ETSI TS 128 535 V17.4.0 (2022-05)

5G;
LTE;
Management and orchestration;
Management services for communication service assurance;
Requirements
(3GPP TS 28.535 version 17.4.0 Release 17)

Reference
RTS/TSGS-0528535vh40

Keywords
5G,LTE

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

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.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

The present document describes closed control loop assurance solution enabling a service provider or an operator to continuously deliver the requested level of communication service quality to the customer and is part of a TS-family covering the 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Management and orchestration of networks, as identified below:

TS 28.535: Management Services for Communication Service Assurance; Requirements

TS 28.536: Management Services for Communication Service Assurance; Stage 2 and stage 3

The solution described builds upon the management services specifications as identified below:

TS 28.530: Management and orchestration; Concepts, use cases and requirements

TS 28.533: Management and orchestration; Architecture framework

TS 28.532: Management and orchestration; Generic management services

TS 28.540: Management and orchestration; 5G Network Resource Model (NRM); Stage 1

TS 28.541: Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3

TS 28.531: Management and orchestration; Provisioning

TS 28.545: Management and orchestration; Fault Supervision (FS)

TS 28.550: Management and orchestration; Performance assurance

TS 28.552: Management and orchestration; 5G performance measurements

TS 28.554: Management and orchestration; 5G End to end Key Performance Indicators (KPI)

1 Scope

The present document describes, concepts and background, and specifies use cases and requirements for closed control loop communication service assurance solution that adjusts and optimizes the services provided by NG-RAN and 5GC.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for the 5G system".

[3] 3GPP TS 28.550: "Management and orchestration; Performance assurance".

[4] 3GPP TS 28.531: "Management and orchestration; Provisioning".

[5] ETSI GS ZSM 002 (V1.1.1) (2019-08): "Zero-touch network and Service Management (ZSM); Reference Architecture".

[6] 3GPP TS 28.545: "Management and orchestration; Fault Supervision (FS)".

[7] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[8] 3GPP TS 28.554: "Management and orchestration; 5G end to end Key Performance Indicators (KPI)".

[9] 3GPP TS 28.532: "Management and orchestration; Generic management services".

[10] 3GPP TS 23.003: " Numbering, addressing and identification".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

communication services: subset of 3GPP defined services. Examples of 3GPP services (e.g. 5G LAN, URLLC) can be found in TS 22.261 [2].

service level specification: specification of the minimum acceptable standard of service.

SLA requirements: service and network requirements derived from SLAs.

NOTE: A provider can add additional requirements not directly derived from SLA's, associated to provider internal [business] goals.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

CN	Core Network
CS	Communication Service
CSA	Communication Service Assurance
CSC	Communication Service Customer
CSP	Communication Service Provider
eMBB	enhanced Mobile BroadBand
KPI	Key Performance Indicator
MDAS	Management Data Analytics Service
MnS	Management Service
NF	Network Function
NSI	NetworkSlice Instance
NSSI	NetworkSlice Subnet Instance
NSP	NetworkSlice Provider
NWDAF	Network Data Analytics Function
QoE	Quality of Experience
SD	Slice Differentiator
SLA	Service Level agreement
SLS	Service Level Specification
S-NSSAI	Single Network Slice Selection Assistance Information
SST	Slice/ServiceType

4 Concepts and background

4.1 Void

4.2 Management control loops

4.2.1 Overview

For communication service assurance one can identify two interactions of management control loops:

1) Between the CSC and the CSP: In this case, the CSC provides the requirements for an assured communication service to the CSP, the CSP provides the corresponding communication service, the CSP also provides feedback to the CSC. The CSP adjusts the resources used by a communication service or the CSC adjusts the SLS continuously to achieve the assured requirements.

2) Between the CSP and the NSP: the communication service provided by CSP requires the network capabilities. For example, the CSP requires a certain network latency. The NSP management system adjusts the network or CSP adjusts the latency requirement continuously to satisfy the latency requirement.

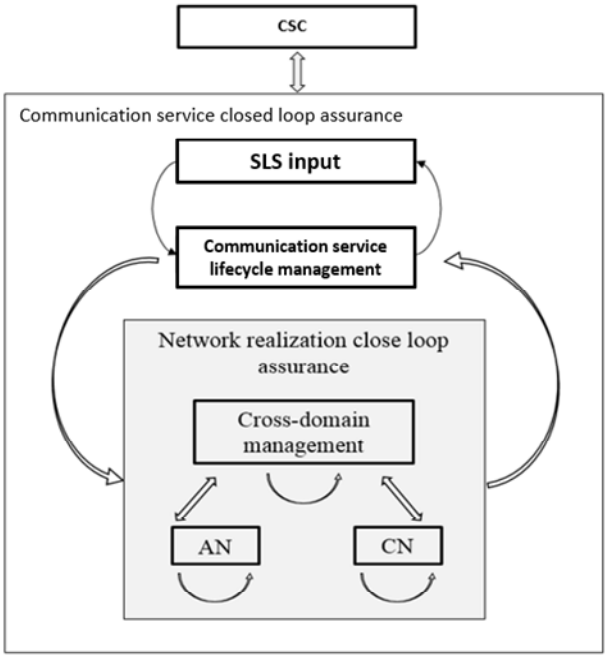

Figure 4.2.1.1: Communication service closed control loop assurance

Figure 4.2.1.1 gives a high level description of interaction process involved in the management closed control loop.

Generally, the management control loop for CSA consists of the steps Monitoring, Analysis, Decision and Execution. The adjustment of the resources used for the communication service is completed by the continuous iteration of the steps in a management control loop. As described in clause 4.1, the management closed control loop for the resources used for the communication service is deployed in the preparation phase and takes effect during the preparation phase and operation phase.

Figure 4.2.1.2 shows the overall process of communication service assurance using a management control loop.

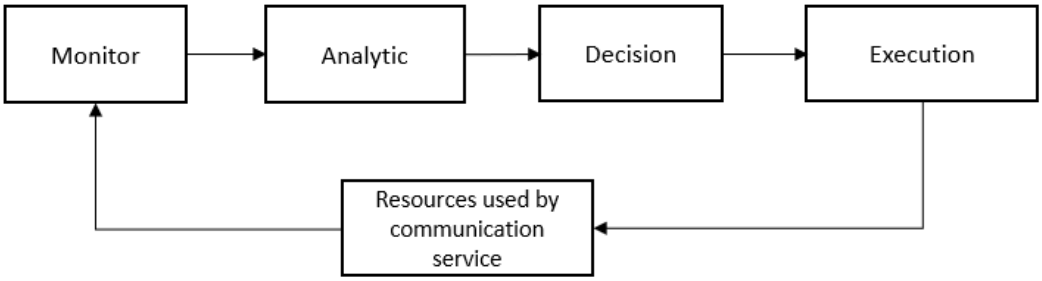

Figure 4.2.1.2: Management Control Loop

4.2.2 Control loops

A control loop is a building block for management of networks and services. The basic principle of any control loop is to adjust the value of a measured or observed variable (expressed as for example an attribute) to equal the value of a desired goal (expressed as for example an attribute). The producer of the measurements or observations, the control service, and the controlled entity are all required to create a control loop.

For the control loop to act on input in the context of the set goal, the control loop provided through following four steps that continuously consume and produce information from each other in a loop in the following sequence monitor, analyse, decide and execute.

A control loop can be an open control loop in which case a human operator or other management entity intervenes inside the loop A control loop can be closed and operates without human operator or other management entity

involvement inside the loop other than possibly the initial configuration of the measurement producer and configuration of control loop.

4.2.3 Open control loops

In an open control loop, the human operator intervenes in one or more of the process steps inside the loop, see Figure 4.2.3.1. The human operator is in control of the steps in the control loop, including decisions taken in the loop. The management system collects, analyses and presents the data to the operator, but the operator decides which action to take. In this case, the completion time for control loop is dependent on availability and reaction time of a human operator or other management entity.

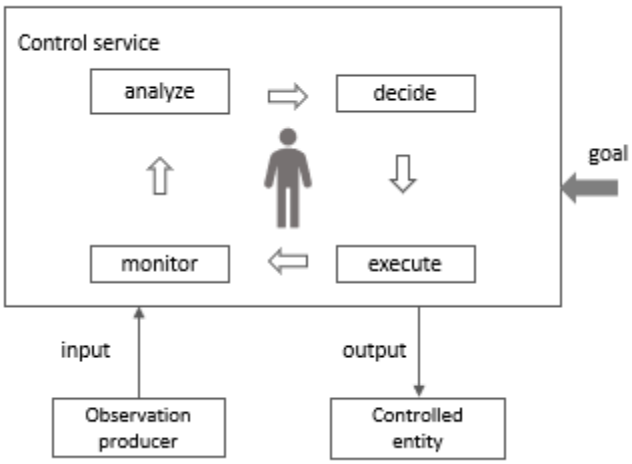

Figure 4.2.3.1: Open control loop entities

4.2.4 Closed control loops

4.2.4.1 Description

In a closed control loop, there is no direct involvement of a human operator or other management entity in the control loop, the control loop is fully automated. As shown in Figure 4.2.4.1 the human operator or management entity is not directly controlling the details inside the process steps but provides control outside the loop. For example, configuring goals for the control loop to make autonomous decisions within the boundaries of the set goal. Once the control loop is configured with the goal, the controlled entity is adjusted according to the set goals.

In a closed control loop the input to the control loop provided by human operator or other management entity may include the goal or policies. The output of the closed control loop may include closed control loop status to a human operator or other management entity.

Typically, the goal is set within certain parameter boundaries, the closed control loop can automatically adjust the output based on the input within the parameter boundaries. Once a control loop cannot automatically adjust, the human operator or other management entity needs to be informed. The human operator or other management entity may decide to change the management of closed control loop so that it becomes an open control loop, where decisions are made by the human operator or other management entity and not by the closed control loop.

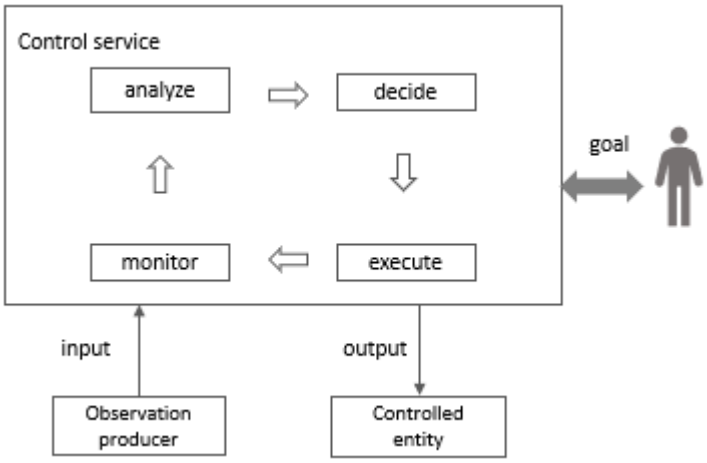

Figure 4.2.4.1.1: Closed control loop entities

4.2.4.2 Lifecycle phases

Communication service assurance is enabled by closed control loops which have their own lifecycle. The lifecycle phases for closed control loops are preparation, commissioning, operation and decommissioning.

- **Preparation phase:**

  Providing a closed control loop starts with preparation, which includes control loop design, collection of relevant goal information from an SLS and preparing the required network configuration for measurement collection. The result of the preparation phase is a closed control loop design.

- **Commissioning phase:**

  Once a closed control loop is prepared, one instance of the closed control loop design is instantiated by configuring the measurement collection and the goals in the network. During this phase the closed control loop may be deployed to allow the network to converge to a state where the communication service assurance is stable and within the boundaries of the SLS. The instantiation activity results in a closed control loop that is ready for operation.

- **Operation phase:**

  After the commissioning phase, the closed control loop is operational. The activation includes actions that make a closed control loop run to pursuit its goal(s). It may include subscription to relevant management services. In the operation phase the closed control loop is first activated. The monitor activity typically includes the real-time or periodic calculation of KPIs that are relevant to the closed control loop and comparison with the goal(s) assigned to the given closed control loop. This activity may result in further actions that involve the other activities in the operation phase, e.g. evaluate and update & upgrade, in order to change the closed control loop settings and improve its performance. The evaluate activity also includes the evaluation of results of Execution step of closed control loops by e.g. investigating differences between the current traffic data and the data taken before the execution. The criteria of this evaluation can be done by specific values such as SLS. The update & upgrade activity includes actions that change the settings of the closed control loop instance to change its behaviour and improve its performance to pursue the assigned goal(s). The update may include changes in the parameters of the management functions that constitute the closed control loop (e.g. changing data sources, KPIs being calculated, models, policies, etc.). The upgrade may include changes in the software version of the management functions. These activities can be executed dynamically while the closed control loop is regularly operating and executing actions, or they can be executed upon a request received from an authorized consumer. The deactivation activity includes actions that make the closed control loop stop to run.

- **Decommissioning phase:**

  When the closed control loop is no longer needed, after being deactivated the closed control loop is decommissioned and after that the lifecycle of the closed control loop is completed.

Figure 4.2.4.2.1 highlights the lifecycle phase sequence involved in the closed control loop assurance.

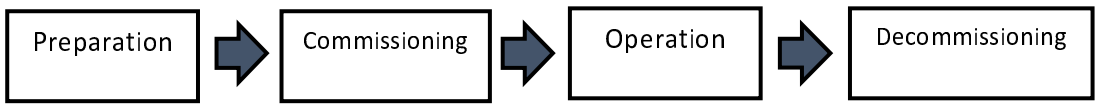

Figure 4.2.4.2.1: Lifecycle phases of a closed control loop

4.2.5 Closed control loop governance and monitoring

4.2.5.1 Overview

The closed control loop can be viewed as an entity to be managed, which means the implementation of the internal capabilities and internal interactions between the steps could not be externally visible. However, some management capabilities (e.g. closed control loop governance and closed control loop monitoring) will exposed by the MnS producer, implementing the closed control loops, to enable the MnS consumer to manage the closed control loops.

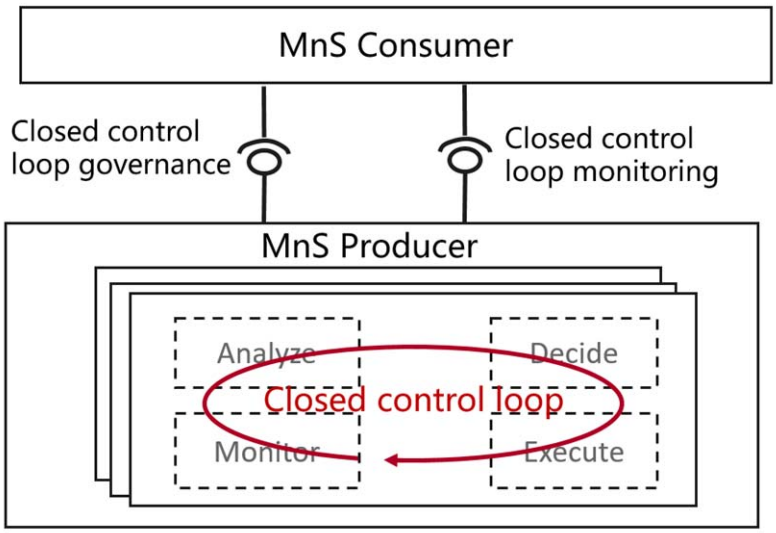

Figure 4.2.5.1 Closed control loop governance and monitoring

4.2.5.2 Closed control loop governance

Closed control loop governance describes a set of capabilities to allow MnS consumer to govern closed control loop, including:

- Lifecycle management of closed control loop, including create, modify,activate/deactivate,delete closed control loop.
- Configure goals for closed control loop.

4.2.5.3 Closed control loop monitoring

Closed control loop monitoring describes a set of capabilities to allow MnS consumer to monitoring the progress and result of closed control loop, including:

Monitor the goal fulfillment of the closed control loop.

Editor's Note: the content needs to be checked when R16 COSLA work is finished.

4.3 Communication service assurance service

Communication service assurance relies on a set of management services that together provide the CSP with the capability to assure the communication service as per agreement (for example an SLS) with a CSC (e.g. enterprise). The overall solution and information flows between management services and the closed control loop steps [5] are shown in Figure 4.3.1.

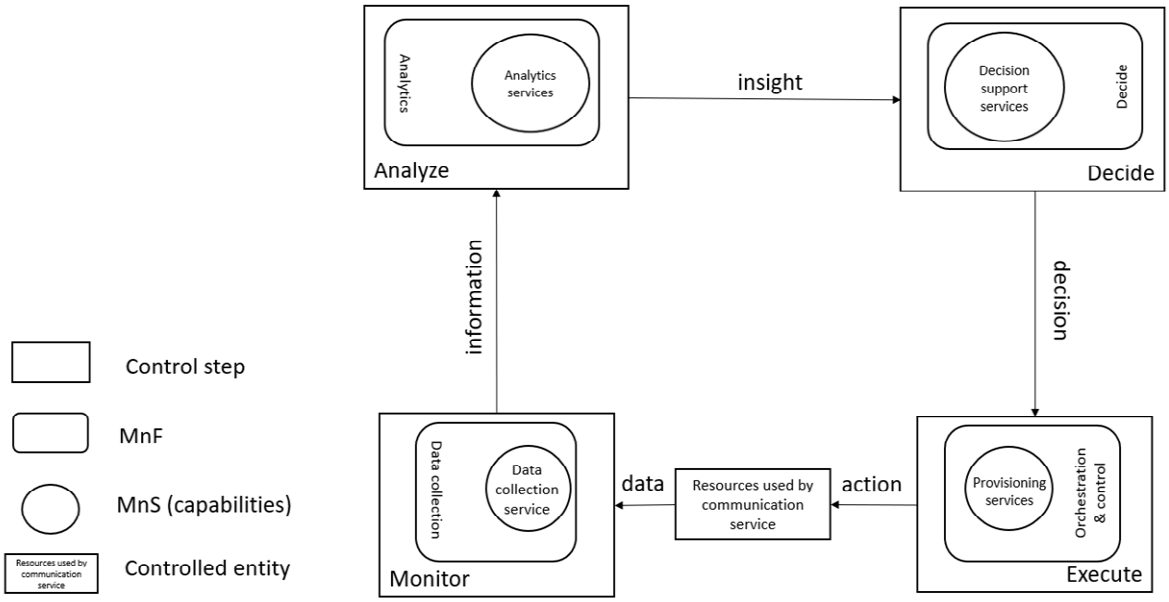

Figure 4.3.1: Overview of closed control loop information flows

In Figure 4.3.1 the controlled entity represents the resources used by a communication service and the assurance of this communication service is provided by the closed control loop between the different management services provided by the management system.

The input to the closed control loop is the data concerning the resources used by the communication service and corrresponding service KPIs which is monitored by the closed control loop and step "Monitor", analyzed by the closed control loop step "Analyze", a decision on potential solution by the closed control loop step "Decide" which may be a possible action for the closed control loop step "Execute", The role of the decision support services is to provide variable degrees of automated decision making and human oversight support. The following two examples demonstrate how a closed control loop can be used:

- when a service experience degradation is detected (for example due to resource shortage or faults in the network), the resources used by a communication service may be adjusted automatically to improve the service experience

- the data associated with the communication service is monitored by the management services for data collection, this management service provides information to an assurance root cause analysis management service (example of an analytics service) and based on that information the assurance root cause analysis takes place, followed by proposing activities, mitigation or suggestions to solve the problem. The proposed activities, for example mitigation or problem-solving suggestion(s) are executed through provisioning services to bring the behaviour of

the communication service within the requested boundaries of the metrics (SLS goals) that are controlled by the closed control loop.

The management services available for the closed control loop steps for "Monitor", "Analyze" and "Decide" are based on file transfer described in TS 28.550 [3], or data streaming described in TS 28.550 [3] and notifications described in TS 28.545 [6].

The information provided from the "Monitor" step to the "Analyze" step includes performance measurements (see TS 28.552 [7]), KPI's (see TS 28.554 [8]), performance threshold monitoring events and fault supervision events (see TS 28.532 [9]).

The insights provided from the "Analyze" step to the "Decide" step includes analytics outcomes that are not specified in the present document.

The decision support services provided from the "Decide" step to the "Execute" step are not specified in the present document.

5 Business level use cases and requirements

5.1 Use cases

5.1.1 Communication service assurance

The CSP needs to meet the CSC expectations on automation as well as internal goals on CAPEX and OPEX efficiency.

The CSP has access to capabilities, procedures and tools that can address both CAPEX and OPEX in the provisioning and management of communication services to their customers (CSC). The CSC expects the CSP to offer a variety of communication services including business critical communication services that allow the CSC (e.g. Enterprise) to run their applications in a predictable manner [2]. Hence automation of the onboarding of the CSC application, which will use communication services provided by the CSP, on a 5GS, is a requirement to meet the following needs:

- reduce the complexity for a CSC application to be on-boarded on a 5GS,
- improve the network performance over time, based on predicting communication service behaviour,
- assure the target goals for a CSC, and
- reduce the cost ownership through automation.

During the operation of the communication service the CSP provides assurance of service quality requirements and CSP meets the CSC expectations on automation as well as internal goals on CAPEX and OPEX efficiency.

REQ-CSA_NSA-FUN-01 The 3GPP management system shall have capabilities to receive communication service requirements from its authorized consumers.

REQ-CSA_NSA-FUN-02 The 3GPP management system shall have capabilities to monitor, and report to its authorized consumers the degree of fulfilment of committed communication service requirements of authorized consumers.

REQ-CSA_NSA-FUN-03 The 3GPP management system shall have capabilities to take actions to adjust the 5GS in order to meet the communication service requirements of authorized consumers.

REQ-CSA_NSA-FUN-04 The 3GPP management system shall have capabilities to act to fulfil the service quality requirements of authorized consumers.

5.1.2 Communication service assurance for shared resources

In this scenario, it is assumed that the SLA's for the two communication services will allow for them to share resources, for example RAN resources.

The management systems CS-Assurance service receives the request from Order Care and using a MDAS CS preparation assistance service, explores and evaluates communication service realisation and impact on other communication services, if any.

Once the Order Care has committed to an SLA with a CSC, the management system activates the communication service.

As the communication service operates, a management service for communication service assurance, CSA, continuously monitors the SLA fulfilment using MDAS, PM assurance services [3] including and core network NWDAF QoE analytics service, if available.

Based on goals for SLA fulfilment, or other KPIs, the CSA service may initiate an action when SLA goals are not met, be that over- or under fulfilment. The CSA service may use an MDAS to assist in selecting proper action and how to best execute the action.

The CSA service triggers the action by using provisioning service [4] towards RAN, transport and core network and monitors the effect of the change.

REQ-CSIA_CON-01: The 3GPP management system shall have the capability providing a management service for assisting in assessing (evaluating) a target SLA for a requested communication service.

REQ-CSIA_CON-02: The 3GPP management system shall have the capability providing a management service for assisting in asserting an agreed SLA for a requested communication service.

5.1.3 Use case for obtaining resource requirements for a communication service

Once a request for a communication service is received, the 3GPP management system needs to identify the network resources to be used by this service in order to do service assurance. For example, during the feasibility study, in order to assure the performance, the 3GPP management system should be able to determine the network availability for that service. This could be done by informing the MDAS provider about the network requirements and check if the requirements can be met with the available network resources.

MDAS provider may already have network requirement for a given service requirement, which is obtained by the historical analysis using offline or online monitoring of network resource usage of similar services. The 3GPP management system may check the feasibility of provisioning the communication services by using the existing network, and if feasible, provision the communication services using that network to go to the operational phase If the network requirement cannot be determined (e.g. not sufficient prior data), the 3GPP management system may assign certain amount of the initial network resources and limit the number of users admitted by configuring the appropriate CN functions. The resource usage information and the services using those resources in a given time period with their performance (e.g. delay) is monitored by the 3GPP management system for different number of UEs to learn the network resource requirement for different service requirements. This data could be used to determine network requirements for future service requests during the provisioning phase or to adjust network resources to reflect the changing service demands for the already admitted communication services.

It may be a continuous learning process in the run-time phase since service degradation could happen due to various reasons and network resources may need to be adjusted to address such situations.

REQ-CSA_RR-CON-01 The 3GPP management system shall be able to determine the network resource requirement for a given communication service requirement.

REQ-CSA_RR-CON-02 The 3GPP management system shall be able to allocate certain amount of network resources for a communication service and configure the 5GC functions to limit the number of users of a given communication service.

5.1.4 Use case for interaction with core network for service assurance

The goal is to enable the 3GPP management system to take early action to prevent service degradation.

The 3GPP management system configures the control plane functions (e.g. NWDAF) so as to report potential service degradation according to the SLS. Service load can be determined by considering both NF(s) load in 5GC and network

utilization in access network. If the service degradation occurs or is predicted when the network capacity is decreased, network capacity could be increased to solve the issue. Therefore, it is necessary for the 3GPP management system to configure the 5GC functions such that in the event of a potential service degradation or prediction of overloading, a notification is sent to the 3GPP management system. This can be done by configuring the overloading conditions (e.g. triggering parameters) in the 5GC functions for a selected service. The 3GPP management system could configure the 5GC functions to trigger when the service load is increased or predicted to be increased beyond a certain threshold level. The 3GPP management system could then increase the network capacity or use an MDAS to find a proper solution.

Similarly, when the network resources are underutilized the 3GPP management system could decrease the network capacity.

REQ-CSA_RR-CON-01 The 3GPP management system shall be able to configure the 5GC functions to enable reporting of a potential service load increase beyond a certain threshold so that the 3GPP management system can increase the network resource capacity in time without impacting the SLS.

REQ-CSA_RR-CON-02 The 3GPP management system shall be able to determine the service load thresholds that need to be used by the 5GC functions to report, so that a potential network resource overprovisioning situation can be ascertained.

REQ-CSA_RR-CON-03 The 3GPP management system shall be able to reduce network resource capacity when a network resource overprovisioning situation is detected, and the overprovisioned capacity is not needed.

6 Specification level use cases and requirements

6.1 Use cases

6.1.1 Communication service quality assurance and optimization

The goal of the use case is to enable communication service quality assurance and optimization for the set of services provided by the network to certain group (category) of UEs. For example, the set can include the communication services provided via certain NSI(s) or to IoT devices in certain area.

The group of NG-RAN and 5GC nodes (deployed and active), which are essential for the set of E2E services, provide provisioning and PM management services. It is also assumed that the providers of the related NSI / NSSI provisioning and PM management services are deployed and active.

The management system is consuming the afore mentioned management services either directly or through proxy nodes that re-expose the management services; the management system is aware of the performance requirements imposed on the set of communication services.

The management system is collecting the service experience information and monitoring the key performance indicators, KPIs, related to the targeted services. Analytics hosted by the MDAF may be utilized for processing of the network data to derive and analyse the KPIs. If the service quality assurance and optimization function detects performance degradation the 3GPP management system may continuously modify the configuration parameters in the corresponding NG-RAN and 5GC nodes and NSI(s)/NSSI(s), to satisfy the SLA requirement. In case that changes of communication service SLS are needed, those changes may result as input to the 3GPP management system.

If the network performance does not recover or improve, the management system may further adjust the network configuration, or roll back to the previous configuration. At all times the management system continues to collect the network data and to monitor the performance indicators.

6.1.2 NWDAF assisted communication service SLS Assurance

The goal of this use case is to assure the SLSs (Service Level Specifications) for a particular communication service is crucial for the 5G network management. The negotiated SLS for a particular communication service should be assured in an autonomous way.

3GPP management system can be leveraged to enable autonomous SLS assurance for a deployed communication service. 3GPP management system can collect QoE data, related to network slice and applications, from NWDAF. Since the data collected will relate to network slice and a single NSI may be serving multiple communication services, the corresponding QoE data for the target communication service needs to be ascertained. Once the QoE data for a communication service is known, the SLS breach can also be ascertained. If the SLS is breached, the root cause analysis is performed to find the cause for SLS breach. Depending on the location of cause (at RAN or at, 5GC), remedial actions will be initiated to mitigate the SLS breach and network optimization is done so that the negotiated SLS can be assured.

The QoE analytical data from NWDAF is per Application for an NSI. It is crucial to derive which communication service is associated to the QoE data from the data received from NWDAF in order to ascertain the SLS breach.

6.1.3 5G Core assisted SLS communication service Assurance

The goal of this use case is to describe 5G Core management to assure compliance to SLSs (Service Level Specifications) for a communication service in 3GPP management system.

3GPP management system receives the SLS requirements that required by CSP or NOP. 3GPP management system is capable to translate e2e SLS goal and set the 5GC goal(s) of SLS related to 5GC and activate a closed control loop for service assurance goal(s). To fulfill the SLS requirements, 3GPP management system is capable to configure the management resource and 5GC network functions (e.g. AMF, SMF, NWDAF) to monitor measurements and fault alarms that are relevant to the SLS. Since, for example, a network slice for eMBB can provide multiple communications services, one or multiple closed control loops for service assurance goals are set, and the network resource and performance measurements which are relevant to the SLS.

During the process of service assurance of 5GC, the 5GC domain MDAS provider can be used to provide analysis of 5GC related network resource, virtual resources and performance assurance related to SLS in 5GC. The 5GC domain analysis report may be provided to 3GPP management system as part of the analysis result(s) of 5GC SLS.

Together with the report from NWDAF, performance measurements and fault alarms related to 5GC NFs are also available for analysis of any potential service degradation.

6.1.4 Communication service SLS assurance control

The goal of this use case is to enable the MnS consumer to control the communication service SLS assurance closed control loop(s) (e.g. specify the SLS to be assured, enable/disable the SLS assurance, specify the assurance time for certain SLS) and obtain the SLS fulfilment information provided by MnS producer. It is assumed that the MnS producer maintains SLS assurance closed control loops for multiple SLSs. The detailed SLSs for network slice assurance are captured in ServiceProfile (e.g. latency, Throughput) associated to network slice and the detailed SLS for network slice subnet assurance are captured in SliceProfile (e.g. latency, Throughput) associated to network slice subnet.

When an MnS producer receives an SLS assurance closed control loops(s) creation request with SLS assurance requirements for certain managed Entity (i.e. network slice, network slice subnet) from an MnS consumer, the SLS assurance requirements may include information of which SLS should be assured (e.g. latency should be assured), the SLS assurance granularity (e.g. per UE, per Network Slice, per S-NSSAI), SLS assurance condition (e.g. SLS assurance duration time, SLS assurance fulfilment requirements (e.g. the ratio of the SLS assurance time during the whole service usage time)), the MnS producer create SLS closed control loop managed object instance contained by the specified managed Entity (i.e. NetworkSlice, NetworkSliceSubnet) and configures the received SLS assurance requirements in the created SLS closed control loop managed object instances. The MnS producer performs the network and/or service management to satisfy the SLS assurance requirements by adjusting the network (e.g. adjust the network topology, configure RRM policy) to satisfy the required SLS assurance requirements.

During the SLS assurance closed control loop operation phase, the MnS consumer may request MnS producer to enable/disable the corresponding SLS assurance or update the SLS assurance requirements if needed, then MnS producer update corresponding the SLS assurance closed control loop managed object instance to ensure the MnS producer perform the SLS assurance closed control loop based on the new request.

During the SLS assurance closed control loop operation phase, the MnS producer may report the SLS assurance closed control loop progress information and fulfilment information (e.g. SLS assurance requirements is satisfied or not) to the MnS consumer.

6.1.5 Network prediction assisted SLS communication service Assurance

The goal of this use case is to identify the management of network prediction assisted SLS communication service assurance. The SLS related to a particular communication service can be assured by considering the predicted network resource usage and performance (e.g. latency, throughtput) for the managed entity (e.g. network slice, network slice subnet) associated with the SLS closed control loop managed object instance within a certain time frame.

The 3GPP management system will have the most comprehensive network operating data, such as network resource utilization, network performance parameters in different periods, which would include different collection granularities (e.g. per UE, per S-NSSAI) and have corresponding performance parameters respectively in NG-RAN or 5GC. By introducing MDAS and NWDAF into both the management system and core network, it is possible that the network operating data can be the input of the closeloop to fulfil SLS requirements from CSP or NOP. The MDAS could predict the network resource usage and performance for the whole network as well as different domain, for example, the MDAS could predict the resource utilization and throughtput for the NSSI in the NG-RAN within a certain time period.

In a certain period of time, the current network condition is good enough to satisfy the SLS requirements. By introducing the prediction results from the analysis of MDAF and NWDAF, the historical data shows that the network will experience a traffic burst in certain area and certain time which can cause network resource shortage and performance degradation. This predictional results can directly trigger the MDAF to analyse the root cause for performance degradation and analyse the solution which is used for making the network desicion such as reconfiguration and resource reallocation before the predicted traffic burst time. And the resource reallocation could be conducted between the multiple NSIs or NSSIs, for example, there are different network slices in the network for SLS communication service assurance, the resources between network slices could be adjusted dynamically based on the MDAF analysis results. Similarly, in office area, the network will not active during holiday but will have network surges on working day, the network prediction can also trigger resource release and network function reconfiguration. This can not only save network operating costs on holiday but also achieve the goal of network service assurance on working day.

6.1.6 Limiting the actions of an assurance closed loop

The goal of this use case is to provide the consumer of an assurance closed loop the ability to limit actions the assurance closed loop can execute. This renders the assurance closed loop taking action (configuration of MoI attributes) that are within the limits of the scope as defined by the consumer.

Assurance closed loops have a defined assurance goal related to a communication service SLS may execute various actions in the deployed operator network. There may be cases in which two or more assurance closed loops can execute the same or related set of actions on a managed entity. For example, assurance closed loops ACL1 and ACL2 for coverage optimization running in neighbouring RAN domains may take independent decision on the radio signal strength and azimuth to optimize the coverage. These assurance closed loops therefore may have the capability to cause a conflict with both simultaneously changing the azimuth to address a coverage-hole thereby causing an unnecessary coverage-overlap instead.

An authorized coordinating entity (authorized common consumer of the two ACL), should be able to configure the closed loops in a way that such occurrences are minimized. To coordinate the execution of multiple such assurance closed loops in the system the common authorized consumer of the assurance closed loop limits the set of actions of the assurance closed loops to avoid possible conflicts between the two or more assurance closed loops. In the example above: The authorized consumer of an assurance closed loops may limit the coverage optimization configurations signal strength and azimuth configurations to be done only by ACL1.

The 3GPP management system shall therefore provide the ability to limit action capabilities (possible configurations of an MoI attributes) that an assurance closed loop can take, this can be for example via operational policy configurations.

The MnS consumer obtains the allowed action capabilities (configurations that assurance closed loops could execute on an managed entitiy) from the MnS producer. The MnS consumer may then internally compare the action capabilities allowed that can be taken by a set of assurance closed loops to determine if possible conflicts exist. If conflicts are found, and the MnS consumer determines a possible resolution by limiting the action capabilities of a set of assurance closed loops, then it requests the MnS producer to limit the set of action capabilities, for example: by configuring new operational policies.

6.1.7 Trigger based Assurance Closed Control Loop (ACCL) state change

The goal of this use case is to provide the consumer of an assurance closed loop the ability to set conditions (example threshold crossings) in the 3GPP management system that when met, trigger changes in ACCL state (enable or diable an ACCL). This implies that an ACCL may be activated or deactivated if the set condition in the 3GPP network is met (example: the threshold is crossed).

Assurance closed loops may be required to run at different times and network conditions in the 3GPP network. For example, an ACCL related to handover optimization may only execute when the handover failure crosses a certain threshold. Similarly, an ACCL managing energy efficiency may be disabled when the network is overloaded beyond a certain threshold. These conditions (network overload, handover failure threshold crossing) can therefore be associated with a change in state (enable/disable) of an ACCL to further support autonomy of the 3GPP management domain.

An authorized entity (authorized consumer of the ACCL), for example, another closed loop or operator, should be able to configure the condition and its association with an ACCL state transition (enable/disable) in the 3GPP management domain.

The 3GPP management system shall therefore provide the ability to configure conditions and associate them with the state transition of an ACCL. The 3GPP management system then configure appropriate listeners to monitor the configured threshold crossing and once triggered execute a state transition (enable/disable) of the associated ACCL.

The MnS consumer obtains the possible conditions as well as the possible ACCL state transitions they can be associated with. The MnS consumer may then configure condition in the 3GPP network. When the threshold crossing notification is received the MnS producer it executes the associated state transition (enable/disable) of the ACCL.

6.2 Requirements

REQ-CSA-CON-01 The 3GPP management system shall have the capability to take actions for a set of communication services serving certain group of UEs based on the target SLS.

REQ-CSA-CON-02 The 3GPP management system shall have the capability to collect service experience information.

REQ-CSA-CON-03 The 3GPP management system shall have the capability to analyse the performance information related to the set of communication services serving certain group of UEs.

REQ-CSA-CON-04 The 3GPP management system shall have the capability to modify the configuration parameters related to the set of communication services serving certain group of UEs.

REQ-CSA-CON-05 The 3GPP management system shall have the capability to collect NSI related data from one or more 5GC NF(s).

NOTE 1: An example for NSI related data may be QoE data.

REQ-CSA-CON-06 The 3GPP management system shall have the capability to derive which communication service is associated to the QoE data from the collected NSI related QoE data.

NOTE 1a: A communication service in the 3GPP management system is identified by an S-NSSAI (the Slice/ServiceType, SST in the S-NSSAI identifies a communication service which can be detailed using the SliceDifferentiattor, SD), see TS 23.003 [10].

REQ-CSA-CON-07 The 3GPP management system shall have the capability to ascertain SLS breach.

REQ-CSA-CON-08 The 3GPP management system shall have the capability to perform the root cause analysis (e.g., identifying the underlying reason) for an SLS breach.

REQ-CSA-CON-09 The 3GPP management system shall have the capability to take corrective actions to ensure the target goal.

REQ-CSA-CON-10 The 3GPP management system shall have the capability to translate network slice requirements to cross domain network slicesubnet SLS goal and single domain network slicesubnet SLS goal.

REQ-CSA-CON-11 The 3GPP management system shall have the capability to collect single domain SLS analysis as input to cross domain SLS analysis.

REQ-CSA-CON-12 The 3GPP management system shall have the capability to allow its authorized consumer to control the SLS assurance (e.g. specify the SLS to be assured, enable/disable, specify the assurance time and update the SLS assurance requirements).

REQ-CSA-CON-13 The 3GPP management system shall have the capability to allow its authorized consumer to obtain the SLS assurance fulfilment status information.

NOTE 2: The management system refers to the producer of management service for SLS assurance.

REQ-CSA-CON-14 The 3GPP management system shall have the capability to do network prediction (e.g. network resource usage and network performance) by analysing the network operation information in special scenarios.

REQ-CSA-CON-15 The 3GPP management system shall have the capability to take actions such asnetwork configuration and perform network resource reallocation according to the network prediction results.

REQ-CSA-CON-16 The 3GPP management system shall have the capability to allow its authorized consumer to limit the set of action capabilities executable by an assurance closed loop.

REQ-CSA-CON-17 The 3GPP management system shall allow an authorized consumer to set a condition to enable/disable an ACCL.

REQ-LCM-CON-01 The 3GPP management system shall have the capability of lifecycle management of a closed control loop.

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2020-07	SA#88e					Upgrade to change control version	16.0.0
2020-09	SA#89e	SP-200750	0008	-	F	Add abbreviations to clause 3.3	16.1.0
2020-09	SA#89e	SP-200750	0009	-	F	Correction of requirements text in clause 5.1.1	16.1.0
2020-09	SA#89e	SP-200750	0010	-	F	Remove Editors Notes from clause 5.1.2	16.1.0
2020-12	SA#90e	SP-201056	0011	-	F	Update and make closed control loop term consistent	16.2.0
2020-12	SA#90e	SP-201050	0012	-	F	Corrections to clause 4.1 and 4.2.1	16.2.0
2020-12	SA#90e	SP-201056	0014	-	F	Update figure and description of Communication service assurance service	16.2.0
2020-12	SA#90e	SP-201075	0001	1	B	Add use case of network resource usage and performance prediction assisted SLS communication service Assurance	17.0.0
2020-12	SA#90e	SP-201075	0019	1	B	Add use case for limiting actions of a AL	17.0.0
2020-12	SA#90e	SP-201075	0021	1	B	Add use case for triggering assurance loop state change	17.0.0
2020-12	SA#90e	SP-201075	0022	-	B	Add concept of closed control loop governing and monitoring	17.0.0
2021-03	SA#91e	SP-210151	0037	1	A	Update use cases and requirements to replace Communication Service	17.1.0
2021-06	SA#92e	SP-210402	0045	-	A	Clarify intelligence in clause 4	17.2.0
2021-06	SA#92e	SP-210405	0046	-	B	Re-introduce use cases	17.2.0
2021-06	SA#92e	SP-210402	0047	-	A	Update description of communication service lifecycle	17.2.0
2021-06	SA#92e	SP-210402	0049	-	A	Update management control loops with lifecycle description	17.2.0
2021-06	SA#92e					Fixing error implementation of CR0046	17.2.1
2021-09	SA#93e	SP-210868	0053	-	F	Update the network prediction assisted SLS communication service assurance use case	17.3.0
2021-12	SA#94e	SP-211470	0059	1	A	Clarify business requirements	17.4.0
2021-12	SA#94e	SP-211470	0062	-	A	Clarify business requirement and correct punctuation	17.4.0
2021-12	SA#94e	SP-211470	0063	1	A	Clarify communication service in requirement CSA-CON-06	17.4.0

History

Document history		
V17.4.0	May 2022	Publication