ETSI GR ENI 010 V1.2.1 (2024-06)

GROUP REPORT

Experiential Networked Intelligence (ENI); Evaluation 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

RGR/ENI-0010v121_AI_App_Net

Keywords

artificial intelligence, categorization, 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 - 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....5
3.1 Terms....5
3.2 Symbols....6
3.3 Abbreviations 6
4 Introduction 6
4.1 Background on categories for AI application to networks 6
4.2 The motivation for evaluating categories of AI application to network....11
4.3 Responsibility Index in Autonomous Network 11
5 Evaluation criteria of categories for AI application to Network 14
5.1 Framework of quantitative evaluation process....14
5.2 Scoring principles and specification of the single scenario....16
5.2.1 Scoring principles and specification 16
5.2.2 Weights determined by Analytic Hierarchy Process 17
5.2.3 Recommended values of KPI for each intelligent level in some scenarios....19
5.2.4 Presentation of evaluation result....21
5.3 Scoring principles and specification of the part of network lifecycle 21
5.3.1 Explorations on evaluation of network deployment autonomicity categories 21
5.3.2 Explorations on evaluation of evaluation of the entire network autonomicity categories 24
5.4 The relationship among the network infrastructure capabilities (KPI) and the network intelligence levels 29
6 Application of quantitative evaluation criteria....30
6.1 Transport Network: 5G and DCN examples 30
6.1.1 General categorization criteria....30
6.1.2 5G transport example....34
6.1.3 DCN transport example 36
6.1.4 IP Network Monitoring and Troubleshooting Process....37
7 Suggested requirements of network infrastructure in different Categories....43
7.1 Knowledge Base....43
7.2 Tool for decision delegation according to Time Dimension 43
7.3 Data classification and grading 44
8 Conclusions 45
Annex A: Change history 46
History 47

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) 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 revises ETSI GR ENI 010 [i.4] to further:

- investigate quantitative evaluation criteria of network autonomicity categories;
- perform a deeper research of more quantitative factors that determine those categories;
- define an accurate scoring criteria that complies with the evolution of the ENI architecture; and
- define a data model covering an entire operator's network or just a specific domain.

This deeper research will be complemented by the description of several example scenarios where the quantitative factors and the scoring evaluation criteria will be illustrated. This can be done by analysing the relationship among network KPIs of different levels, e.g. between the network infrastructure capabilities and the network intelligence levels.

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] Void.

[i.2] ETSI GR ENI 004 (V3.1.1): "Experiential Networked Intelligence (ENI); Terminology".

[i.3] ETSI GR ENI 007 (V1.1.1): "Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks".

[i.4] ETSI GR ENI 010 (V1.1.1): "Experiential Networked Intelligence (ENI); Evaluation of categories for AI application to Networks".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

autonomous networks: set of self-governing programmable and explainable systems that seamlessly deliver secure, context-aware, business-driven services that are created and maintained using model-driven engineering and administered by using policies

Autonomous Network Responsibility Index (ANRI): level of responsibility delegated to the AN in all the Operational Procedures bind to the lifecycle management of each Autonomous Domain and E2E Service

digital twin: virtual representation of a physical object or system across its lifecycle, using real-time data to enable understanding, learning and reasoning

NOTE: As defined on the IBM® website.

domain technical expert: technical expert that has authority within a domain

evaluation dimension: viewpoint that can be divided into five dimensions

NOTE: This can be subdivided into Decision Making Participation, Data Collection and Analysis, Degree of Intelligence and Environment Adaptability, as defined in ETSI GR ENI 007 [i.3].

evaluation object: AI application or a part of Network Lifecycle, defined from two dimensions: the subsystems and the network lifecycle

Network Digital Twin (NDT): Virtual Digital Twin of telecom network, including its own Network lifecycle

NOTE: Some of the dimensions can be tailored or merged in line with actual conditions.

network lifecycle: work-flow of activities including network planning, network deployment, network service provisioning, network changes, network maintenance, network optimization in real-time

quantitative evaluation criteria: give a score to specific network intelligent application or system considering multiple dimensions

subsystem: network element, management system, network platform

technical expert: person in charge of defining or supporting Operational Procedures within a CSP Network (e.g. in charge of Capacity Planning, Engineering and Designing, Troubleshooting)

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR ENI 004 [i.2] and ETSI GR ENI 007 [i.3] apply.

4 Introduction

4.1 Background on categories for AI application to networks

At present, artificial intelligence technology has achieved single breakthrough and application in local scene and local field of network. But there is no unified description language and evolution route of network autonomicity. The realization of autonomous network needs to evolve step by step in exploration, which cannot be accomplished at a single stroke. Therefore, a unified standard categories of network autonomicity should be established to measure the intellectualization level of network and guide the development of network. At present, a variety of network intelligent grading evaluation systems have been formed in different standards organizations.

Since 2018, ETSI ISG ENI has initiated the network intelligence classification project, officially released in November 2019. On the basis of TMF classification standard, it further describes the characteristics of each level from the perspectives of market and technology.

The present document will mainly refer to the intelligence grading standard proposed by ETSI ENI and its application for relevant research and exploration. The definition of categories for AI application to networks is shown in Table 4-1.

Table 4-2 support evaluation of the level of Autonomicity, identifying the responsibility shift from human operator to the System.

For details, refer to ETSI GR ENI 007 [i.3].

Table 4-1: Categories of network intelligence from a technical point of view (Source: ETSI GR ENI 007 [i.3])

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Decision Making and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenario
Level 0	Traditional manual network	O&M personnel manually control the network and obtain network alarms and logs	How (command)	All-manual	Single and shallow awareness (SNMP events and alarms)	Lack of understanding (manual understanding	Fixed	Single scenario
Level 1	Partially automated network automated diagnostics	Automated scripts are used in service provisioning, network deployment, and maintenance. Shallow perception of network status and decision making suggestions of machine	How (command)	Provide suggestions for machines or humans and help decision making	Local awareness (SNMP events, alarms, KPIs and logs)	A small amount of analysis	Little change	Few scenarios
Level 2	Automated network	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	Comprehensive awareness (Telemetry basic data)	Powerful analysis	Little change	Few scenarios

Category	Name	Definition	Man-Machine Interface	Decision Making Participation	Decision Making and Analysis	Degree of Intelligence	Environment Adaptability	Supported Scenario
Level 3	Self-optimization network	Deep awareness of network status and automatic network control, meeting users' network intentions	HOW (declarative)	Most of the machines make decisions	Comprehensive and adaptive sensing (such as data compression and optimization technologies)	Comprehensive knowledge Forecast	Changeable	Multiple scenarios and combinations
Level 4	Partial autonomous network	In a limited environment, people do not need to participate in decision-making and adjust themselves	WHAT (intent)	Optional decision-making response (decision comments of the challenger)	Adaptive posture awareness (edge collection + judgment)	Comprehensive knowledge Forward forecast	Changeable	Multiple scenarios and combinations
Level 5	Autonomous network	In different network environments and network conditions, the network can automatically adapt to and adjust to meet people's intentions	WHAT (intent)	Machine self-decision	Adaptive deterioration optimization (edge closed-loop, including collection, judgment, and optimization)	Self-evolution and knowledge reasoning	Any change	Any scenario & combination

Table 4-2 below referenced from ETSI GR ENI 007 [i.3] report the level of network autonomicity from a Market point of view, showing the users perception relating to the business functions of BSS. It is in good alignment with concept defined within TMforum. The scheduling, perception, analysis, customer experience, system capabilities & network generation may be mapped to technical capabilities. Some like perception and analysis are a one to one mapping. Others, like MMI degree of intelligence and environment adaptability may each have both a customers and systems aspects.

As reported in clause 5.2 in ETSI GR ENI 007 [i.3] about market relevance: "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".

The 6 levels as described below are an ENI view.

Table 4-2: Level of network autonomicity from a market point of view (Source: ETSI GR ENI 007 [i.3])

Level	Name	Definition	Scheduling execution	Perception monitoring	Analysis and decision-making	Customer experience	System capability	Example of network generation
Level 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
Level 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
Level 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

Level	Name	Definition	Scheduling execution	Perception monitoring	Analysis and decision-making	Customer experience	System capability	Example of network generation
Level 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
Level 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
Level 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

4.2 The motivation for evaluating categories of AI application to network

Evaluation for categories of AI application to network is proposed to give a score to a specific network intelligent application considering multiple dimensions (e.g. data collection, analysis, decision, etc.).

Based on the definition of categories and of application cases, according to the use of AI in the implementation process:

1) the technical requirements of each link and step are detailed;

2) the test verification scheme and specification are formulated;

3) the evaluation criteria and index are quantified.

In the evaluation, it is necessary to avoid the requirements for the specific implementation methods of intelligence, and focus on the evaluation of the implementation effect, such as the degree of automation, whether closed-loop, unit efficiency, etc.

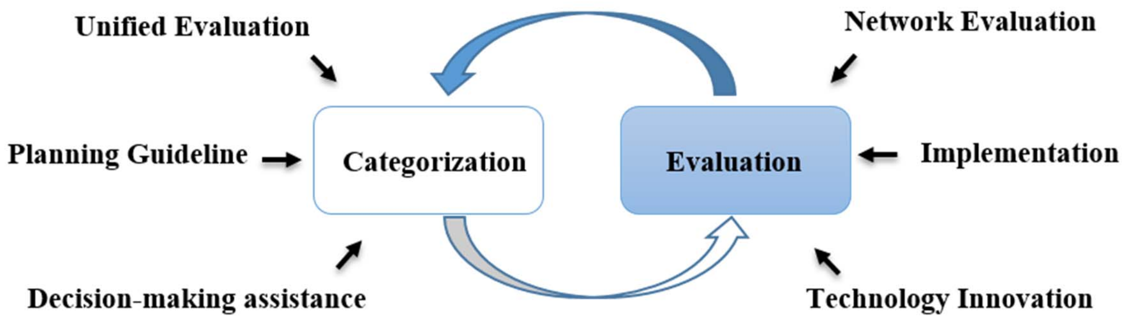

Figure 4-1: The categorization and evaluation for AI application to network

The definition and evaluation of categories for AI application to network complement each other, jointly promote network evolution.

The goals and motivation of definition of network autonomicity categories:

- Unified evaluation: Provide basis for categories of network intelligence and promote the whole industry to form a unified understanding of intelligent network and other related concepts.
- Planning Guideline: Provide reference for operators to formulate relevant strategies, and clarify the stage division and stage objectives of development planning.
- Decision-making assistance: Provide decision-making assistance for operators, equipment manufacturers and other industry participants in technology cooperation, product planning, etc.

The goals and motivation of quantitative evaluation criteria:

- Network Evaluation: quantitatively evaluating capability of autonomous network.
- Implementation: defining a process of evaluating network autonomicity categories.
- Technology Innovation: cognizing the disadvantages of the current network and applications, developing new technologies to improve the level of network autonomicity.

4.3 Responsibility Index in Autonomous Network

Autonomous Network introduce a new aspect to be considered in parallel to the technical capabilities of the Network and related management systems in themselves. Responsibility and Liability related to autonomous decision represent a relevant point to be taken into account.

The defining characteristic of an Autonomous Network is its ability to assume Responsibilities that the Humans accept to delegate it.

According to this statement, the level of Autonomicity assumed by network can potentially be regarded less as a technical one and more related to the decision responsibilities delegated to network by the Operator. Refer to Table 4-2 for more information on Operator vs Network responsibilities and roles.

ENI Engine is an enabler for network decision making process across the overall lifecycle of the assisted system.

The Operator, according to AI training and a proper growth in trust for the network capacity to take final decision, can delegate the responsibility of the decision to AN stepwise.

Any reference in the follow up to the network Responsibility, refers to the level of Responsibility the Operator delegated to the network to autonomously take the final decision before it get executed.

In some specific case, Human intervention could be needed to execute actions according to decisions taken automatically by network (e.g. expansion of a datacentre according to a capacity plan generated automatically).

In this case, the Responsibility remains with the network (final decision), regardless of the Executor.

In general, responsibility is with the entity taking the ultimate decision, independently of how and who implement the related actions.

The Operator, in delegating the network for final decision, express trust in network to be properly trained by its experts and to correctly behave in obtaining expected results. The liability for errors, SLA breach or wrong investment or any unexpected side effects remain within the Operator remit and is out of scope for the determination of the Autonomicity Level of the network itself.

Autonomous Network have to control the lifecycle of two main entities: Autonomous Domains and E2E Services.

The Responsibility Level is than strictly related to the level of Autonomicity of the Network in managing the lifecycle of all its Autonomous Domains and E2E Services.

A quantification of the overall Responsibility Level assumed by the network could be estimated by analysing the lifecycle and relative Operational phases (network planning, network deployment, network service provisioning, network changes, network maintenance, network optimization) of each individual Autonomous Domain within the network, as well as of any E2E Service type.

To properly quantify the Responsibility Level within a Network, Responsibility Matrixes have to be created, having the phases of the Operator Lifecycle in each column and in each row the Technology Domains (e.g. Transport, Radio, Fixed Access) or E2E Services (e.g. VoLTE, Enterprise Hybrid Cloud connection, Enterprise VPN).

For each cell of the matrix, a Responsibility Index (e.g. 0-5) could be estimated according to:

1) operator responsible of the decision;

2) network has tool to guide and support Operator decision and immediate side effects;

3) network recommend decision presenting a complete view of the element supporting the decision and the possible side effects;

4) as per level 3, but network has the possibility to take fully autonomous decision in off-peak hours;

5) network fully autonomous in taking decisions, with escalation to Technical Experts in case of severe unforeseeable events.

The following Tables 4-3 and 4-4 are indicative and modification to lifecycle phases or additions of other Autonomous Domains or E2E services is possible network planning, network deployment, network service provisioning, network changes, network maintenance, and network optimization.

Table 4-3: Operator Lifecycle Responsibility within Network Domains

Lifecycle/ Autonomous Domain	Auto DomainWeight	Total	Network planning		Network deployment		Network service provisioning		Network changes		Network maintenance		Network optimization	
			Score	Comment	Score	Comment	Score	Comment	Score	Comment	Score	Comment	Score	Comment
Phase Weight (0..1)	X	x	1		1		1		1		1		1	
RAN	1													
Transport	1													
Core Network	1													
Fixed Access	1													
Total														

Table 4-4: Operator Lifecycle responsibility within E2E Services

Lifecycle/E2E Services	E2E Service Weight	Total	Network planning		Network deployment		Network service provisioning		Network changes		Network maintenance		Network optimization	
			Score	Comment	Score	Comment	Score	Comment	Score	Comment	Score	Comment	Score	Comment
Phase Weight (0..1)	X	x	1		1		1		1		1		1	
VoLTE	1													
Enterprise VPN	1													
FWA	1													
Enterprise Hybrid Cloud Connectivity	1													
Total														

For both the Autonomous Domain and the E2E Services, a partial Autonomous Network Responsibility Index (ANRI) have to be calculated, respectively ANRItd and ANRIes. For each row a weighted mean value of all the Lifecycle phases will be calculated. A following weighted mean values of those results will be done on a column bases.

A total ANRI Responsibility Index is than calculated with a weighted mean value of the two value above:

$$ANRI = \frac{Wtd \times ANRItd + Wes \times ANRIes}{Wtd + Wes}$$

The calculated (ANRI) could be an additional component of the Score S determined in Table 5-2.

On the other side, due to the completeness of the evaluation required to evaluate the ANRI, it can be considered as the achieved level of Autonomicity achieved by the network itself.

ANRI is a methodology for calculating the S_{dmp} (score of Decision Making Participation) as defined and used in clause 5.2.

5 Evaluation criteria of categories for AI application to Network

5.1 Framework of quantitative evaluation process

The general process of evaluating categories of AI application to network includes five steps: the identification of the evaluation object, the division of the evaluation dimension, the analysis of the evaluation object, the scoring of the evaluation dimension and the acquisition of the evaluation result, as shown in Figure 5-1.

Figure 5-1: Framework of quantitative evaluation process

The specific process is as follows:

1) The identification of the evaluation object

   When the evaluation object is selected from the actual production system, it needs to be defined from two dimensions: the end to end subsystems and network lifecycle, so as to better analyse the corresponding quantitative indicators. Some examples are given in Table 5-1.

Table 5-1: Examples of evaluation object

	Network Planning and Design	Network Deployment	Network Service Providing	Network Changes	Network Maintenance	Network Optimization
Network Element	Intelligent Hardware Recognition	Network Element Cutover			Network Element Fault Location	MM Parameter Optimization and Base Station Energy Saving
Management System	Site Planning Tool	Network Expansion Tool	Service Management System	Node upgrade management		Wireless Network Optimization Tool
Network Platform	The Platform of Network Planning System	The Platform of Device Online	Operation Support System	Network upgrade management	Intelligent Monitoring System	Intelligent Network Optimization System

2) The Division of the Evaluation Dimension

According to Table 4-1, when evaluating an object, it can be divided into five dimensions such as ManMachine Interface, Decision Making Participation, Data Collection and Analysis, Degree of intelligence and Environment adaptability or some of the dimensions can be tailored or merged in line with actual conditions.

3) The Analysis of the Evaluation Object

After defining the evaluation dimensions of the evaluation object, each evaluation dimension can be divided into the following indices. Information extraction and status analysis are carried out for each index, so as to realize the quantification of each index and to support the scoring in step 4.

Table 5-2: Analysis of evaluation objects

ManMachine Interface (MMI)	Decision Making Participation (DMP)	Data Collection and Analysis (DCA)	Degree of Intelligence (DI)	Environment Adaptability (EA)
User Requirements	Decision-making - Content	Collection Content	Analysis Content	Robustness index
Interface mode	Decision-making Methods	Collection Methods	Analysis Methods	Adaptation mode
System Requirements	Decision-making Results	Collection Results	Analysis Results	Adaptation Result/Time

NOTE 1: The accuracy of adaptive time division needs further study.

NOTE 2: How to quantify environmental change needs further study.

4) The Scoring of the Evaluation Dimension

In accordance with the scoring principles in clause 5.2.1, after obtaining the detailed status of each dimension in step 3, each dimension will be scored.

5) The Acquisition of the Evaluation Result

At the end of the scoring of each dimension, it is necessary to perform a weighted calculation based on each score to obtain the score of the entire evaluated object. The presentation of the evaluation results is described in clause 5.2.3.

5.2 Scoring principles and specification of the single scenario

5.2.1 Scoring principles and specification

According to the evaluating process defined, the evaluation of categories for single scenario involves two parts:

1) Scoring of each evaluation dimension ($S_{mmi}, S_{dmp}, S_{dca}, S_{di}, S_{ea}$):

The purpose of this step is to complete the scoring of ManMachine Interface, Decision Making Participation, Data Collection and Analysis, Degree of Intelligence and Environment Adaptability, and lay the foundation for the overall scoring of the evaluation object. Note that inevitable subjective factors will influence the evaluation.

According to Table 4-1, the score of each dimension can be divided into six categories: S=0, S=1, S=2, S=3, S=4, S=5. The scoring rules are as follows:

- S_{mmi}: means the score of ManMachine Interface. According to Tables 5-1 and 5-2, Interface Mode is the index that has the greatest impact on the score of this dimension. For example, when the interface mode is command, the dimension score is S=0 or S=1. But the more accurate score can be determined by two other indices: User Requirements and System Requirements. Obviously, when S=1, the requirements generated by the system should be greater than the user's, or the system can better understand the command.
- S_{dmp}: means the score of Decision Making Participation. Decision-making Methods is the index that has the greatest impact on the score of this dimension. When the proportion of work done by the system is 0 %, S=0; When the proportion of work done by the system is less than 50 %, S=1; When the proportion of work done by the system is 50 %~75 %, S1=2; When the proportion of work done by the system is 75 %~90 %, S=3; When the proportion of work done by the system is more than 90 %, S=4. When the proportion of work done by the system is 100 %, S=5. The percentage can be determined by two other indices of the evaluated object: Decision-making Dimension and Decision-making Results.
- S_{dca}: means the score of Data Collection and Analysis. Collection Methods is the index that has the greatest impact on the score of this dimension. When the proportion of work done by the system is 0 %, S=0; When the proportion of work done by the system is less than 50 %, S=1; When the proportion of work done by the system is 50 %~75 %, S1=2; When the proportion of work done by the system is 75 %~90 %, S=3; When the proportion of work done by the system is more than 90 %, S=4. When the proportion of work done by the system is 100 %, S=5. The percentage can be determined by two other indices of the evaluated object: Collection Content and Collection Results.
- S_{di}: means the score of Degree of Intelligence. Analysis Methods is the index that has the greatest impact on the score of this dimension. When the proportion of work done by the system is 0 %, S=0; When the proportion of work done by the system is less than 50 %, S=1; When the proportion of work done by the system is 50 %~75 %, S1=2; When the proportion of work done by the system is 75 %~90 %, S=3; When the proportion of work done by the system is more than 90 %, S=4. When the proportion of work done by the system is 100 %, S=5. The percentage can be determined by two other indices of the evaluated object: Analysis Content and Analysis Results.
- S_{ea}: means the score of Environment Adaptability.

NOTE: How to quantify environmental change needs further study.

2) The overall scoring of evaluation object (S):

After completing the evaluation of each dimension, the overall score of the evaluation object can be completed based on the following formula：

$$\mathrm{S} = \mathrm{w}_{\mathrm{mmi}} \times S_{mmi} + \mathrm{w}_{\mathrm{dmp}} \times \mathrm{S}_{\mathrm{dmp}} + w_{dca} \times S_{dca} + w_{di} \times S_{di} + w_{ea} \times S_{ea}$$

$\mathrm{w}_{\mathrm{mmi}}$ means the weight of ManMachine Interface.

$\mathrm{w}_{\mathrm{dmp}}$ means the weight of Decision Making Participation in overall scoring.

$\mathrm{w}_{\mathrm{dca}}$ means the weight of Data Collection and Analysis in overall scoring.

w_{di} means the weight of Degree of Intelligence in overall scoring.

w_{ea} means the weight of Environment Adaptability in overall scoring.

The weight can be determined by the following methods:

- Expert experience.
- From the perspective of evaluation dimension, it can be determined by some fuzzy quantization algorithms, e.g. the Analytic Hierarchy Process (AHP) introduced in clause 5.2.2.
- From the perspective of key effect indicators of evaluation objects, the weight is determined by analysing the influence of dimensions on effect indicators, e.g. accuracy, real-time, unit income, etc.

The corresponding relation between network autonomicity categories and overall score is shown in Table 5-3.

Table 5-3: The corresponding relation between categories and overall Score

Category	Score (S)
L0	$S < 1$
L1	$1 \leq S < 2$
L2	$2 \leq S < 3$
L3	$3 \leq S < 4$
L4	$4 \leq S < 5$
L5	$S = 5$

5.2.2 Weights determined by Analytic Hierarchy Process

Analytic Hierarchy Process (AHP) is a decision analysis method that combines qualitative and quantitative methods to solve complex multi-objective problems. The specific steps of applying this method to evaluate network autonomicity categories are as follows:

1) Establish a hierarchical model

Firstly, according to the relationship among the decision alternative (categories), decision criteria (dimension) and target (evaluation objects), it is divided into the highest level, the middle level and the lowest level, as shown in Figure 5-2:

- The highest level refers to the purpose of the decision or the problem to be solved. Here, the verification goal is the autonomicity categories of the evaluation object.
- The middle level refers to the factors to be considered or the criteria for decision making. Here, it refers to the evaluation dimensions.
- The lowest level refers to the alternatives for decision making, here it refers to categories L0 ~ L5.

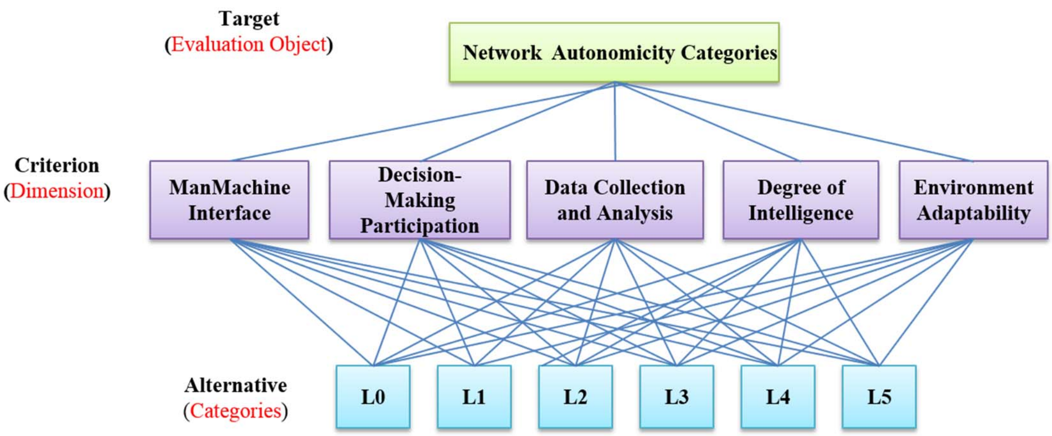

Figure 5-2: Hierarchy chart of network autonomicity categories

2) Constructing a judgment(paired comparison) matrix A

- Expert experience is used to judge the importance of each criterion relative to the target, the quantification value of the importance degree of each criterion(dimensions) compared with other criteria is given reasonably, which can be obtained through Table 5-4.

Table 5-4: Quantitative value of the importance of each dimension

Comparison between criterion I and criterion J	Quantization value
Equally important	1
Slightly important	3
More important	5
Strongly important	7
Extremely important	9
Intermediate value of two adjacent judgments	2, 4, 6, 8

- The weights are arranged in order to construct the following judgment (paired comparison) matrix:

$$A = \begin{Bmatrix} a_{mmi\_mmi} & a_{mmi\_dmp} & a_{mmi\_dca} & a_{mmi\_di} & a_{mmi\_ea} \\ a_{dmp\_mmi} & a_{dmp\_dmp} & a_{dmp\_dca} & a_{dmp\_di} & a_{dmp\_ea} \\ a_{dca\_mmi} & a_{dca\_dmp} & a_{dca\_dca} & a_{dca\_di} & a_{dca\_ea} \\ a_{di\_mmi} & a_{di\_dmp} & a_{di\_dca} & a_{di\_di} & a_{di\_ea} \\ a_{ea\_mmi} & a_{ea\_dmp} & a_{ea\_dca} & a_{ea\_di} & a_{ea\_ea} \end{Bmatrix}$$

a_{mmi_mmi} means the quantization value of comparison between ManMachine Interface and ManMachine Interface.

a_{mmi_dmp} means the quantization value of comparison between ManMachine Interface and Decision Making Participation.

a_{mmi_dca} means the quantization value of comparison between ManMachine Interface and Data Collection and Analysis.

a_{mmi_di} means the quantization value of comparison between ManMachine Interface and Degree of Intelligence.

a_{mmi_ea} means the quantization value of comparison between ManMachine Interface and Environment Adaptability. Others and so on.

3) Consistency test and weight determination

The eigenvector corresponding to the largest eigenvalue (λ_{max}) of the judgment matrix is normalized to W. Generally, when consistency ratio $\mathrm{CR} = \frac{CI}{RI} < 0{,}1$, it is considered that the degree of inconsistency of A is within the allowable range, with satisfactory consistency, and passes the consistency test. The final weight vector can be obtained by its normalized eigenvector:

$$W = \{w_{ac}, w_{da}, w_{an}, w_{de}, w_{dm}\}$$

Otherwise, the paired comparison matrix A should be reconstructed.

- The consistency index CI is defined as $\mathrm{CI} = \frac{\lambda - n}{n-1}$: n represents as the number of dimensions; when $\mathrm{CI} = 0$, it means complete consistency; the greater the value of CI, the greater the inconsistency.

- In order to measure the scope of CI, the random consistency index RI is introduced, as shown in Table 5-5.

Table 5-5: The values of RI (Random Index)

n	1	2	3	4	5	6	7	8	9	10	11
RI	0	0	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51

5.2.3 Recommended values of KPI for each intelligent level in some scenarios

Network KPI is an important reference to evaluate the level of network intelligence, and can even be one of the decisive factors.

After determining the intelligence level of the evaluation object through the methods mentioned in clauses 5.2.1 and 5.2.2, find out the KPI that the evaluation object needs to meet in this level according to Table 5-6. If not, it can be concluded that the evaluation result is not convincing.

Instruction:

1) Due to the diversity of network intelligent application scenarios, Table 5-6 only lists the common typical scenarios of existing stage studies, and KPI indicators of each level are for reference only.

2) At present, the intelligence level of most scenarios is between L1 and L2, while L5 is the long-term goal of intelligence. Therefore, the proposed KPI for L1 and L5 is not required to be provided temporary.

Table 5-6: Recommended values of KPI for each intelligent level in some scenarios

Lifecycle	Application scenario	KPI for CSP	Significance	Target value of L2	Target value of L3	Target value of L4
Network Planning	Network capacity expansion planning	Expansion accuracy	Cost reduction	90 %	92 %	95 %
Network Deployment	Network agile deployment	Preparation time of devices deployment	Operation efficiency improvement	2 minutes	N/A	N/A
	Wireless network management deployment	Installation time of network management	Operation efficiency improvement	Silent (Auto) install < 120 minutes	Automatic north interface docking, Self-checking, deployment report output < 90 minutes	N/A
	Intelligent base station opening	Amount and duration of base station data configuration parameters	Operation efficiency improvement	Number of templated adjustment parameters < 20	Time from automatic site opening to report output < 60 minutes	N/A
Network Maintenance	Network anomaly detection, diagnosis and intelligent recovery	Average unavailable time of monthly special line business	Network quality improvement	1 hours	0,5 hours	0,3 hours
	Analysis and diagnosis of low optical power level in PON link	Low optical power level rate of ONU	Network quality improvement	Accuracy of diagnosis and analysis > 70 %	Accuracy of diagnosis and analysis > 80 %	Accuracy of diagnosis and analysis > 90 %
	Network fault root-cause analysis	Alarm compression rate; Alarm automatic root cause analysis accuracy	Operation efficiency improvement	Realize root cause analysis and compression of top6 alarm: automatic analysis rate > 70 %, compression > 45 %	Realize root cause analysis and compression of all alarms: automatic analysis rate > 90 %, compression > 70 %	Alarm root cause diagnosis and self-healing accuracy rate > 90 %
Network Optimization in real-time	CDN intelligent scheduling	CDN traffic balance deviation	Network utilization improvement	20 %	10 %	5 %
	KPI analysis and optimization	CDN hotspot miss rate	User experience improvement	25 %	10 %	5 %
		Automation proportion of KPI optimization process	Network quality improvement	Achieve basic perception automation rate > 85 %	The accuracy of anomaly index and cell identification > 80 %; the accuracy of automatic output optimization scheme > 85 %	30 % improvement of major KPI
	Intelligent Energy Management of BS	Energy saving effect	cost reduction	Energy saving rate in idle time > 20 %	Energy saving rate in idle time > 25 %	Energy saving rate in idle time > 30 %

5.2.4 Presentation of evaluation result

In order to better demonstrate the process and results of the category evaluation, tuples and radar maps can be used to represent them.

1) Representation in quintuple form

In order to fully display the key information of the evaluation object, it is expressed as follows:

{Name of evaluation object, Autonomous domain, Subsystem, Network lifecycle, Category}

Autonomous domain includes RAN, Transport, Core Network, Wireless network, Fixed Access, etc.

2) Representation in radar map

As shown in Figure 5-3, each axis of radar map represents an evaluation dimension. Radar map can intuitively represent the distribution state of intelligence degree of each dimension. At the same time, it can intuitively compare the current status with the evolution targets (next level) of evaluation object.

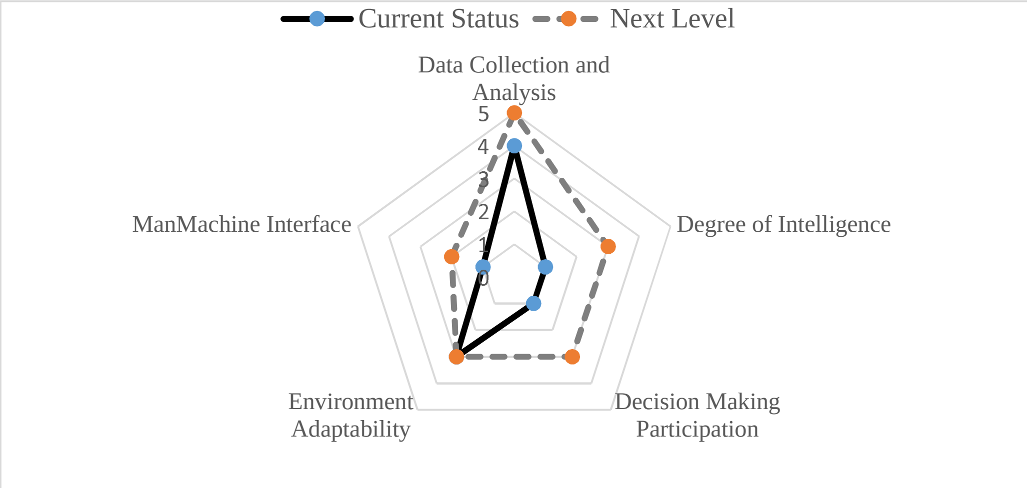

Figure 5-3: Example of radar map representation of categories evaluation results

5.3 Scoring principles and specification of the part of network lifecycle

5.3.1 Explorations on evaluation of network deployment autonomicity categories

Based on the scoring principles and specification of single scenario, further in order to realize the evaluation of the entire network autonomicity categories, it is necessary to explore the network lifecycle. This clause takes the Network Deployment as an example to explore the intelligent level evaluation for the network lifecycle.

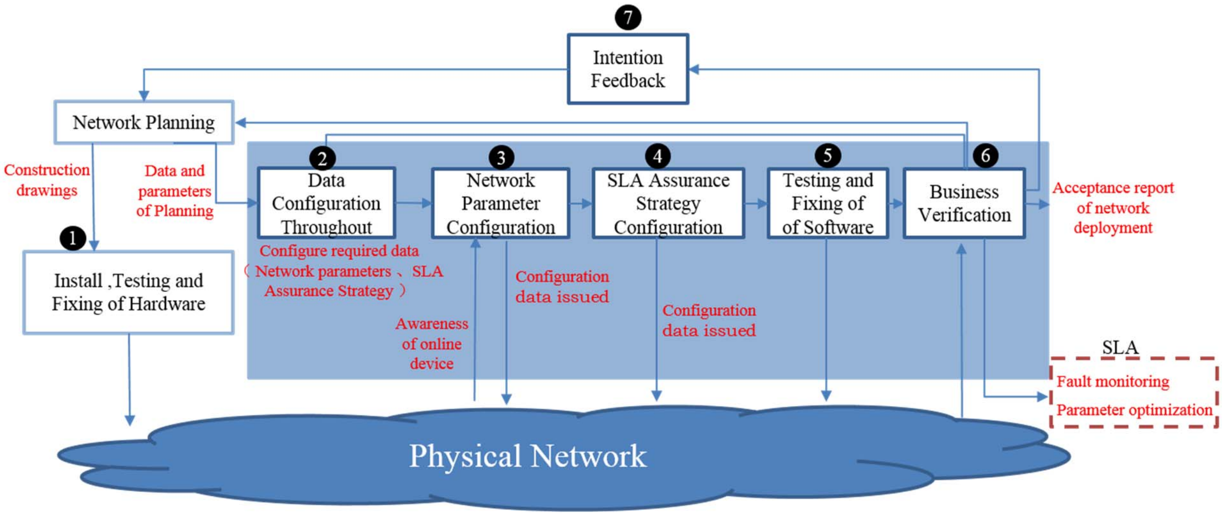

Figure 5-4: The Closed-loop of Network Deployment

As shown in Figure 5-4, the closed-loop of Network Deployment, including 7 steps throughout: Install, Testing and Fixing of Hardware, Data Configuration Throughout, Network Parameter Configuration, SLA Assurance Strategy Configuration, Testing and Fixing of Software, Business Verification and Intention Feedback.

Step 1 Install, Testing and Fixing of Hardware: Install the network hardware devices according to the construction drawings produced in the Network Planning stage.

Step 2 Data Configuration: Analyse and process the collected network raw data, and configure the data required by the links of Network Parameter Configuration and SLA Assurance Strategy Configuration.

Step 3 Network Parameter Configuration: Responsible for the awareness of online devices and distribution of network parameter configuration data.

Step 4 SLA Assurance Strategy Configuration: Distribute SLA assurance strategy configuration data based on the results of Data Production, and be responsible for dynamic adjustment of assurance strategy.

Step 5 Testing and Fixing of Software: Responsible for the generation and implementation of the network software debugging scheme, analysing and optimizing the software according to the debugging results.

Step 6 Business Verification: Responsible for the generation and implementation of the validation scheme, analysis and decision-making of the verification results based on the fault monitoring; Feedback the results of Business Verification to Link 2; Output the acceptance report of network deployment.

Step 7 Intention Feedback: Carry out requirement analysis again based on the acceptance report, output to the planning and design stage, and optimize the network planning scheme and construction drawings.

The evaluation content of Network Deployment is shown in Table 5-7, 5 dimensions (ManMachine Interface, Decision Making Participation, Data Collection and Analysis, etc.) of the above 7 steps throughout should be analysed respectively（"/" indicates that this dimension is not involved in this step).

Table 5-7: Relationship between 7 steps throughout and 5 evaluation dimensions of Network Deployment

Step/ Dimension	Install, Testing and Fixing of Hardware	Data Configuration	Network Parameter Configuration	SLA Assurance Strategy Configuration	Testing and Fixing of Software	Business Verification	Intention Feedback
ManMachine Interface	√	/	√	√	√	/	√
Decision Making Participation	/	/	√	√	/	√	/
Data Collection and Analysis	/	√	√	/	/	/	/
Degree of Intelligence	/	√	/	√	/	√	√
Environment Adaptability	√	/	/	/	√	/	/

Compared with a single system/scenario, the evaluation of network lifecycle is more complex, involving multiple systems and scenarios. Therefore, the corresponding evaluation dimensions (ManMachine Interface, Decision Making Participation, Data Collection and Analysis, etc.) are also transformed from a single action to an action with multiple steps.

Take the evaluation dimension Degree of Intelligence as an example, Figure 5-5 shows the comparison of Degree of Intelligence in single scenario and network lifecycle. The scoring content of Degree of Intelligence is detailed.

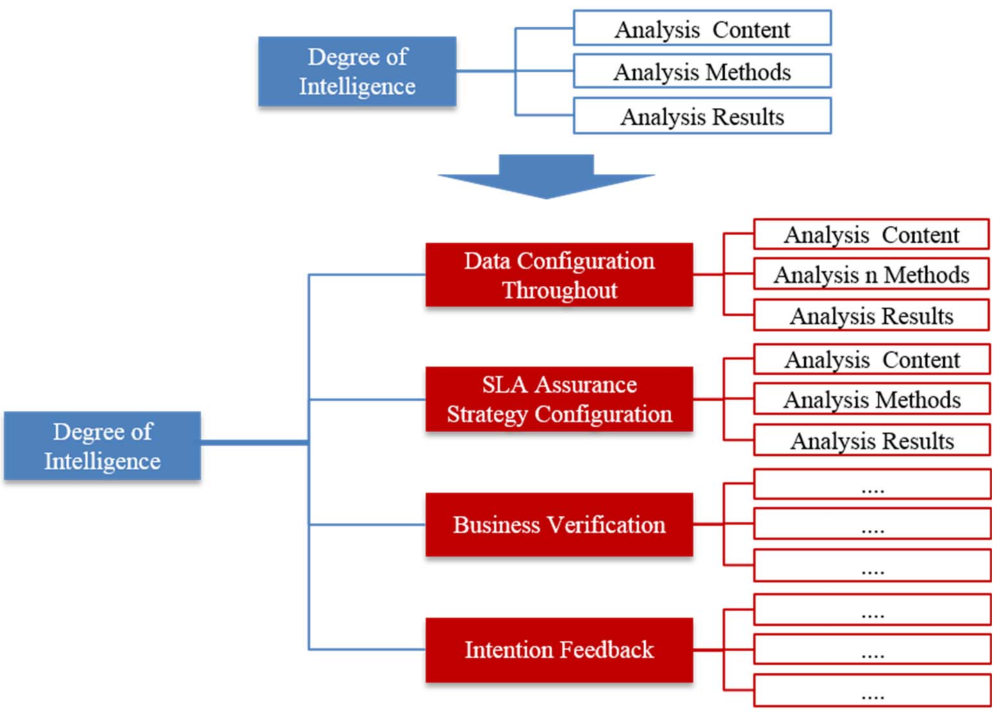

Figure 5-5: Comparison of evaluation dimension (Degree of Intelligence) in single scenario and network lifecycle

5.3.2 Explorations on evaluation of evaluation of the entire network autonomicity categories

As previously defined, the work-flow of activities of network lifecycle includes 6 phases: Network Planning, Network Deployment, Network Service Provisioning, Network Changes, Network Maintenance, Network Optimization in real-time. The category of entire network autonomicity is determined by all of them. This clause will introduce other phases except the Network Deployment described in clause 5.3.1, and analyse the steps to be considered in each phase.

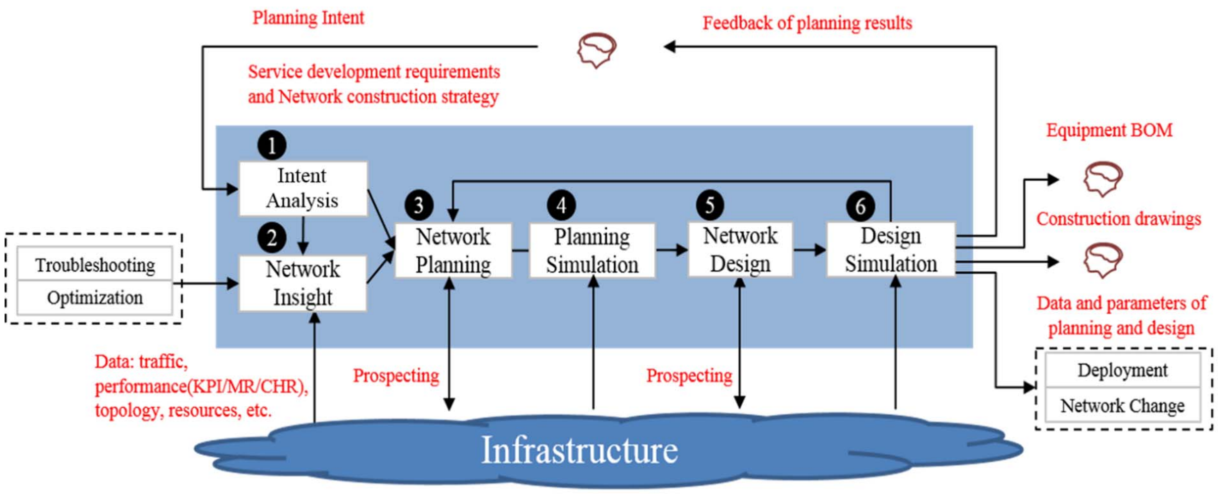

Figure 5-6: The Closed-loop of Network Planning

As shown in Figure 5-6, the closed-loop of Network Planning includes 6 steps throughout:

Step 1 Intent Analysis: Output network planning requirements (coverage area, capacity demand, etc.) according to user's business intention, service development requirement and network construction strategy.

Step 2 Network Insight: According to the requirements of troubleshooting and network optimization, insight and analysis of the network situation based on the data of traffic, performance, topology, resource, etc. And output the insight analysis report (such as network capacity prediction, etc.).

Step 3 Network Planning: Output HLD (network architecture, capacity requirements, networking scheme, etc.) according to the network planning requirements of intention translation and insight analysis results.

Step 4 Planning Simulation: According to the results of network planning, the correctness and rationality of HLD scheme planning are evaluated and tested by simulation.

Step 5 Network Design: According to the HLD scheme, combined with the current network prospecting, equipment procurement selection, networking technical requirements in the solution and other factors, output LLD (such as naming specification, address planning, number of wireless site cells, frequency points, bandwidth, TAC, etc.).

Step 6 Design Simulation: According to the results of network design, the correctness and rationality of LLD scheme planning are evaluated and tested by simulation.

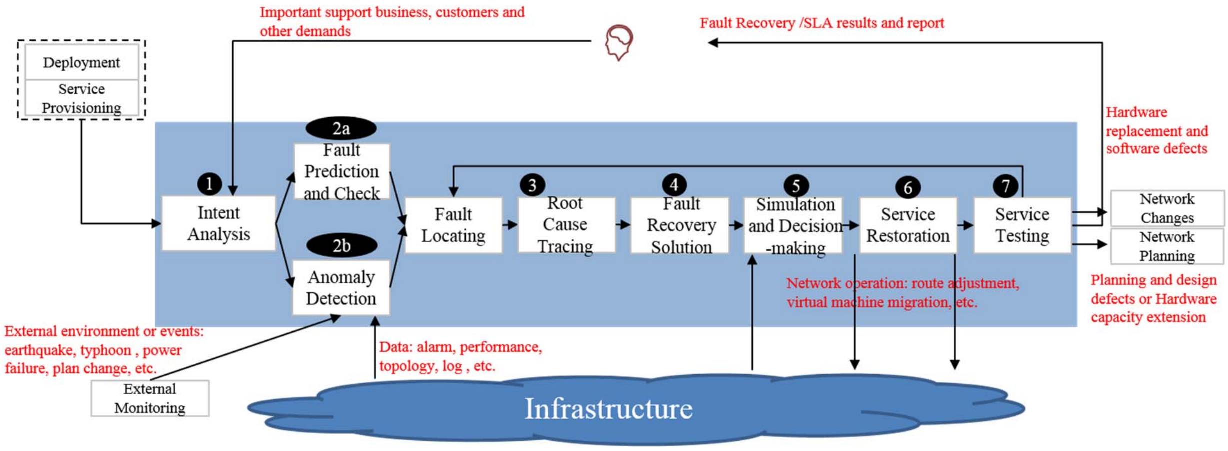

Figure 5-7: The Closed-loop of Network Maintenance

As shown in Figure 5-7, the closed-loop of Network Maintenance includes 8 steps throughout:

Step 1 Intent Analysis: Determine network monitoring rules (such as monitoring area, monitoring object (e.g. network element or service), alarm category, alarm level, KPI category, report alarm strategy on KPI exception, etc.) according to the monitoring support demands of important business/customers, as well as the SLA assurance strategy of network deployment and service provisioning. The system monitors the network based on these network monitoring rules.

Step 2a Fault Prediction and Check: Monitor and analyse the network operation data and external environment data, predict the development trend of network software and hardware status, and discover the potential hazards that may lead to abnormal in advance.

Step 2b Anomaly Detection: Monitor and analyse the network operation data and external environment data, timely find out the unplanned service interruption or service quality degradation of the network.

Step 3 Root Cause Tracing: Trace the specific hardware and software reasons (configuration, board, optical module, etc.) of the fault, which can support the generation of the fault recovery solution and repair the business as soon as possible.

Step 4 Fault Recovery Solution: Generate several alternative repair/recovery schemes (such as modifying the configuration, restarting the network element, replacing the board, isolating the network element, etc.) according to the result of the fault root cause tracing.

Step 5 Simulation and Decision-making: Comprehensive evaluation of alternative recovery schemes (such as whether the repair solution can solve the problem, whether the repair cost is acceptable, and the additional impact on the network), and output the optimal solution.

Step 6 Service Restoration: According to the optimal scheme after the evaluation decision, the fault recovery and hidden danger elimination actions are carried out.

Step 7 Service Testing: After the fault recovery and hidden danger elimination actions are implemented, the implementation results are verified and confirmed, such as whether the business service interruption is restored, whether the quality deterioration is restored, whether the alarm and KPI exception are eliminated.

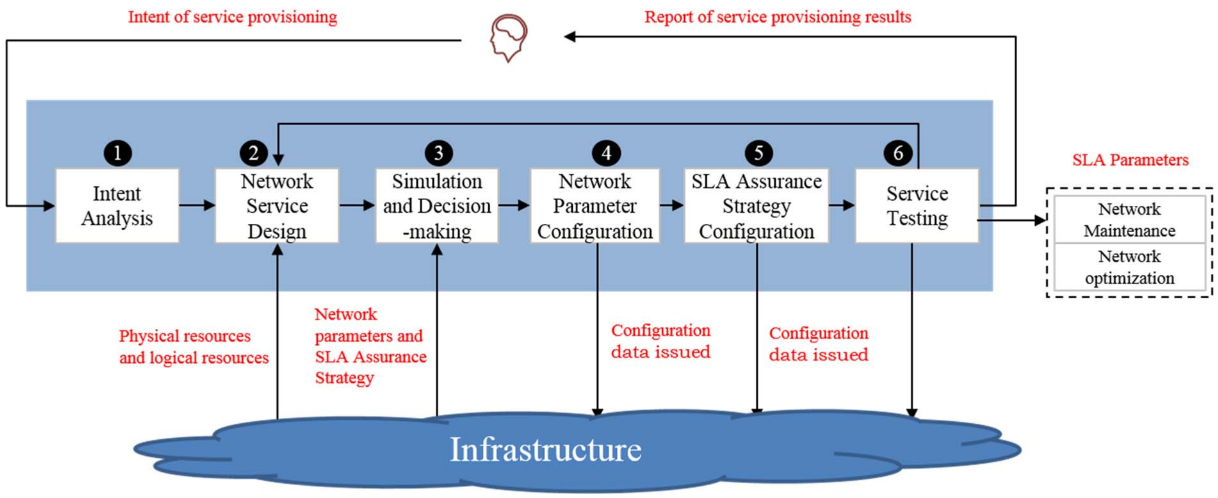

Figure 5-8: The Closed-loop of Network Service Provisioning

As shown in Figure 5-8, he closed-loop of Network Service Provisioning includes 6 steps throughout:

Step 1 Intent Analysis: According to the user's business service demands (such as the number of user's sites, site location, traffic volume, security demands, etc.), it is translated into specific network requirements (such as bearer technology, protection requirements, network element (including VNF) list, security policy, SLA assurance strategy, etc.).

Step 2 Network Service Design: Design service provisioning scheme (topology, protocol, protection scheme, resource allocation, etc.) based on the translated network requirements.

Step 3 Simulation and Decision-making: Comprehensively evaluate the service provisioning scheme (such as whether it meets the demands of users, whether it affects the existing business, whether the resources meet the requirements, etc.), and output the evaluation results.

Step 4 Network Parameter Configuration: According to the final scheme after evaluation and decision, the network parameters are issued to the network.

Step 5 SLA Assurance Strategy Configuration: According to the final scheme after evaluation and decision, the SLA assurance strategy is issued to the network.

Step 6 Service Testing: After the implementation of the scheme, the implementation results are verified and confirmed, such as whether the business is connected, whether the service SLA meets the requirements, etc.

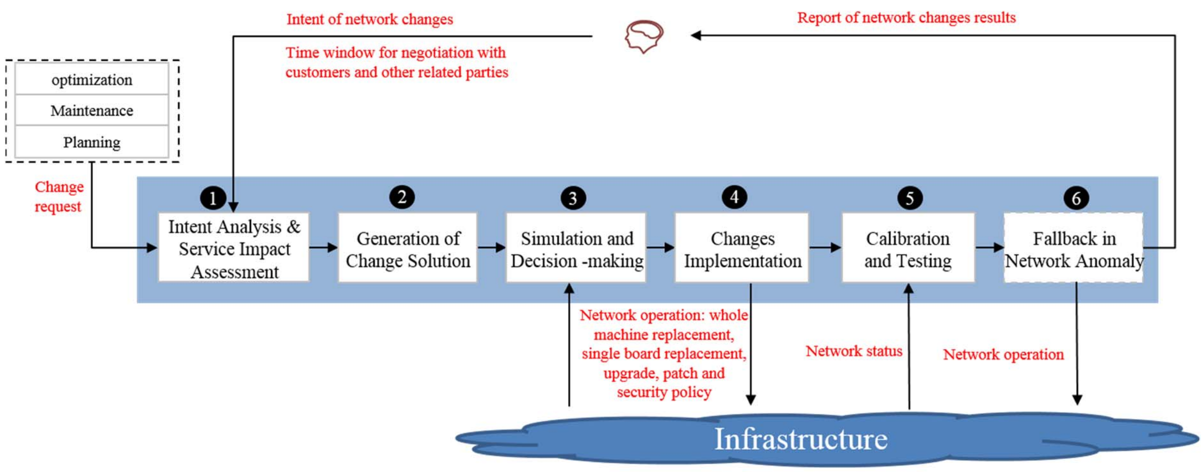

Figure 5-9: The Closed-loop of Network Changes

As shown in Figure 5-9, the closed-loop of Network Changes includes 6 steps throughout:

Step 1 Intent Analysis & Service Impact Assessment: According to the network change request (change type, area scope, network element involved, etc.), evaluate the user range affected by the change, and output the change constraint conditions (such as change time window, service interruptible time, etc.) in combination with the factors such as user business SLA and allowed change time period.

Step 2 Generation of Change Solution: According to the change constraints of user intention and business impact assessment output, complete the alternative change scheme design.

Step 3 Simulation and Decision-making: Comprehensive evaluation of alternative change schemes (e.g. satisfaction of change constraints, acceptability of cost, etc.), and output the optimal scheme.

Step 4 Changes Implementation: Translate the optimal scheme into implementation instructions and issue them to the network infrastructure.

Step 5 Calibration and Testing: After the implementation of network changes, calibrate and test the implementation results, such as whether the business SLA achieves the expected objectives.

Step 6 Fallback in Network Anomaly: Monitor the network status and fallback in time when network anomaly occurs.

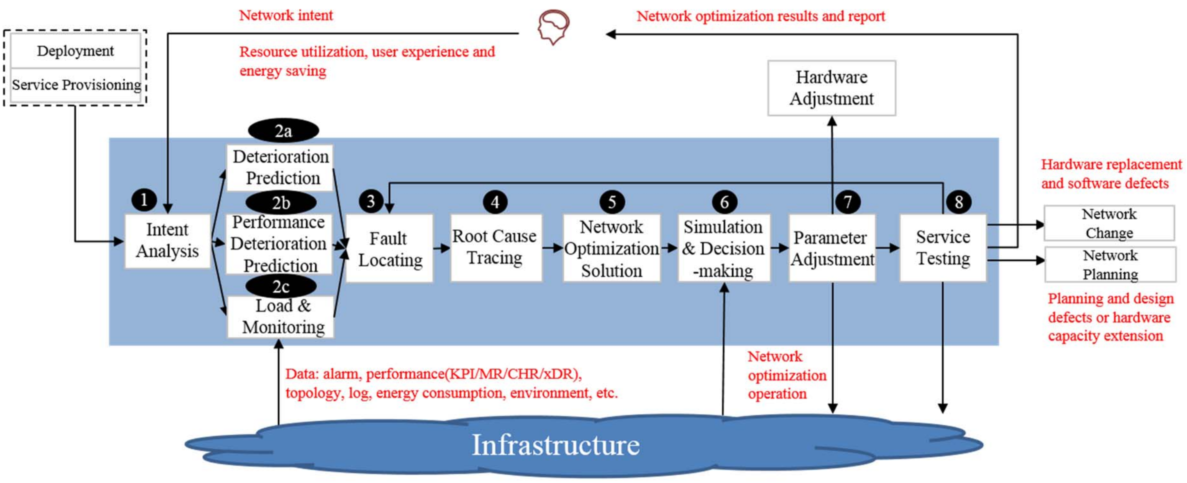

Figure 5-10: The Closed-loop of Network Optimization in real-time

As shown in Figure 5-10, he closed-loop of Network Optimization includes 10 steps throughout:

Step 1 Intent Analysis: According to the requirements of resource utilization, reservation rate, user experience, energy saving, public opinion analysis and user initiative planning/promotion, the network monitoring rules (such as monitoring area, monitoring object (such as network element or business), KPI category, reporting alarm strategy on KPI exception, etc.) are determined.

Step 2a Deterioration Prediction: Monitor and analyse the network operation data (such as alarm, KPI, KQI, topology, log, etc.) and external environment data, predict the development trend of network performance/resource utilization, and discover the potential risks that may affect customer experience (such as insufficient capacity on holidays and insufficient license).

Step 2b Performance Optimization Identification: Monitor and analyse the network operation data and external environment data and timely identification of the problems to be optimized that affect customer experience (such as weak coverage area), unreasonable resource use (excessive energy consumption, uneven resource load), or user active performance potential tapping identification.

Step 2c Load & Monitoring: The system monitors the network status and collect data based on the network monitoring rules.

Step 3 Fault Locating: According to the abnormal performance identification or deterioration prediction information, delimit the fault combined with the environmental monitoring situation. For cross domain scenarios, they are delimited to specific technical domains (such as wireless, transport and core), and for single domain scenarios, they are delimited to specific optimization objects (such as network elements).

Step 4 Root Cause Tracing: According to the results of problem/fault demarcation, trace and locate the specific hardware and software causes (configuration, air conditioning, dynamic loop, etc.) that lead to abnormal performance, and support the generation of network optimization solution.

Step 5 Network Optimization Solution: According to the result of step 3 and step 4, output several alternative parameter adjustment schemes (such as modifying software parameters, adjusting hardware, etc.).

Step 6 Simulation and Decision-making: Comprehensive evaluation of alternative parameter adjustment schemes (such as whether it affects the customer experience, whether the adjustment scheme meets the optimization goal, whether the adjustment cost is acceptable), and output the optimal scheme.

Step 7 Parameter Adjustment: According to the optimal scheme after simulation and evaluation, issue the optimized parameter configuration to the network.

Step 8 Service Testing: After the execution of the parameter adjustment action, verify and confirm the execution results, such as whether the customer experience, energy saving requirements and resource utilization meet the requirements.

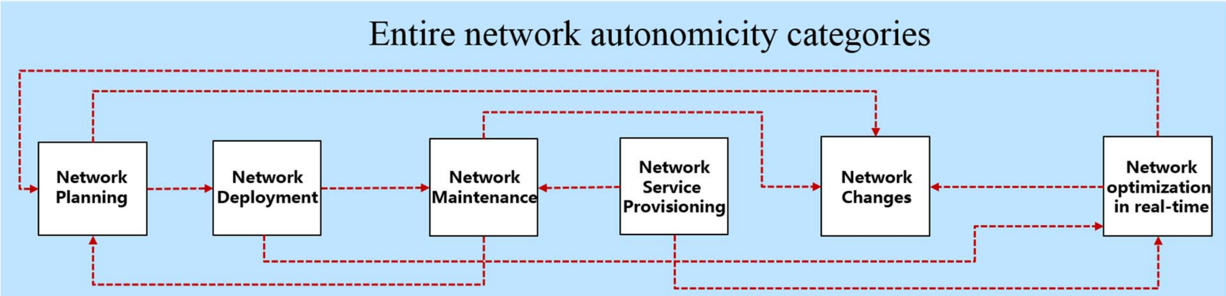

Figure 5-11: The whole lifecycle chart of communication network

After the evaluation and scoring of Network Planning, Network Deployment, Network Service Provisioning, Network Changes, Network Maintenance, Network Optimization in real-time, the score of the entire network can be calculated by the following two ways:

1) Calculates average based on following formula, which cannot reveal different features of each phase in network lifecycle, while can avoid impact of subjective factor:

$$S = \frac{S_{np}+S_{nd}+S_{ns}+S_{nc}+S_{nm}+S_{no}}{4}$$

S_{np} means the score of Network Planning.

S_{nd} means the score of Network Deployment.

S_{ns} means the score of Network Service Provisioning.

S_{ns} means the score of Network Changes.

S_{nm} means the score of Network Maintenance.

S_{no} means the score of Network Optimization in real-time.

Calculates weighted sum based on following formula, which can reveal different features of each phase in network lifecycle. But predefined weight coefficients are affected by subjective factor:

$$S = w_{np}S_{np} + w_{nd}S_{nd} + w_{ns}S_{ns} + w_{nc}S_{nc} + w_{nm}S_{nm} + w_{no}S_{no}$$

w_{np} means the weight of Network Planning.

w_{nd} means the weight of Network Deployment.

w_{ns} means the weight of Network Service Provisioning.

w_{nc} means the weight of Network Changes.

w_{nm} means the weight of Network Maintenance.

w_{no} means the weight of Network Optimization in real-time.

5.4 The relationship among the network infrastructure capabilities (KPI) and the network intelligence levels

Standard operation management tasks refer to the operation management tasks that define the L0-L5 management and operation intelligence level grading technical requirements in the professional field of network management and operation intelligence level. As shown in Figure 5-12, different colour blocks express different grading technical requirements: white indicates that the operation management task is completed manually; Light green indicates that the operation management task is jointly completed by manual and information communication systems; Dark green indicates that the operational management task is completed by the information and communication system. In the grading technical requirements of the professional field, the intelligent level grading technology of the standard operation management tasks in the field is required to provide a specific text description. It should be noted that the intelligent capabilities of each operation management task are continuously evolving, and the colour is only a qualitative identification, and the requirements of the same colour of operation management intelligent capabilities can be different.

MANO	Task	L0	L1	L2	L3	L4	L5
Executive	TaskA1						
	TaskA2						
Cognition	TaskB1						
	TaskB2						
Analysis	TaskC1						
	TaskC2						
Decision Making	TaskD1						
	TaskD2						
Intent Management	TaskE1						
	TaskE2						

Figure 5-12: Graded technical requirements for L0-L5 of standard operations management tasks

Map the decomposed set of operations management tasks to the standard operations management tasks. In principle, each operation management task can correspond to a unique standard operation management task, and there cannot be a one-to-many situation. If an operations management task maps to multiple standard operations management tasks, the operations management task needs to be further decomposed.

When the operation management task corresponds to the only standard operation management task, the hierarchical technical requirements of the operation management task are obtained.

6 Application of quantitative evaluation criteria

6.1 Transport Network: 5G and DCN examples

6.1.1 General categorization criteria

Transport Network underpinning 5G and DCN (Data Centre Network) service are complex and error prone system, where automation of lifecycle operations could be particularly beneficial.

The reference lifecycle considers both infrastructure and service management:

1) Network Planning

2) Network Deployment

3) Network Service Provisioning

4) Network Change

5) Network Maintenance

6) Network Optimization

Within this exercise, autonomicity level 2 to 4 are considered due to the fact that current technologies either already have those functionalities available or there is a foreseeable evolution to make them available.

Refer to Table 4-2 for more information on Operator vs Network responsibilities and roles within each level of automation.

Level 2 automation:

1) Network Planning:
   a) Manual and tool-assisted analysis: capacity management, robustness analysis, and traffic direction analysis.
   b) Semi-automatic design based on offline tools and manual operations.

2) Network Deployment:
   a) New devices can be commissioned and managed by system automatically.
   b) Manual acceptance and commissioning procedure.
   c) Remote manual configuration.

3) Network Service Provisioning:
   a) Manual solution design based on network model and template, expert review and confirmation.
   b) Controller automatically provision the solution in live.
   c) Manual and tool assisted check and acceptance of the connectivity among the Applications and towards the external world.

4) Network Change:
   a) New releases and functionalities introduction done manually with help of Tools for basic consistency check.
   b) Manual acceptance and commissioning.
   c) Automatic rollback procedure available for configuration only.

5) Network Maintenance:

   a) Manually monitoring tools configuration and maintenance.

   b) Manually monitor alarms, log and performance indicators.

   c) Manually recover from fault conditions, workaround and automatic rerouting available from basic protection mechanisms and protocols.

6) Network Optimization

   a) No dynamic adaptation and overflow avoidance, possible packet loss.

   b) Detect service degradation based on fixed policies.

   c) Manual optimization based on experience.

Level 3 automation:

1) Network Planning:

   a) Capacity management, robustness analysis, and traffic direction analysis are automatically generated based on Declarative Policies, site distribution and service requirements.

   b) Automatically generate network planning solutions based on live network analysis results and service planning requirements.

   c) By means of Network Digital Twins (NDT), provide capacity simulation and traffic direction simulation to verify the designed solution.

2) Network Deployment:

   a) Automatic configuration deployment.

   b) Automatic acceptance and automatic execution of acceptance test cases.

   c) Connectivity and performance test execution.

3) Network Service Provisioning:

   a) Declarative Policies Service request interpretation (e.g. Service Provisioning, SLA definition).

   b) Automatic service design creation and resource allocation.

   c) Service simulation and verification before implementation by means of NDT.

   d) Automatic service implementation and acceptance.

   e) Automatic service rollback in case of failure.

   f) Services are automatically verified after deployment Monitoring tasks are automatically created.

4) Network Changes.

5) Rule based service Declarative Policies from Operator influence the generation of automatic online change:

   a) Automatically deploy new release and new features adapting design.

   b) Supports network simulation (utilizing NDT) before deployment:

      - reachability/isolation, loop, black hole and path simulation of impacted services;

      - simulation of impact on existing services;

      - Manually select the more fitting according to the simulation result.

   c) Automatically execute deployment operations and acceptance tests.

   d) Automatic roll-back to previous snapshot of network configuration.

6) Network Maintenance:

   a) Service driven telemetry, with automatic choice of relevant indicators.

   b) Automatically perform Root Cause Analysis of active faults.

   c) Automatic recommendation of fault remediation.

   d) Update Knowledge Base when according to the Customer confirmation of Fault resolution to refine the recommendation of the best solution.

7) Network Optimization:

   a) Redirect flows automatically according to priorities, aiming at zero packet loss.

   b) Establish dynamic baseline to detect service SLA deterioration.

   c) Automatic actions recommendation, with manual confirmation.

   d) Simulation of optimization actions effects by means of NDT.

   e) Automatic deployment and verification.

Level 4 automation:

1) Network Planning:

   a) Collect Planning Intent from Operators to autonomously Plan the network accordingly.

   b) Obtain live network information online and predict the capacity and traffic direction.

   c) Autonomously generate network planning solutions based on forecast results and service planning requirements.

2) Network Deployment:

   a) Autonomous generation of deployment error correction policies.

   b) Software acceptance errors are automatically corrected.

   c) Provide rectification suggestions for hardware acceptance errors.

3) Network Service Provisioning:

   a) Customer provide Intent as way to request what he wants but giving no indications on how to realize it.

   b) The system autonomously completes the simulation of Service Deployment verifying the impact on the existing services and resources by means of NDT.

   c) The system autonomously performs acceptance and provides an acceptance report.

   d) Any discrepancies are corrected autonomously.

4) Network Changes:

   a) Autonomously design network changes according to service intent (e.g. network evolution, service migration, topology change, device upgrade) evaluating impacts and alternatives using simulations (NDT). Autonomously select the more fitting according to active services in some scenarios.

   b) Autonomous design review and expansion according to observed and forecasted traffic/service evolution.

   c) Autonomous verification of the network change results generating report accordingly.

5) Network Maintenance:

   a) Autonomously select isolation and recovery plan better suited for current network status, reducing the impact on overall Service SLA impact.

b) Fault prediction for both Hardware and Software faults (e.g. memory leak, process hanging).

c) Fault self-healing.

6) Network Optimization:

a) Predictive service optimization, forecasting services need and anticipating overall optimization.

b) System simulation (using NDT) and what-if analysis, automatic decision-making.

6.1.2 5G transport example

In the following Table 6-1 an example of 5G transport network categorization with major procedure and target nodes is specified, detailing the list in clause 6.1.1.

Table 6-1: 5G transport Categorization Evaluation example

Full 5G transport lifecycle	Level 2		Level 3		Level 4	
	Key Features	Key Capabilities	Key Features	Key Capabilities	Key Features	Key Capabilities
Network Planning	Offline semi-automatic planning	New access rings, new areas (aggregation rings), new bearer networks, and 5G edge cloud manual offline design with automatic consistency check	On-line Automatic Planning Based on Simulation	New access rings, new bearer networks, and 5G edge cloud planning based on Network Digital Twin (NDT) capacity simulation and robustness analysis	Autonomous planning based on prediction	New access rings, new bearer networks, and 5G edge cloud planning based on evolution forecast (NDT) and service planning requirements
Network Deployment	Automatic device management and manual remote configuration	Commissioning and configure devices connected on the access ring, regional, or edge cloud remotely, with compatibility check	Devices automatically go online	Bringing devices on the access ring, regional, or edge cloud online with automatic configuration deployment and automatic acceptance test execution	Devices autonomously go online without manual software commissioning.	Bringing devices on the access ring, regional, or edge cloud online. Configuration related acceptance error automatically corrected
Service provisioning	Automatic service provisioning	VPN, tunnel and single-station service provisioning based on network model and template, with expert review and confirmation	Service-driven automation	1. 5G bearer: VPN service provisioning, intelligent clock provisioning, and slicing service automatic provisioning with service simulation and verification before implementation 2. 5G edge cloud: interconnection between the edge cloud and central cloud, interconnection between edge clouds, and collaboration between the edge cloud and bearer network	Intent-driven automation	Intent driven service management (e.g. new VPN site addition, new 5G MEC applications, and 5G B2B access). System performs in advance the simulation of Service Deployment verifying the impact on the existing services and resources by means of NDT. Compute

Full 5G transport lifecycle	Level 2		Level 3		Level 4	
	Key Features	**Key Capabilities**	**Key Features**	**Key Capabilities**	**Key Features**	**Key Capabilities**
Network change	Tool-assisted network change	Service migration (CPE relocation), topology change (ring addition or deletion, single-homing to dual-homing), capacity expansion and replacement (NEs, boards, and links), and version and patch change. Manual acceptance and commissioning, automatic rollback	Automatic network change	Service migration (base station port migration), topology change (ring addition or deletion, single-homing to dual-homing), capacity expansion and replacement (NEs, boards, and links), and version and patch change. Simulation (utilizing NDT) before deployment. Service driven telemetry with automatic choice of relevant indicators	Autonomous network change	Autonomously perform smooth evolution, ring to tree, service migration, topology change, capacity expansion and replacement, and version and patch change according to observed and forecasted traffic service evolution Autonomous verification of the network change result generating a report
Network Maintenance	Manual monitoring and troubleshooting	1. Network-level visibility 2. NE-level monitoring and troubleshooting 3. Manual monitor of alarm and performance 4. Manual recovery from fault conditions	Service- and network-level automatic monitoring and troubleshooting	1. Visualization: service visualization (service overview and single service) and network visualization (NEs, topologies, protocols, tunnels and slices) 2. Automatic service and network exception identification and troubleshooting 3. Automatic recommendation of fault remediation actions 4. Interaction with operator's Technical Expert to grow knowledge base	Autonomous Monitoring, troubleshooting and healing based on prediction	1. Visualization: service visualization (service overview and single service) and network visualization (NEs, topologies, protocols, tunnels, and slices) 2. Service and network exception identification and fault self-healing 3. Fault prediction for both Hardware and Software faults (e.g. memory leak, process hanging)
Network Optimization	Manual optimization	1. Tunnel-level optimization 2. No dynamic adaptation and no overflow avoidance, possible packet loss	Policy-based, manual decision-making and automatic optimization	Network optimization (such as link usage balancing) and service optimization (SLA assurance such as bandwidth and latency). NDT help in optimize the connection path by means of simulating the best overall resource assignment	Autonomous optimization based on service intents	1. Forecast-based optimization by means of NDT, where SLA breach forecast is simulated 2. Preventive connections path redefinition is triggered autonomously with SLA monitoring during the execution

6.1.3 DCN transport example

The DCN remit is another transport use case where the operational procedure will evolve according to the generic criteria identified in clause 6.1.1.

Table 6-2: DCN Categorization Evaluation example

Full DCN transport lifecycle	L2 Key Capabilities	L3 Key Capabilities	L4 Key Capabilities
Network Planning	System-aided DC network design and evaluation. Technical Expert supervise and review.	Automatic DC network design by means of pre-defined Declarative Policies (such as Creation or expansion of DC network) Automatically calculate DC needed network capacity. Automatically evaluate with pre-event simulation and manual decision-making.	Full-autonomous design based on DC network simplified planning intent and service evolution prediction. Autonomous error correction according to the result of pre-event simulation and post-event verification.
Network Deployment	Manually generate configurations of Router, Switch and Firewall, automatically bring online and deliver configurations.	Automatically generate configurations, automatically deployment, check topology and connectivity of the DC network by means of NDT.	Autonomously corrects errors in acceptance, correct configuration of DC connectivity.
Service provisioning	Manual design and expert review, Service fulfilment with predefined template (such as VPC, Subnet, Security-group, etc.).	Automatic design based on Declarative Policies service requests (such as application rollout, capacity expansion, offline, and mutual access) and real-time status of Fabric network, system-aided decision-making with automatic pre-event simulation, automatic acceptance and application monitoring.	Autonomous design based on customized and simplified service intent, specifying what is requested (e.g. which service, SLA). Autonomous cross check of resource impact on existing services before. Deployment, roll-out, verification and possible roll-back decision.
Network change	Manual change solution design (such as port, board and device replacement, or software upgrade and patch) according to constraints of SLA (acceptable service Interruption time and operation time window), automatically deliver configuration.	Automatic network changes to solution design based on Declarative Policies service requests (such as device capacity, server capacity and VAS capacity expansion, SW upgrade, patch management, device replacement, port replacement, etc.). System-aided decision-making with automatic pre-event simulation, multi-level rollback based on manual generated snapshots (such as fabric, tenant, VPC, etc.).	Autonomous change solution design based on simplified service intent and impact simulation (by means of NDT). Autonomous decision-making and snapshots generation.
Network Maintenance	Manually select predefined monitor template, automatic network status collection with SNMP polling and alarm reporting, network-level visibility with detailed indicator, manual inspection, troubleshooting and fault recovery.	Automatic monitor, automatic network status collection with real-time telemetry, visibility of device, network, protocol, overlay and application health status, visibility of fault and potential risk, automatic root cause analysis, system-aided fault recovery.	More accurate fault risk prediction, autonomous fault recovery and correction verification. Autonomous backup path creation granting SLA preservation.
Network Optimization	Fixed forwarding queue, best-effort forwarding.	Automatic flow control based on dynamic queue adjustment according to predefined traffic model.	Autonomously perform optimization and adjustment in advance based on service deterioration prediction (NDT) to ensure that the network continuously meets requirements.

6.1.4 IP Network Monitoring and Troubleshooting Process

In terms of IP network monitoring and troubleshooting capabilities, carriers expect to evaluate the availability of network resources and check and predict the health status in real time, identify network bottlenecks in real time, proactively detect 100 % faults, automatically and intelligently diagnose faults, and quickly self-healing services to reduce the impact on customers.

Based on the closed-loop elaboration process, the monitoring and troubleshooting process of IP networks can be divided into nine subtasks: intent translation, monitoring visualization, fault identification, potential risk prediction, demarcation and locating, solution generation, evaluation and decision-making, solution implementation, and service verification. These nine subtasks can be mapped to the general workflow of network management and operation, so that it is able to make further analyse the intelligent classification capability of each single task.

Based on the general network management and operation process reported in Figure 5-7, the closed-loop of network maintenance can be used to obtain the following tasks for IP networks:

- **Intent management tasks:**
  - Translation of monitoring and troubleshooting intent: convert network monitoring assurance requirements, such as monitoring scope, reliability requirements, and service SLA requirements, into specific operations for network monitoring assurance, such as collection objects, indicators, alarms, events, and logs, alarm aggregation and filtering, and fault mode matching. Rectify faults, such as recommendation and service self-healing.
- **Perception tasks:**
  - Visualized monitoring: monitors and collects network and service status, events, and performance indicators, analyses and processes the collected information, and displays the collected information in multiple dimensions.
- **Analysis tasks:**
  - Fault identification: aggregates alarms and events and identifies fault types.
  - Potential risk prediction: predicts and warns network resource consumption, network hardware subhealth, network security threats, and configuration potential risks.
  - Demarcation and locating: demarcate and locate network faults, perform correlation analysis on service-level problems and network-level problems, and determine the root cause of the faults.
  - Solution generation: a self-healing solution is generated for services affected by faults. If manual recovery is required, a description is provided.
- **Decision-making tasks:**
  - Evaluation and decision-making: simulate the service recovery solution, evaluate the simulation results, such as whether the simulation results meet user requirements, whether existing services are affected, and whether resources are satisfied, and determine the final recovery solution.
- **Execution tasks:**
  - Solution implementation: implement the recovery solution based on the decision-making result.
  - Service verification: verify and confirm the execution result of the recovery solution, including the service connectivity and whether the SLA meets requirements.

In Table 6-3 the description of Intelligent IP Network Monitoring and Troubleshooting procedure for the 6 Autonomous Levels can be found.

Table 6-3: Hierarchical capabilities of IP network monitoring and troubleshooting

General Process	Tasks	L0	L1	L2	L3	L4	L5
Intent management	**Monitor troubleshooting intent translation**	**Manual:** The network monitoring assurance requirements are converted to specific operations and fault analysis methods.	**Manual:** The network monitoring assurance requirements are converted to specific operations and fault analysis methods.	**Manual:** Transfer the network monitoring assurance requirements to specific operations and fault analysis methods.	**Templates are preset in the system. Users can select and adjust templates to complete the monitoring and troubleshooting intention translation.** The monitoring template and assurance policy are preconfigured in the system. During operation, the user selects the template and assurance policy based on the scenario to complete intent translation.	**Templates are preset in the system. During the running, the system automatically matches the template to complete monitoring and troubleshooting intent translation.** The system preconfigured monitoring templates and assurance policies. The system automatically selects templates and assurance policies based on scenarios during operation, and completes intent translation.	In all scenarios, the system automatically completes the entire process of intent mapping, monitoring visualization, fault identification, potential risk prediction, demarcation and location, recovery evaluation, and verification, implementing intelligent verification in all scenarios.

General Process	Tasks	L0	L1	L2	L3	L4	L5
Perceptions	**Monitoring**	**Manual:** Manually query and collect information about network and service status, events, and performance indicators.	**Use tools to simplify the collection process:** Users use tools to detect network and service status, events, and performance indicators.	**The resource collection template is preset in the system. The collection monitoring based on the service resource definition can be started.** When monitoring services, the personnel determine the resources used by the services and start the corresponding monitoring based on the preconfigured resource collection template.	**Users can start monitoring on demand. The system automatically breaks down monitoring tasks. Users can define visualized content online.** The system automatically starts monitoring resources used by services. Users can customize visualized content by dragging and developing scripts.	**The system automatically determines the monitoring scope and content as required, and recommends visualized content based on user monitoring behaviour.** The system can determine the monitoring scope and indicators based on the service running status, priority, and network situation.	
	Fault identification	**Manual:** Searching for Faults Triggered by User Complaints	**Use tools to periodically check the network to detect faults.** Identify network faults based on the information scanned by the tool.	**The system denoise and dedupe alarm events based on the preset rules.** Denoising and deduplication include alarm filtering and alarm flapping suppression.	**The system automatically aggregates alarm events and corresponds to the preset fault mode.** The system automatically extracts features of alarm events and related network resources and aggregates alarm events with AI algorithms.	**The system automatically learns the new fault mode and identifies unknown faults.** For unknown faults, the system can perform fault profiling and use the AI technology to form a new fault mode.	

General Process	Tasks	L0	L1	L2	L3	L4	L5
	Potential risk prediction	**Manual:** Network engineers manually check items one by one and identify potential risks.	**The system provides the trend chart of historical data. The following information based on experience can be predicted:** Network engineers identify potential risks based on data trends and maintenance experience.	**Based on historical data, the system uses algorithms to predict a few resource types.** The system provides prediction results based on historical data, with low accuracy.	**The system uses the AI algorithm to predict potential risks for most resources.** The system supports multi-dimensional feature extraction for data prediction, improving the accuracy.	**The system automatically starts AI-based prediction and provides prediction reliability.** The system supports predictive maintenance, predicts the service SLA trend and system resource usage trend, and provides the reliability of the trend prediction.	
Analysis	Fault Identification	**Manual:** Manually use ping and trace methods to demarcate the fault. Check logs, device status, and route information to locate the fault.	**Manually simplify operations with the help of tools:** The tool simplifies the process of obtaining information. The demarcation and locating still requires the personnel to perform operations and judgment based on experience.	**The system provides real-time network information and locates faults based on preset rules.** Based on maintenance experience, the system automatically locates faults based on the obtained data matching rules.	**Based on AI learning and inference, the system identifies the relationship between abnormal information and accurately locates the abnormal information.** Consolidate manual experience into AI features or knowledge graph to help identify relationships between abnormal information and automatically search for associated information for location.	**The system automatically learns fault propagation relationships in new scenarios and accurately identifies root causes.** The system algorithm has good generalization ability, less use of human experience, and can update fault propagation relationship in changing scenarios.	

General Process	Tasks	L0	L1	L2	L3	L4	L5
	Solution generation	**Manual:** Design a problem rectification solution based on the problem demarcation and location result.	**The system provides static rectification suggestions for specific faults.** The system preconfigured static rectification suggestions for specific faults, and personnel completed the rectification scheme based on the suggestions.	**The system supports online design and saving of the repair solution.** A repaired solution online by using scripts and commands can be designed. The solution can be saved or referenced.	**The system automatically matches the fault mode to generate a recovery solution.** Based on the demarcation and location result, the system automatically matches the repair process and generates a repair scheme.	**The system automatically learns the following rectification solutions for the new fault mode:** Rectify the fault mode automatically learned by the system.	
Decision-making	**Evaluation Decision**	**Manual:** Experts review the repair solution, provide review and correction opinions, and decide on the optimal solution.	**Manual:** Experts review the repair solution, provide review and correction comments, and select the optimal solution.	**The system supports simple analysis and verification of preconfigured rules to assist manual decision-making.** The network engineer reviews the alternative solution recommended by the system, selects and confirms the solution manually.	**The system provides the simulation result and recommends the optimal repair solution. The following is a manual decision:** The network engineer reviews the optimal solution recommended by the system and confirms the solution manually.	**The system automatically completes simulation and decision-making:** The system automatically decides the optimal scheme based on the pre-simulation calculation results.	
Execution	**Solution implementation**	**Labor:** The network engineer manually completes the repair according to the approved final solution.	**Single-step execution by using tools/systems:** Use tools/systems to perform the repair solution.	**The system automatically executes the entire process:** The system automatically executes all steps of the solution.	**The system automatically executes the entire process and supports rollback when an error occurs.** The system automatically executes all steps of the solution and rolls back the solution based on the policy error.	**Same as L3**	

General Process	Tasks	L0	L1	L2	L3	L4	L5
	Verify services	**Manual:** Perform service acceptance through service dialling test.	**Tools used by people:** The tool provides service dialling test, alarm observation, and service KPI observation capabilities. Users can perform service acceptance with the help of the tool.	**Perform step-by-step acceptance using the system:** The system supports the function of viewing object information in batches and assisting personnel to complete service acceptance.	**The system automatically performs the verification and provides the acceptance report.** The system automatically completes service acceptance, compares the service information before and after the execution, and generates an acceptance report.	Same as L3	

7 Suggested requirements of network infrastructure in different Categories

7.1 Knowledge Base

The Network Infrastructure tend to grow in Autonomicity within its evolution process due to the simplification of the Operational team tasks and due to the consequent OpEx reduction.

On the other side, trust in automation mechanisms is currently not widespread within Telco Operators.

For example, VNF autonomous scaling operation are still not enabled in many Telco Operators due to lack of trust in providing service continuity and in the underlying decision making process.

To properly increase in autonomicity, the Network have increased the level of confidence provided to the Telco Operator.

In particular, the network has to properly grow its Knowledge Base in term of technical and procedural aspects.

The basics of the Knowledge Base come from information contained in the Product Documentation, from direct observation of the network and services behaviours and so on.

To increase the Knowledge Base, the Network has to interact with the Domain Experts present within each Technology and Service related departments of the Telco Operator.

From Level 2 Autonomicity onwards, when the Network has to take a decision, it is not confident with, Technical Expert will continue to play their role.

Also, within level 5 Autonomicity, the Human Supervision will not be completely removed, levels defined in ETSI GR ENI 007 [i.3].

As an example within Car industry, level 5 Autonomous driving car has a system allowing a remote operator to take control in case of problems or unforeseen situations.

The Network have to present to the relevant Technical Experts the possible viable solutions (Recommendations) for them to provide indications on the proper way ahead, levels defined in ETSI GR ENI 007 [i.3].

The Technical Expert will receive the full details for all the viable alternatives, including evolution forecasts, SLA level and other elements that could be needed for the Technical Expert to evaluate each proposed alternative at best without having to investigate on its own further on.

The Technical Expert will select the more appropriate Recommendation, and the network will update its KB accordingly, to be able to increase its level of confidence whenever a similar situation will be faced again.

The Technical Expert will have a proper profile within the network, to properly get prompted when needed.

On top of this profiling, the network will be able to fine tune it based on multiple aspects:

- inputs they provide within the different domain;
- how often their suggestions and recommendations turn out to be correct from outcome perspective.

In this way, the system will increase be ability to address the proper set of experts for each recommendations/decision needed.

7.2 Tool for decision delegation according to Time Dimension

The Autonomous Network have to be able to execute and check the decided actions, but mainly what distinguish an Autonomous Network from an automatic one is the autonomicity in decision taking.

AI technology enable the network to recommend the proper way ahead when a decision needs to be taken.

Decision can be taken manually, network can recommend multiple solution for the Operator to choose from, automatically with the need for human validation, fully automatically.

The Operator can decide to delegate decisions responsibility to the network when it feels confident that the network will fulfil two factors:

1) take the best decision possible;

2) have low probability of side effects on the ongoing services and resources.

The responsibility delegation process involves Humans interaction, and as underlined in clause 6.1.1, also in level 5 there could be escalation in need for human intervention that remains accountable for the proper network delivery, management and evolution (see clause 4.2 on Responsibility Index description in 5 levels).

The Technical Experts within Operators will have to decide on case by case basis, what kind of decision to delegate to the network.

In case of specific Operational Procedure, a different level of delegation could be accorded to the network based on Time Dimension.

If the above first factor is not changing overtime, the second factor about side effects of Autonomous Decisions decrease in off-peak timeframe.

For example, during night time, Automatic fault recovery or new release/functionalities rollout could take place automatically, while during peak hours human supervision could be recommended.

7.3 Data classification and grading

The ability of data classification and grading refers to the sampling and query of structured and unstructured data stored on the platform under the big data platform, and identifying, matching, data type labelling, and classification and grading tags of data samples based on data characteristics, data identification strategies, and classification and grading strategies, so as to form a data classification and grading list, important and core data catalogues. The data classification and grading capability is exposed in the form of APIs to realize the reuse of basic capabilities and reduce the cost of duplicate construction. For example, when data is ingested into the lake, the Data Classification and Grading API can be called to identify and classify and mark the data entering the lake, different security protection solutions for different types of data can also be reinforced:

1) Corresponding scenario

This capability is applicable to data ingress to the data lake, data usage, data egress to the lake and data O&M:

2) Main features

Data processing, the data samples were sliced and sampled, and the samples were cleaned and formatted.

Data Identification, using key technologies such as regular matching, keyword matching, and algorithm matching, the characteristics of the sample were analysed to identify the data type of the sample.

Data classification and grading, according to the identified data feature types, combined with the data classification and grading strategy, the data is classified and graded.

Data list, summarize and display the results of data classification and grading, mark the storage location, data type, data level, and data classification of data assets, and form a list of data assets, important and core data catalogs.

Audit filing, manually audit and correct the classification and grading results of automatic identification data, and generate a complete classification and grading asset list based on the data provided by the business side, and perform filing processing. The ICP filing list is distributed to the business side to provide a basis for differentiated security protection on the business side.

Capacity, open data classification and grading capabilities through interfaces to provide support for other systems or security capabilities.

8 Conclusions

Evaluation of Autonomous Level within the entire operators' network or within a specific domain within the operators' network is essential to determine the next steps needed to evolve towards higher levels of autonomicity.

The development of network autonomicity not only depends on the maturity and empowerment of artificial intelligence technology, but also needs to be based on the further development of network operator's infrastructure (both hardware and software), including virtualization, SON, etc.

ENI adapts the need of every assisted system to provide the best support and evolution: a thorough evaluation of the system is essential to determine the best form of integration.

A careful analysis of the assisted system is fundamental to determine which functionalities are required to integrate ENI; thus enabling the level of autonomicity of the overall system.

Evaluation needs to be done on the overall system using multiple aspects, involving the identified dimensions and lifecycle phases. This analysis determines the system responsibilities when performing actions and taking decisions.

The development of the standard on categories for AI application to networks is in the ascendant. The present document makes further exploration based on the definition in ETSI GR ENI 007 [i.3], and puts forward a set of scientific, general, and standardized evaluation methods. That have guiding significance for the implementation of autonomous network. These studies have not been yet fully completed, there are many issues that need to be addressed together, such as:

- How to implement and configure the merger and evaluation dimensions in-line with actual conditions.
- How to quantify environmental change, this needs further study.
- The relationship among network KPIs. The network infrastructure capabilities and the network intelligence levels.

The use of the present document unites with communication industry partners:

1) to deepen the knowledge of the evaluation of network intelligence;
2) to promote the quantifiable degree of network intelligence;
3) to enable implementation of evaluation methods; and
4) to assist the guidance on network evolution and its implementation.

This promotes the development of network intelligence.

Annex A: Change history

Date	Version	Information about changes
2021-06-22	0.0.1	A new draft is uploaded - V 0.0.2 with status: Early draft - with comment: Baseline from ENI_18 ENI(21)018_007
2021-06-22	0.0.2	Draft contributed - V 0.0.2 contributed for Information in ENI(21)000028 as Early draft
2021-08-03	0.0.3	A new draft is uploaded - V 0.0.3 with status: Early draft - with comment: Call_188
2021-08-03	0.0.4	A new draft is uploaded - V 0.0.4 with status: Early draft - with comment: Call_184
2021-08-03	0,0.4	Draft contributed - V 0.0.4 contributed for Information in ENI(21)000_169 as Early draft
2021-08-31	0,0.4	Draft contributed - V 0.0.4 contributed for Information in ENI(21)019_025 as Early draft
2021-10-25	0,0.4	Draft contributed - V 0.0.4 contributed for Information in ENI(21)000_215 as Early draft
2021-11-17	0,0.4	Draft contributed - V 0.0.4 contributed for Information in ENI(21)000_245 as Early draft
2022-03-02	0,0.4	Draft contributed - V 0.0.4 contributed for Information in ENI(22)021_010 as Early draft
2022-03-10	0,0.4	Draft contributed - V 0.0.4 contributed for Information in ENI(22)000_072 as Early draft
2022-05-31	0,0.4	Draft contributed - V 0.0.4 contributed for Information in ENI(22)022_009 as Early draft
2022-06-07	0,0.4	Early draft proposal in contribution ENI(22)022_009 was Revised by ENI
2022-06-07	0,0.4	Draft contributed - V 0.0.4 contributed for Decision in ENI(22)022_009r1 as Early draft
2022-06-24	0.0.5	A new draft is uploaded - V 0.0.5 with status: Early draft - with comment: Approved in ENI_22
2022-06-24	0.0.5	Draft contributed - V 0.0.5 contributed for Information in ENI(22)000_139 as Early draft
2022-08-09	0.0.5	Draft contributed - V 0.0.5 contributed for Information in ENI(22)023_010 as Early draft
2022-09-07	0.0.5	Early draft proposal in contribution ENI(22)023_010 was Revised by ENI
2022-09-07	0.0.5	Draft contributed - V 0.0.5 contributed for Information in ENI(22)023_010r1 as Early draft
2022-09-08	0.0.6	A new draft is uploaded - V 0.0.6 with status: Early draft - with comment: Approved in ENI_23
2022-09-09	0.0.6	Draft contributed - V 0.0.6 contributed for Information in ENI(22)000_190 as Early draft
2022-12-22	0.0.6	Draft contributed - V 0.0.6 contributed for Information in ENI(23)000_001 as Early draft
2023-02-17	0.0.6	Draft contributed - V 0.0.6 contributed for Information in ENI(23)025_017 as Early draft
2023-05-05	0.0.6	Draft contributed - V 0.0.6 contributed for Information in ENI(23)026_021 as Early draft
2023-08-08	0.0.6	Draft contributed - V 0.0.6 contributed for Information in ENI(23)000_121 as Early draft
2023-09-07	0.0.7	A new draft is uploaded - V 0.0.7 with status: Early draft - with comment: At ENI_27
2023-09-07	0.0.7	Draft contributed - V 0.0.7 contributed for Information in ENI(23)000_140 as Early draft
2023-12-14	0.0.8	A new draft is uploaded - V 0.0.8 with status: Stable draft - with comment: in ENI_28
2023-12-15	0.0.8	Draft contributed - V 0.0.8 contributed for Information in ENI(24)000_001 as Stable draft
2024-03-06	0.0.9	Draft contributed - V 0.0.9 contributed for Information in ENI(24)000_001 as Stable draft, and ready for TB approval

History

Document history		
V1.1.1	March 2021	Publication
V1.2.1	June 2024	Publication