ETSI TS 128 535 V16.0.0 (2020-07)

TECHNICAL SPECIFICATION

5G;
LTE;
Management and orchestration;
Management services for communication service assurance;
Requirements
(3GPP TS 28.535 version 16.0.0 Release 16)

Reference

DTS/TSGS-0528535vg00

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 - NAF 742 C

Association à but non lucratif enregistrée à la

Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

ETSI

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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 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 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".

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 may 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].

CS	Communication Service
CSA	Communication Service Assurance
CSC	Communication Service Customer

CSP	Communication Service Provider
SLA	Service Level agreement
SLS	Service Level Specification

4 Concepts and background

4.1 Lifecycle of a communication service

Communication service assurance applies to different phases in the life of communication services these lifecycle phases are; preparation, commissioning, operation and decommissioning.

- **Preparation phase:**

Providing a communication service starts with preparation, which includes communication service design, pre-planning, feasibility check, i.e., checking the attainable communication service quality from both resource and service aspects, negotiation of the communication service attributes, preparing communication service and network requirements derived from SLA.

- **Commissioning phase:**

Once a communication service is prepared, it can be established by converting the communication service requirement to network requirements (interaction and use of NF resources including RAN, CN) be deployed on the network resources and ready to be used by the communication service consumers (subscribers, UEs). Before allowing the maximum agreed number of communication service consumers to use this communication service a communication service assurance (CSA) control loop is 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 assurance control loop learns the communication service behaviour during an initial deployment or trail phase.

- **Operation phase:**

After the commissioning phase, the communication service is activated for use of all communication service consumers (subscribers, UEs) that are allowed to use the communication service. The initial deployment or trail phase for the training of the communication service assurance algorithms has entered the operation phase. A communication service that is activated allows run-time operations e.g., quality of experience assurance, quality of service assurance. The optimization of the utilization by communication services may continue during the operation phase of the communication service.

- **Decommissioning phase:**

When the communication service is no longer needed, after being de-activated, the lifecycle of the communication service ends with termination.
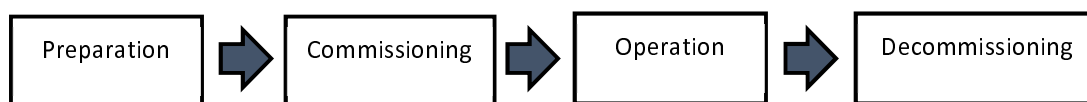

Figure 4.1.1: Lifecycle of a communication service

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.
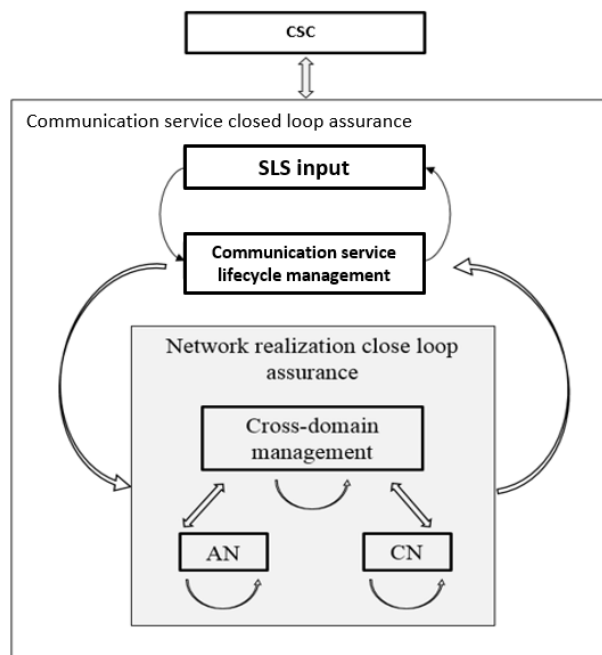
Figure 4.2.1.1: Communication service closed loop assurance

Generally, the management control loop for Communication Service Assurance, 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.

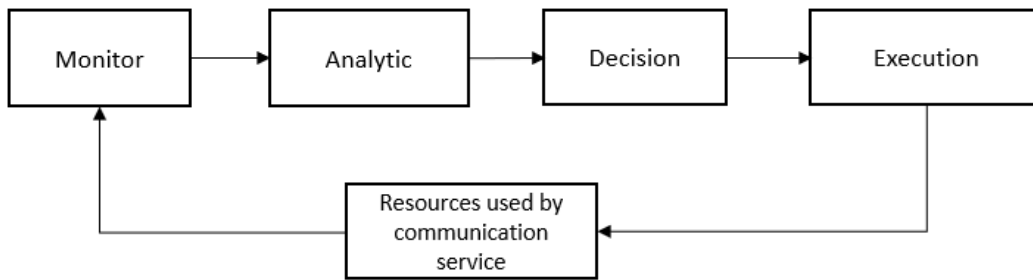For the control loop to act on input in the context of the set goal, the control loop provided through following four steps that continuously consume and produce information from each other in a loop in the following sequence monitor, analyse, decide and execute.

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.
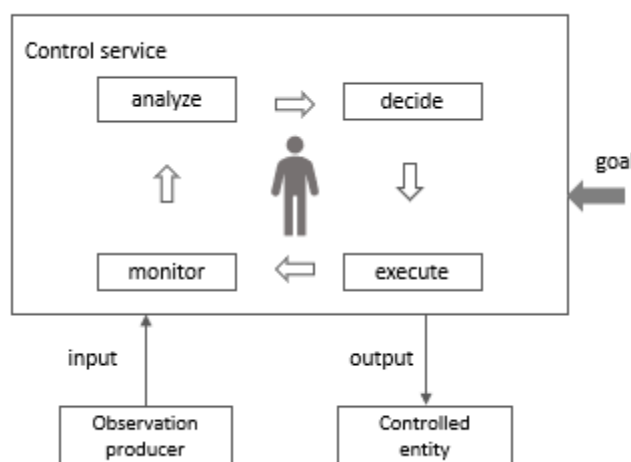

Figure 4.2.3.1: Open control loop entities

4.2.4 Closed control loops

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 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 control loop may include closed loop status to a human operator or other management entity.

Typically, the goal is set within certain parameter boundaries, the 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 becomes to an open control loop, where decisions are made by the human operator or other management entity and not by the closed control loop.
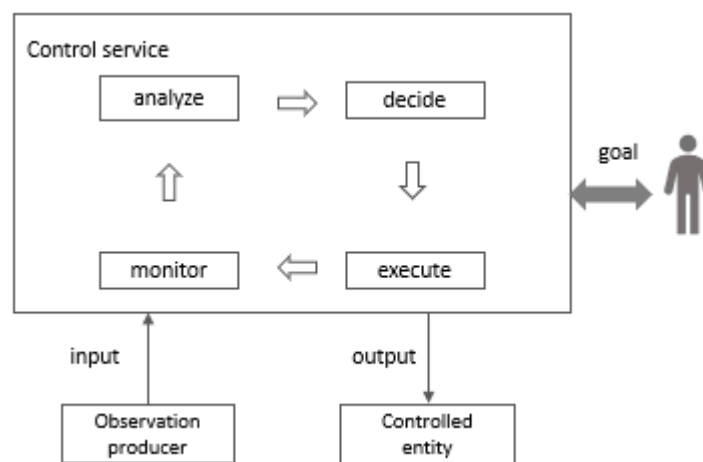
Figure 4.2.4.1: Closed control loop entities

5 Business level use cases and requirements

5.1 Use cases

5.1.1 Communication service assurance

The CSP wants 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 on-boarding 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;

- reduce the cost ownership through automation.

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

REQ-CSA_CSA-FUN-01 The CSP shall be able to provide a statement of CS service requirements to a 5GS and receive capability information about these from the 5GS.REQ-CSA_CSA-FUN-03 The 5GS shall have the capabilities to monitor, and report to CSP the fulfilment of committed CS requirements and actions taken to adjust for deviations.

REQ-CSA_CSA-FUN-03 The 5GS shall have the capabilities to monitor and report to CSP actions taken to adjust deviations on committed CS requirements.

REQ-CSA_CSA-FUN-04 The 5GS shall have the capability to provide in-operation assurance of service quality expectation.

REQ-CSA_CSA-FUN-04 The 5GS shall have the capability to ensure the service quality requirements during the service operations.

Editor's Note: The specification level requirements on OAM are for FFS.

5.1.2   Communication service assurance for shared resources

Editor's Note: The need for a use case of communication service assurance for dedicated resources is FFS.

A CSP network where at least one eMBB service is operating, providing services to end-users. A CSC requests from the CSP Order Care a new eMBB service (or any other communication service) for business-critical application(s), submitting an initial proposed communication service SLA. The management system assists CSP Order Care with analysis of the proposed SLA and, when SLA is committed, works together with NF's to ensure communication service SLA goals and optimal use of resources for previous as well as the new communication service(s).

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 and TN 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 KPI's, 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.

Editor's Note: Whether provisioning services shall be including also management of SON functions when such are available, is FFS.

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

REQ-CSIA_CON-03: The 3GPP management system shall have the capability to process 5GS data and provide analytics services to its consumers.

Editor's Note: information exchange with application such QoE reporting, is FFS

5.1.3 Use case for obtaining resource requirements for a communication service

Once a request for a communication service is received, in the communication service provisioning phase, the 3GPP management system needs to identify the resources required for 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 resource availability for that service. This could be done by requesting the MDAS provider about the resource requirements and checking the available resources.

MDAS provider may already have resource requirement for a given service requirement, obtained by the historical analysis using offline or online monitoring of resource usage of similar services. In that case, the 3GPP management system can determine the feasibility and if feasible provision the communication services using those resources to go to the operational phase.

If the resource requirement cannot be determined (e.g. not sufficient prior data), the 3GPP management system may assign certain amount of initial 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 resource requirement for different service requirements. This data could be used to determine resource requirements for future service requests during the provisioning phase or to adjust 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 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 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 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 resource utilization in access network. If the service degradation occurs or predicted when the resources are scaled down, resources could be scaled up to solve the issue. Therefore, it is necessary for the 3GPP management system to configure the 5GC functions such that in the event that a potential service degradation or overloading is predicted, that is sent to the 3GPP management system. This can be done by properly configuring the overloading conditions (e.g. triggering parameters) in the 5GC functions of 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 do resource scaling or use MDAS to find a proper solution.

Similarly, when the resources are underutilized the 3GPP management system could do scaling down or deactivation of resources.

REQ-CSA_RR-CON-01 The 3GPP management system shall be able to configure the 5GC functions to make them report of a potential service load increase beyond a certain threshold so that the 3GPP management system can do scaling up of resources in time without impacting the SLA.

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 resource overprovisioning situation can be ascertained.

REQ-CSA_RR-CON-03 The 3GPP management system shall be able to perform scaling down of resources when a resource overprovisioning is detected, and the overprovisioning is not needed.

6　Specification level use cases and requirements

6.1　Use cases

6.1.1　Communication service quality assurance and optimization of communication services

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.

It is assumed that the relevant NFs are deployed and active in NG-RAN and 5GC. The group of NG-RAN and 5GC nodes, 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 above 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 SLA/SLS are made, those changes may result as input to the 3GPP management system.

If the network performance does not recover or improve, the management system may adjust the modifications, for example roll back to previous configuration. In any case it continues collecting the network data and monitoring of 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 particular 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 control loop for particular 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 particular 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 control loop 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 resource 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 control the communication service SLS assurance closed 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 fulfil information provided by MnS producer. It is assumed that the MnS producer maintains SLS assurance closed 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 MnS producer received SLS assurance closed loops(s) creation request with SLS assurance requirements for certain managed Entity (i.e. network slice, network slice subnet) from 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 loop managed object instance contained by the specified managed Entity (i.e. NetworkSlice, NetworkSliceSubnet) and configure the received SLS assurance requirements in the created SLS closed loop managed object instances. The MnS producer perform 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 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 loop managed object instance to ensure the MnS producer perform the SLS assurance closed loop based on the new request.

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

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.

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 against the root cause identified.

REQ-CSA-CON-10 The 3GPP management system shall have the capability to translate communicate service requirements to cross domain SLS goal and single domain 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 progress information and fulfil information.

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

Annex A (informative):
Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-09	SA5#126					Skeleton	0.0.0
2019-10	SA5#127	S5-196611				pCR 28.535 Add scope	0.1.0
2019-10	SA5#127	S5-196612				pCR 28.535 Add introduction	0.1.0
2019-10	SA5#127	S5-196483				pCR 28.535 Introduce table of content	0.1.0
2019-10	SA5#127	S5-196615				pCR 28.535 Add lifecycle of a communication service	0.1.0
2019-10	SA5#127	S5-196478				pCR 28.535 Add management control loops	0.1.0
2019-11	SA5#128	S5-197582				pCR 28.535 Communication service assurance scenario	0.2.0
2019-11	SA5#128	S5-197585				pCR 28.535 use case for obtaining resource requirements for a communication service	0.2.0
2019-11	SA5#128	S5-197787				pCR 28.535 Service quality assurance and optimization	0.2.0
2019-11	SA5#128	S5-197833				pCR 28.535 Interaction with core network for service assurance	0.2.0
2019-12	SA#86	SP-191186				Presented for information	1.0.0
2020-03	SA5#129	S5-201488				pCR 28.535 Add text for clause 4.2 Management control loops	1.1.0
2020-03	SA5#129	S5-201437				pCR 28.535 Add UC on NWDAF assisted SLS Assurance	1.1.0
2020-04	SA5#130e	S5-202382				Update clause 6.2 requirements	1.2.0
2020-04	SA5#130e	S5-202395				pCR TS 28.535 update of use case in subclause 6.1.1	1.2.0
2020-04	SA5#130e	S5-202383				pCR clarify service load in use case for interaction with core network for service assurance	1.2.0
2020-04	SA5#130e	S5-202340				pCR TS 28.535 Move Annex A Management control loop in different layers to TS 28.536	1.2.0
2020-06	SA5#131e	S5-203289				pCR TS 28.535 Remove CSI definition	1.3.0
2020-06	SA5#131e	S5-203219				pCR 28.535 Update Clause 4.2 Management control loops	1.3.0
2020-06	SA5#131e	S5-203430				pCR TS 28.535 Generalise requirements	1.3.0
2020-06	SA5#131e	S5-203431				pCR TS 28.535 Add use case for 5GC service assurance	1.3.0
2020-06	SA5#131e	S5-203435				pCR 28.535 Add use case of SLS assurance control	1.3.0
2020-06	SA5#131e	S5-203429				pCR 28.535 Update Clause 4.2 Management control loops	1.3.0
2020-06	SA#88-e	SP-200478				EditHelp/MCC review Presented for approval	2.0.0
2020-07	SA#88e					Upgrade to change control version	16.0.0

History

Document history		
V16.0.0	July 2020	Publication