AI model under certain external environments.
- Level 3 - conditional autonomous network: Building on L2 capabilities, the system with awareness can sense real-time environmental changes, and in certain network domains, optimize and adjust itself to the external environment to enable intent-based closed-loop management.
- Level 4 - high autonomous network: Building on L3 capabilities, the system enables, in a more complicated cross-domain environment, analyse and make decision based on predictive or active closed-loop management of service and customer experience-driven networks.
- Level 5 - full autonomous network: This level is the ultimate goal for telecom network evolution. The system possesses closed-loop automation capabilities across multiple services, multiple domains, and the entire lifecycle, achieving autonomous networks.

History

Document history		
V1.1.1	November 2019	Publication