ETSI GS ZSM 009-2 V1.1.1 (2022-06)

Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 2: Solutions for automation of E2E service and network management use cases

Disclaimer

The present document has been produced and approved by the Zero-touch network and Service Management (ZSM) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference
DGS/ZSM-009-2_CLA_sol

Keywords
automation, network management, use case

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

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

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 of ETSI GS ZSM 009-1 [3].

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.

1 Scope

The present document presents solutions to scenarios related to closed loops using the ZSM specified service capabilities. New service capabilities are specified where the need arises based on the scenarios solution requirements.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

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 necessary for the application of the present document.

[1] ETSI GS ZSM 007 (V1.1.1): "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".

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

[3] ETSI GS ZSM 009-1 (V1.1.1): "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 1: Enablers".

2.2 Informative references

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

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

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

[i.1] ETSI GS ZSM 001: "Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios".

3 Definition of terms, symbols, abbreviations and conventions

3.1 Terms

For the purposes of the present document, the terms given in ETSI GS ZSM 007 [1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS ZSM 007 [1] apply.

3.4 Conventions

Clause 5 of the present document specifies expected solutions to typical automation scenarios using ZSM specified capabilities. For each step a corresponding capability is referenced from ETSI ISG ZSM specifications. The scenarios are briefly described in the description part of each clause. The solutions are provided in a table similar to table 3.4-1 that provides a pre-condition, a target, examples of expected steps for the solution and references to ZSM capabilities that may be used to achieve that step.

The table format with explanation of each of the parts is provided in table 3.4-1.

Table 3.4-1: Table used for solutions to scenarios

Precondition: The conditions/assumptions of the scenario **Target:** The target to be achieved by the solution of the scenario
Solution alternative
Step 1: Step 1 of the solution. For this the capability X specified in clause Y.x is used. Step 2: (Steps may refer to a picture).

4 Introduction

The present document specifies solutions to automation scenarios. The scenarios and corresponding solutions are presented together in clause 5. Scenarios are grouped in four categories, namely:

1) Generic management scenario solutions addressed in clause 5.1.

2) Scenario solutions relating to analytics in clause 5.2.

3) Scenario solutions relating to closed loops' coordination in clause 5.3.

4) Scenarios to solutions relating to closed loops' governance in clause 5.4.

Clause 6 specifies additional capabilities which extend existing ZSM services supporting the solutions.

5 Solutions supporting selected scenarios

5.1 Generic management using closed loops

5.1.1 Inclusion of a new physical resource into a management domain

5.1.1.1 Description

When a new physical resource is added to a management domain all other relevant authorized management domains should become aware of the management domain's ability to provide services based on the inclusion of the new resource. For example: when a new radio is added to the RAN domain of an operator the E2E management domain of the operator detects that it has the ability to provide services in an updated coverage area. This scenario is related to the scenario in clause 6.2.3.6 of ETSI GS ZSM 001 [i.1].

5.1.1.2 Proposed Solution

Table 5.1.1.2-1: Steps in solution

Pre-condition: The operator network exists and is operational, and a new physical resource is added into a management domain, say MD1. **Target:** To notify relevant management domains of the update in services based on the availability of the new resource in a management domain.	
Solution alternative	
Step 1:	MD1 updates its inventory and service capabilities based on the inclusion of a new resource. This is an internal capability of the management domain.
Step 2:	Other management domains authorized to view the changes in service/resource capabilities of MD1 can view these changes at their respective abstraction level. The solution to do this is specified in clause 5.1.4.
Step 3:	The management domains can use the updated capabilities of MD1.

5.1.2 Provisioning services in back up domains

5.1.2.1 Description

A new E2E Service may be provisioned in one or more management domain(s) as determined by the E2E management domain. However, if during the lifetime of the service one of the management domains, (say MD1) becomes unable to host its part of the E2E service (for example: MD1 encounters a failure) then the E2E service may need to provision an equivalent part of the E2E service that was hosted by MD1 to another management domain (say MD2) to ensure the continued operation of the E2E service. This solution is related to scenarios in clause 6.2.3 of ETSI GS ZSM 001 [i.1].

5.1.2.2 Proposed Solution

Table 5.1.2.2-1: Steps in solution

Precondition: The E2E management domain has deployed an E2E service across management domains MD1, MD2, MD3. The E2E management domain detects that MD1 is unable to support its part of the E2E service. **Target:** The E2E management domain can deploy the E2E Service in a new set of management domains, say, MD-A, MD-B, MD-C. NOTE 1: The relationship between MD-A-C , MD1-3 is intentionally not specified. That is to say that, for example MD-B could be identical to MD-2.	
Solution alternative:	
Step 1:	E2E management domain evaluates E2E service requirements and deploys the E2E service across multiple Management domains, say MD1, MD2, MD3. The manage service lifecycle capability as in clause 6.5.5.2.1 of ETSI GS ZSM 002 [2] is used for this purpose.
Step 2:	The E2E management domain detects that the domain MD1 is no longer able to support its part of the requested service and re-evaluates that the desirable new solution is MD-A, MD-B and MD-C. If the E2E MD is unable to find a new set of MDs to support the E2E Service, it issues an alarm to the ZSM consumer. See clause 5.1.5 on the solution for how this is done.
Step 3:	The E2E MD deactivates the request from MD2, MD3 and deploys it on MD-A, MD-B, MD-C. The manage service lifecycle capability as in clause 6.5.5.2.1 of ETSI GS ZSM 002 [2] is used for this purpose.
NOTE 2:	The use case focuses on deployment, other procedures required to support the deployment are not addressed.

5.1.3 Automated service healing capability

5.1.3.1 Description

An E2E service is deployed across a set of management domains. During the lifetime of the E2E service a failure occurs in one management domain which then intends to automatically heal the service without involving the other management domains of the E2E management domain. If self-healing is not possible in the management domain local scope, the management domain escalates the problem towards the E2E management domain, which then evaluates the problem, initiates service self-healing actions in the E2E scope, and drives the management domains to perform the required reconfigurations in the underlying management domains. The solution is related to clauses 6.2.3.3 and 6.5.3 of ETSI GS ZSM 001 [i.1].

5.1.3.2 Proposed Solution

Table 5.1.3.2-1: Steps in solution

Precondition: The E2E management domain has deployed an E2E service across a set of management domains, e.g. MD1, MD2, MD3. **Target:** The service is automatically self-healed by a management domain or by the E2E management domain when an infrastructure failure occurs in a management domain.	
Solution alternative:	
Step 1:	Domain analytics management functions subscribe to fault events service running at management domains to detect fault events regarding the deployed E2E service originating from the infrastructure resources of the respective management domain, e.g. MD1, MD2, MD3. For this the provide notification capability of the fault events service as specified in table 6.5.2.2.1-2 of ETSI GS ZSM 002 [2] is used.
Step 2:	The E2E domain analytics management functions subscribe to anomaly detection service running at management domains and/or E2E anomaly detection service. For this the provide analysis results capability of the anomaly detection service as specified in table 6.5.3.2.1-2 of ETSI GS ZSM 002 [2] is used.
Step 3:	When a failure occurs in a domain, the reactive incident analysis service of the corresponding management domain (e.g. MD1) tries to heal the impacted service locally. This capability is domain internal.
Step 4:	When the service healing is not possible in the management domain's local scope then the problem is escalated towards the E2E management domain using the health issue reporting service. For this the provide health issue notification of the health issue reporting service as specified in clause 6.5.4.2.5 of ETSI GS ZSM 002 [2] is used.
Step 5:	The E2E management domain evaluates the situation using the E2E anomaly detection service and the responsible E2E service closed loop determines the required management domain level reconfiguration actions, e.g. in MD1 and MD2. This capability is domain internal
Step 6:	The required actions are performed in the respective MDs using the manage resource configuration capability of the Resource configuration management service.

5.1.4 Capability change notification across management domains

5.1.4.1 Description

In this scenario a Management Domain (MD) A use capabilities provided by another management domain B. Over the course of time management domain B may improve or remove capabilities such as, for example: management domain B adds the capability to support new geographies, or technologies that support shorter delay in the network, no support for an older technology. In such cases MD A should automatically become aware of these changes.

5.1.4.2 Proposed Solution

Table 5.1.4.2-1: Steps in solution

Precondition: Management Domain A and B exist. **Target:** Management domain A is informed of any changes in Management Domain B's resources. NOTE: Either of the domains could be the E2E MD.	
Solution Alternative 1: Event driven.	
Step 1:	Management Domain A configures a condition using the condition detection service of Management Domain B, requiring to report any changes in inventory of management domain A (this is typically done via the integration fabric). For this the manage conditions detection service (as specified in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]) in an MD is used.
Step 2:	After a new resource appears in MD B, the condition management service publishes an event over the integration fabric notifying MD A that new capability is available in MD B. For this, the event publication capability Provide condition state change Notifications of condition detection service (as specified in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]) in an MD is used.
Solution Alternative 2: Using monitoring closed loop.	
Step 1:	MD A creates a periodic closed loop, with a configurable period, consisting only of the observe, decide, and act stages. For this the Request M2O CL capability as specified in clause 6 is used.
Step 2:	In the observe stage MD A gets updated with the set of resources from MD B, if any. For this the manage inventory capability of the domain inventory management service as specified in clause 6.5.5.2.6 of ETSI GS ZSM 002 [2] is used.
Step 3:	In the decide stage, MD A checks internally if there are changes in the set of resources of MD B as reported in Step 2. if yes, the act state is triggered. This is an internal capability.
Step 4:	In the act stage, MD A updates the related inventories. For this the manage inventory capability of the domain inventory management service as specified in clause 6.5.5.2.6 of ETSI GS ZSM 002 [2] is used.
Step 5:	MD A checks for updates again same as in step 2 after the period has passed.

5.1.5 Automated detection of a management domain's inability to support the assigned part of the E2E Service

5.1.5.1 Description

In this scenario a E2E Management Domain (MD) A use a service provided by another management domain B to support the E2E Service. Over the course of time management domain B may not be able to support its part of the E2E service such as, for example: due to removal of an older technology, failure in MD B network. In such cases MD A should automatically become aware of these changes.

5.1.5.2 Proposed Solution

Table 5.1.5.2-1: Steps in solution

Precondition: E2E MD A and MD B exist. MD B supports E2E A in at least one E2E service. **Target:** E2E MD A shall be notified if MD B is unable to support the part of at least one E2E service in MD B	
Solution Alternative 1: Event driven	
Step 1:	E2E MD A asks the inter-domain integration fabric to configure a condition relating to the SLA/SLS of the part of the E2E Service using the condition detection service in Management domain B. For this the post execution coordination service detection service (as specified in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]) in an MD is used.
Step 2:	The integration fabric uses the condition detection service instance in management domain B to evaluate if it is possible to set such a condition. If yes, the condition is set using the manage conditions detection service (as specified in clause 6.6.3.2.2 of ETSI GS ZSM 002 [2]).
Step 3:	When an SLA/SLS is violated in MD B, the MD B condition management service publishes an event over the integration fabric. MD A is notified of the failure since it has subscribed to such notifications. For this the event publication capability Provide condition state change Notifications of domain condition detection service (as specified in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]) is used.
Step 4:	The inter-domain integrations fabric informs E2E MD A about event.
Solution Alternative 2: Monitoring closed loop	
Step 1:	E2E MD A creates a periodic closed loop consisting of observe, decide, and act stages. For this the Request M2O CL capability as specified in clause 6 is used.
Step 2:	In the observe stage E2E MD A monitors the performance KPIs of the MD B part of the E2E Service. For this the get batch measurements capability of the performance measurements collection service as specified in clause 6.5.2.2.3 of ETSI GS ZSM 002 [2] is used.
Step 3:	In the decide stage, E2E MD A checks if the monitored KPIs meet the requirement of the respective E2E Service. If not, act state is triggered with the appropriate resolution. This is an internal capability.
Step 4:	In the act state the appropriate resolutions from the decision state are carried out. This uses the capabilities related to domain orchestration (clause 6.5.5) or domain control (clause 6.5.6) of ETSI GS ZSM 002 [2] as required.
Step 5:	After the period, MD A checks for performance updates again repeating step 2.

5.2 Analytics in closed loops

5.2.1 Dynamic configurability of E2E service monitoring

5.2.1.1 Description

Every time a new E2E Service is deployed, various aspects of the E2E Service need to be monitored to ensure that the overall service KPIs (with regards to maintaining the SLA/SLS of the service) are being met. In addition to basic monitoring for adherence to SLA/SLS, the E2E service may, for example, also be monitored to draw inference about the expected performance of the E2E service by the respective analytics service. In this scenario the analytics service may require different information at different levels of detail (for example periodicity) at different times. Hence there may be a need for the E2E management domain to dynamically change the requested monitoring details from the respective management domains where the E2E service is deployed. This solution is related to clauses 6.4.1 and 6.4.4 of ETSI GS ZSM 001 [i.1].

5.2.1.2 Proposed Solution

Table 5.2.1.2-1: Steps in solution

Precondition: The E2E management domain receives a request to deploy a E2E service with certain SLA/SLS. **Target:** The monitoring of the E2E service reported from the management domains to the E2E domain is dynamically configurable.
Solution alternative:
Step 1: E2E service domain evaluates E2E service SLA/SLS requirements and sends requests to the management domain for the required monitoring data. This is done using the "Configure Measurements" capability in clause 6.5.2.2.2 or Configure batch measurement capability of clause 6.5.2.2.3 of ETSI GS ZSM 002 [2]. Step 2: Based on the requested monitoring data the E2E management domain receives monitoring data from the respective domains. For this the provide measurements capability of clause 6.5.2.2.2 or Provide batch availability Notifications of clause 6.5.2.2.3 of ETSI GS ZSM 002 [2] is used. Step 3: At a later stage new monitoring configuration requirements towards the management domains may be derived. EXAMPLE: The analytics service may request different data). This is an internal capability. Step 4: These new configurations are applied (same as in Step 1) to the MDs. New monitoring data is received from the management domains based on the new request configuration same as in Step 2. The loop (Step 3 to Step 4) continues as long as the E2E service is active.

5.2.2 Modifying services based on analytics' insights

5.2.2.1 Description

A new E2E Service is deployed across a set of management domains as determined by the E2E management domain. During the lifetime of the E2E service, the analytics services of an involved management domain provide insights that may result in the E2E management domain modifying the E2E service. This solution is related to clauses 6.4.2 and 6.4.3 of ETSI GS ZSM 001 [i.1].

5.2.2.2 Proposed Solution

Table 5.2.2.2-1: Steps in solution

Precondition: The E2E management domain has deployed an E2E service across management domains, say MD1, MD2, MD3. **Target:** The E2E service is modified based on insights received from any one of the domains MD1-3.
Solution alternative:
Step 1: E2E management domain evaluates E2E service requirements and deploys the E2E service across management domains MD1, MD2, and MD3. The manage service lifecycle capability as in clause 6.5.5.2.1 of ETSI GS ZSM 002 [2] is used for this purpose. Step 2: The analytics service in any one of the domains MD1, 2, 3 or the E2E MD provides an insight about the E2E service. The insight is received by an E2E MD as it may not be possible to be handled locally. EXAMPLE 1: The insight is about the possible increase in demand in a specific coverage area. See clause 5.1.5 on the solution for how this is done. Step 3: The E2E MD based on the received insight modifies the E2E service. EXAMPLE 2: Increases the resources, like spectrum, for that coverage area. The manage service lifecycle capability as in clause 6.5.5.2.1 of ETSI GS ZSM 002 [2] is used for this purpose.

5.2.3 Maintaining AI Models in Analytics

5.2.3.1 Description

AI models can be applied in domain analytics services for a specific goal (e.g. anomaly detection, root cause analysis). The models developed using training data collected during a certain time period may degrade as time passes and the target environment changes, causing incorrect analysis results or overlooking failures. To detect such performance degradation of AI models and improve them, a set of management services (AI model management service, deployed AI model assessment service, AI training data management service, Deployed AI model performance evaluation service) are specified in ETSI GS ZSM 002 [2]. The present scenario provides a possible solution for the maintenance of AI models by those management services in a zero-touch manner.

5.2.3.2 Proposed Solution

Table 5.2.3.2-1: Steps in solution

Precondition: The AI model created by AI model management service is operational in the domain analytics service. **Target:** The AI model is updated based on its performance to keep a proper closed-loop operation.	
Solution alternative	
Step 1:	Deployed AI model performance evaluation service producer as specified in clause 6.6.3.2 of ETSI GS ZSM 002 [2] provides the notification of performance degradation of the AI model to the deployed AI model assessment service via the appropriate integration fabric.
Step 2:	The deployed AI model assessment service producer as specified in clause 6.6.4.2.2 of ETSI GS ZSM 002 [2] publishes the decision result on the most appropriate action for the degraded deployed AI model in the cross-domain integration fabric.
Step 3:	If the decision result in Step 2 is re-training, AI model management service producer as specified in clause 6.6.4.2.1 of ETSI GS ZSM 002 [2] updates the AI model using new AI training data derived by AI training data management service producer as specified in clause 6.6.4.2.3 of ETSI GS ZSM 002 [2].
Step 4:	The AI model management service producer configures the domain analytics to replace the existing AI model used in its analysis with the updated one at a particular time.

5.3 Closed loop coordination

5.3.1 Coordination between multi-domain closed loops

5.3.1.1 Description

When an unexpected event occurs such as an earthquake or when a large-scale event is held, demands for network services increase. It may be necessary for a specific Management Domain (say MD-A) to cope with the increase of demands e.g. a sudden increase of traffic or loads on managed entities. In such cases, CLs in MD-A take action and may need to report information (e.g. results of action taken by the CL in MD-A) to CLs in E2E service MD. In such cases, to proactively mitigate the impact caused by the event, CLs in E2E service MD should have the ability to delegate roles (e.g. of Analytics or Decision) to lower CLs in other MDs (say MD-B). This definition is related to clause 7.2.2 of ETSI GS ZSM 009-1 [3].

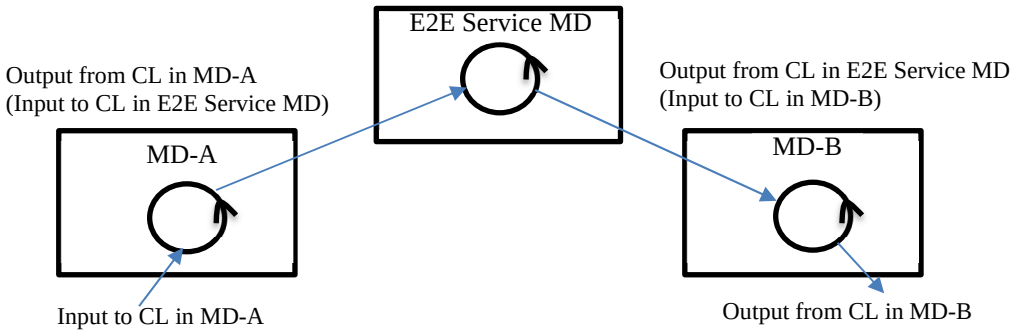

Figure 5.3.1.1-1: Interaction between CLs at different levels

5.3.1.2 Proposed Solution

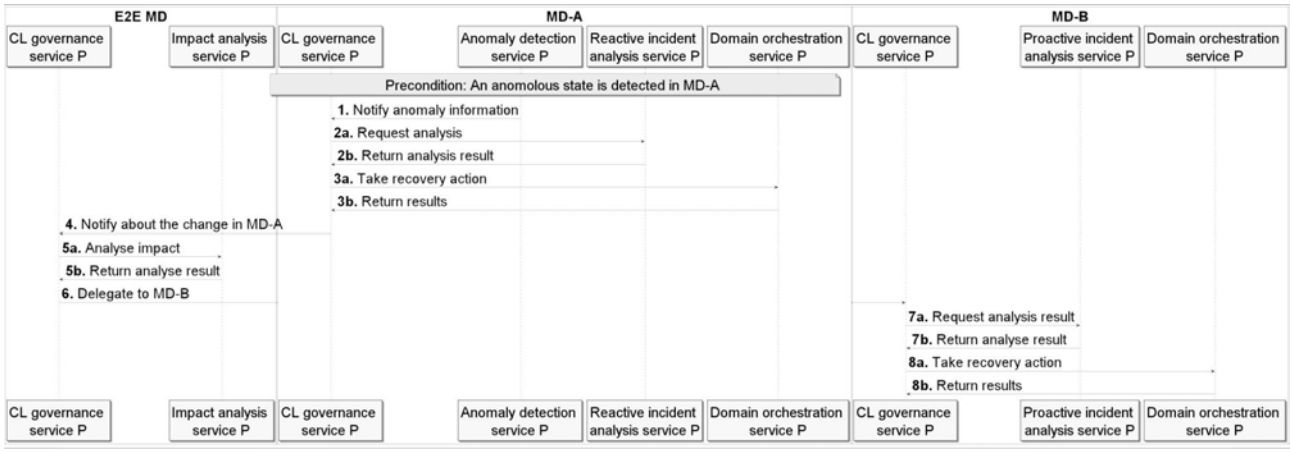

Figure 5.3.1.2-1: Solution alternative for coordination between multi-domain closed loops

Table 5.3.1.2-1: Steps in solution

Precondition: The E2E management domain has deployed an E2E service across management domains and the CL governance service producer in MD-A has set a subscription to get information related to anomaly in MD-A. **Target:** MD-A reports the changed management information which also has an impact on management information in E2E MD. Based on the change in MD-A, the CL in E2E MD further delegates to MD-B.	
Solution alternative	
Step 1:	An anomalous state (e.g. sudden increase of traffic or load on managed entity, etc.) is detected in MD-A and Anomaly detection service producer notifies the information to CL governance service producer, using Provide analysis result capability as described in clause 6.5.3.2.1 in ETSI GS ZSM 002 [2].
Step 2:	The reactive incident analysis service producer analyses the anomalous state using Request analysis result capability as described in clause 6.5.3.2.1 in ETSI GS ZSM 002 [2].
Step 3:	Based on the analysis derived in Step 2, the CL in MD-A takes a recovery action by using Manage service lifecycle and/or Execute workflow capabilities as described in clause 6.5.5.2.1 of ETSI GS ZSM 002 [2], offered by Domain orchestration service producer. The change to management information in the MD-A has an impact on management information in E2E service MD.
Step 4:	The change derived in Step 3 is notified to higher closed loop entity such as E2E service MD using Request issue resolution capability of Closed loop governance service producer as described in clause 9.2.1 in ETSI GS ZSM 009-1 [3].
Step 5:	The CL governance producer in E2E service MD request Impact analysis service producer to analyse the report from MD-A, and derives which MD is affected by the change with the service capability Request analysis result as described in clause 6.6.3.2.1 in ETSI GS ZSM 002 [2].
Step 6:	Delegation to lower closed loop entity such as MD-B is proceeded through closed loop governance service producer in MD-B providing Manage goal capability as described in clause 9.2.1 in ETSI GS ZSM 009-1 [3].
Step 7:	CL governance service producer in MD-B requests Proactive incident analysis service producer to analyses the information from E2E Service MD through the Request analysis result service capability as described in clause 6.5.3.2.1 in ETSI GS ZSM 002 [2].
Step 8:	The Domain orchestration service producer takes a necessary action using Manage service lifecycle and/or Execute workflow capability as described in ETSI GS ZSM 002 [2].

5.3.2 Knowledge sharing across closed loops

5.3.2.1 Description

The knowledge within a closed loop provides means for storing and retrieving knowledge data that is shared between the stages of the closed loop, as well as between different closed loops. The types of stored knowledge data can be configuration data, operational data, and historical data. This stored knowledge data can be accessed by some functions in the ZSM framework that need such data for assessment, deriving insights, making decisions, and so forth. To share the stored knowledge data cross closed loops, a set of cross-domain data services (data store management service, data persistence services, data processing service) specified in ETSI GS ZSM 002 [2] may be utilized.

5.3.2.2 Proposed Solutions

5.3.2.2.1 Knowledge Sharing across management domains

Table 5.3.2.2.1-1: Steps in solution

Precondition: An E2E Service is deployed in a set of management domains (e.g. AN in MD1, TN in MD2, CN in MD3) as determined by the E2E management domain. Each management domain supports a part of the E2E service. It is assumed that within each management domain, MD1, MD2, and MD3, closed loops CL1, CL2, CL3 are respectively running each with corresponding knowledge, K1, K2, K3. **Target:** The stored knowledge data is used to enhance the functioning of closed loops across management domains.	
Solution alternative	
Step 1:	During the lifecycle of the E2E service, the MD1 detects that it needs shut down for maintenance and is not able to support a part of the E2E service: The MD1 reports the shutdown event to the E2E management domain. This is done using the Escalate issue capability of the closed loop governance service in clause 9.2.2 of ETSI GS ZSM 009-1 [3].
Step 2:	The E2E management domain determines that a new management domain MD4 needs take over the responsibilities of MD1 based on evaluating knowledge data in K1 of CL1 and from other MDs. The E2E MD uses the Query knowledge capability of the Knowledge base service as specified in clause 6.5.4.2.4 of ETSI GS ZSM 002 [2].
Step 3:	After checking the access rights, the E2E management domain may choose to share securely some knowledge data (e.g. models/algorithms for insight derivation, list of root causes and the recommended solutions) from K1 (of CL1 in MD1) with the Knowledge (say, K4) of CL4 in MD4 to help CL4 accelerate the convergence speed of models/algorithms or enhance the accuracy of deriving insight and making decision when managing part of its service. This is done using a combination of create knowledge base, if it is absent, and add new data set using the corresponding capabilities defined in Knowledge base service as specified in clause 6.5.4.2.4 of ETSI GS ZSM 002 [2]. If the knowledge base service is available at the E2E level, then the MD4 may also access knowledge data needed from the E2E management domain.

5.3.2.2.2 Knowledge Sharing to detect the effects of Closed Loops actions after their execution

Table 5.3.2.2.2-1: Steps in solution

Precondition: An E2E Service is deployed in the E2E management domain with a set of closed loops deployed within the same management domain or different management domain. It is assumed that closed loops CL1, CL2, CL3 are running each with corresponding knowledge, K1, K2, K3. **Target:** CL1 detects the effects of its actions on CL2 and CL3.	
Solution alternative:	
Step 1:	CL1 triggers the execution of an action via the Domain orchestration service producer which takes the necessary action using Manage service lifecycle and/or Execute workflow capability as described in clause 6.5.5.2.1 in ETSI GS ZSM 002 [2].
Step 2:	CL1 notifies E2E MD about the action and request analysis of the executed action through the service capability Request analysis result as described in clause 6.5.3.2.1 in ETSI GS ZSM 002 [2].
Step 3:	The E2E MD notifies CL2 and CL3 about the action executed by CL1 and requests CL2 and CL3 to evaluate the action through the service capability Request analysis result as described in clause 6.5.3.2.1 in ETSI GS ZSM 002 [2].
Step 4:	CL2 and CL3 monitor the effects (e.g. on their respective KPIs) of the CL1 action. CL2 and CL3 analyse the effects and impacts of CL1 action.
Step 5:	CL2 and CL3 notify the E2E MD about observed effects using the post-execution coordination service (clause 9.3.3 of ETSI GS ZSM 009-1 [3]) and the Provide notification of conflicting actions capability. The notification may be an indication that the action conflicts with the actions of CL2 or CL3. The notification may refer to an index that quantitatively describes the quality of the action.
Step 6:	The E2E MD notify CL1 about the effects observed or computed by CL2 and CL3 based on the action that was executed by CL1 using the Provide analysis result capability as described in clause 6.5.3.2.1 in ETSI GS ZSM 002 [2].

5.3.3 Limiting actions of a closed loop

5.3.3.1 Description

There may be cases where two or more CLs can execute concurrent actions on a managed entity. These CLs may therefore cause conflicts in the functioning of the managed entity. A coordinating entity (authorized common consumer of the two CLs), for example, another closed loop or operator, should be able to configure the closed loops to minimize such occurrences. One possible solution consists in limiting the actions a CL can take over the managed entity.

5.3.3.2 Proposed Solution

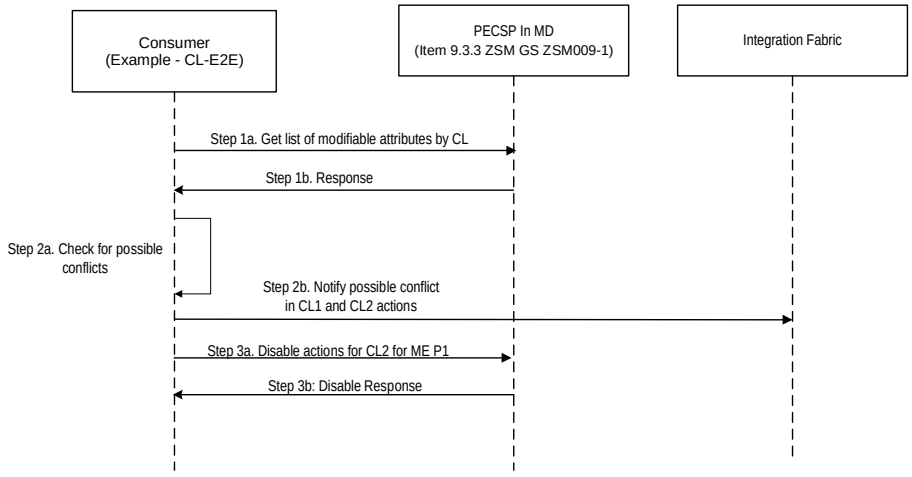

Figure 5.3.3.2-1: The steps in proposed solution

Table 5.3.3.2-1: Solution to scenario

Precondition: In an operator network a closed loop (CL-E2E) is running in the E2E MD and coordinates with CL1 and CL2 in MD1. CL1 and CL2 both act on configuration parameter P1 of managed entity ME1. In this case the CL-E2E is the Consumer. **Target:** The CL-E2E disables CL2 for configuring parameter P1.	
Solution alternative:	
Step 1:	The CL-E2E gets all possible actions that CL1 and CL2 can execute, including those on ME1 from the Post-Execution Coordination Service Producer (PECSP). For this the capability Manage Closed Loop action as specified in clause 6 of the present document is used.
Step 2:	The CL-E2E using a proprietary algorithm determines that the probability of conflict between CL1 and CL2 for parameter P1 of ME1 is high and as a resolution determines that only CL1 should configure P1. This is an internal capability. If a conflict is detected a notification of conflict detection may be published in the integration fabric using the provide notification of conflicting actions capability of the post execution coordination service as specified in clause 6 of the present document. Any entity interested in this notification may subscribe to receive it via the integration fabric.
Step 3:	CL-E2E disables CL2 from configuring P1. For this the capability Enable/Disable actions as described in clause 9.3.3 in ETSI GS ZSM 009-1 [3] is used.

5.3.4 Pre-action conflict management between closed loops

5.3.4.1 Description

When multiple closed loops are running on managed entities, their actions may cause undesirable results on the managed entities. To avoid this, the closed loops should be able to interact and optimize the effects of their actions. One possible solution is to check action plans before their execution to identify conflicting actions. After identification of conflicting decisions or action plans, the correct set of action plans needs to be selected - this implies using the manage closed loop action plans capability to create new or disable existing action plans for a given CL.

5.3.4.2 Proposed Solution

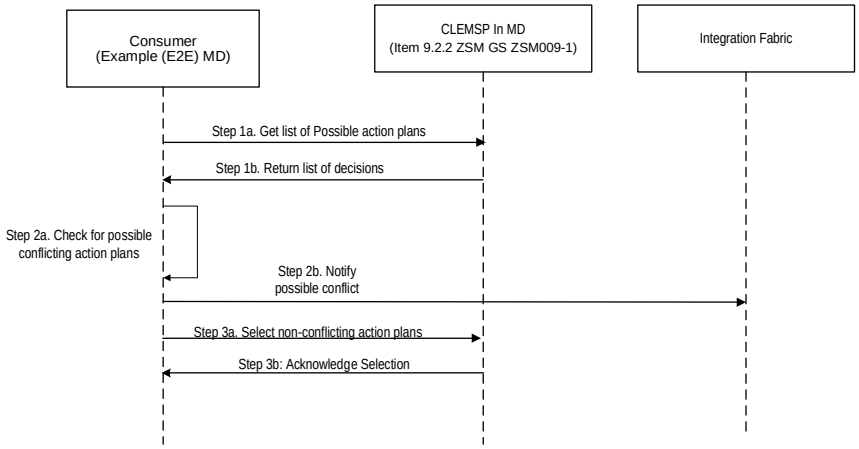

Figure 5.3.4.2-1: The steps in proposed solution

Table 5.3.4.2-1: Solutions to scenario

Precondition: The (E2E) MD has deployed an (E2E) service across MDs including MD1. The (E2E) MD coordinates CL1 and CL2 in MD1. **Target:** The (E2E) MD detects a conflict in the action plans provided by CL1 and CL2 after the decision stage and selects appropriate decisions/action plans to avoid such a conflict. NOTE: "(E2E) MD" is used to signify either the E2E MD or just an MD.
Solution alternative
Step 1: The consumer (for example (E2E) MD) retrieves the action plans from CL1 and CL2 from the closed loop execution management service producer (CLEMSP) in MD1. For this the capability Manage Closed Loop action plans as described in clause 9.2.4 in ETSI GS ZSM 009-1 [3] is used. Step 2: The (E2E) MD checks if there are any conflicting actions based on the information of action plans. If yes, the CL-E2E notifies the existence of the conflict to CL1 and CL2. For doing this the capability provide notifications of conflicting action plans of the Pre-action coordination service as described in clause 9.3.2 in ETSI GS ZSM 009-1 [3] is used. Step 3: Non-conflicting action plans in CL1 and CL2 are selected. This can be done by disabling the conflicting action plans in one of the CL and/or adding other possible action plans to the CLs. For this the capability Manage Closed Loop action plans as described in clause 9.2.4 in ETSI GS ZSM 009-1 [3] is used.

5.4 Closed loop governance

5.4.1 Enabling pause points in a closed loop

5.4.1.1 Description

Closed loops within the ZSM framework shall allow the consumer (operator or another closed loop) to enable "pause points" of a closed loop at points in the CL chain. When enabled, at each of these "pause points" all flows of the closed loop are paused, and the CL consumer is notified. The CL consumer can then review the status of the CL at that point and decide to let it continue or not. Other stages in the closed loop may continue to execute in parallel. For example: prior to letting a closed loop execute certain actions, the operator may review these actions. To do this the operator enables a pause point prior to execution. Once the operator trusts the execution of the closed loop, the pause point is disabled.

5.4.1.2 Proposed Solution

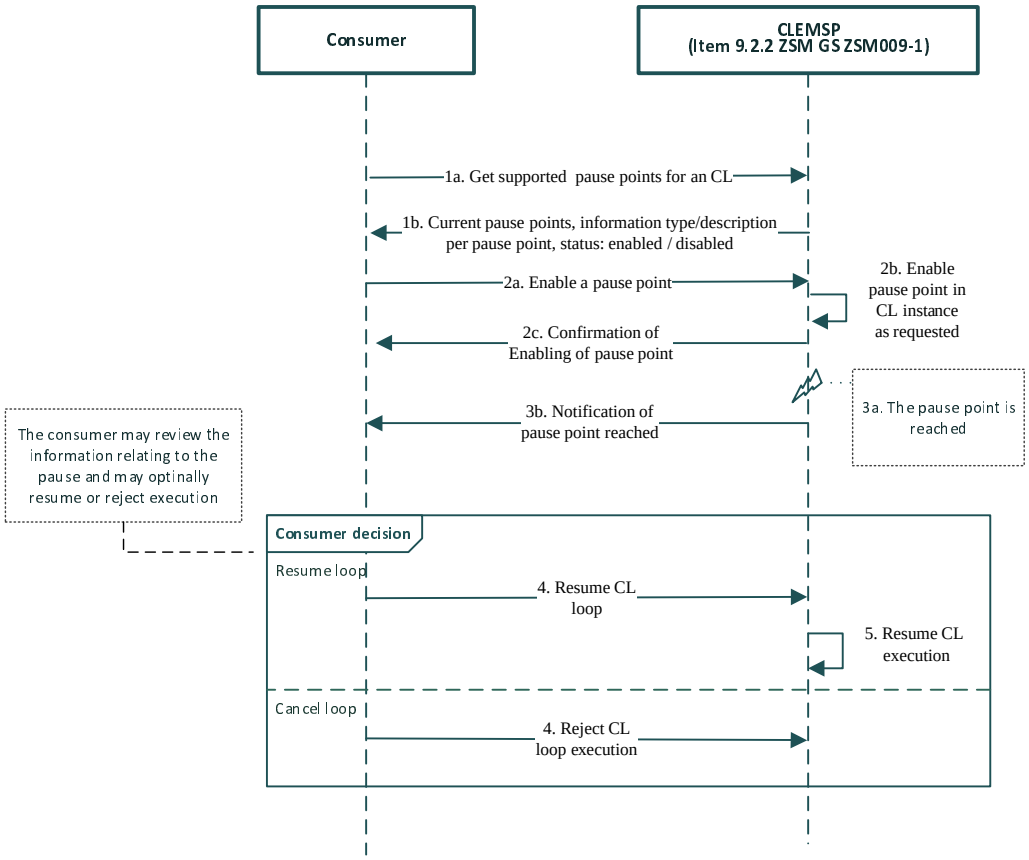

Figure 5.4.1.2-1: Solution for enabling a pause point of a closed loop

Table 5.4.1.2-1: Steps in solution in figure 5.4.1.2-1

Precondition: A closed loop (CL1) is running in MD1. **Target:** The consumer enables the pause point to pause the execution of all flows of CL1 before actions are executed to be able to review the said actions. Then the consumer approves the actions for execution.
Solution alternative (Steps refer the sequence diagram in figure 5.4.1.2-1)
Step 1: The consumer gets all pause points are supported by a CL (in this case CL1) from the closed loop execution management service producer (CLEMSP) in MD1. For this the capability Provide closed loop pause point information as described in clause 9.2.4 in ETSI GS ZSM 009-1 [3] is used. Step 2: The consumer enables a pause point in CL1 chain using the CLEMSP. For this the capability Enable/Disable pause point(s) as described in clause 9.2.4 in ETSI GS ZSM 009-1 [3] is used Step 3: Eventually a flow in CL1 reaches the enabled pause point and the CLEMSP notifies the consumer. For this the capability Provide notification for a pause point reached as described in clause 9.2.3 in ETSI GS ZSM 009-1 [3] is used. Step 4: The consumer reviews the actions about to be executed by CL1 and approves them for execution using the CLEMSP. For this the capability Continue closed loop execution as described in clause 9.2.4 in ETSI GS ZSM 009-1 [3] is used. Optionally, the consumer may choose to reject further execution. Step 5: If the consumer approves further execution of the CL, the execution of CL1 resumes.

5.4.2 CL Goal configuration

5.4.2.1 Description

E2E services and the MD services composing them will be deployed in the respective management domains with the respective SLA or SLS. These SLA/SLS may be translated to closed loop goals in the respective MDs. Goals at both E2E and MD level would need to be configured in the individual management domains. In addition, these goals would need to be translated to conditions that the closed loops will track or translated to other goals. The solution alternative for doing so is shown in figure 5.4.2.2-1.

5.4.2.2 Proposed Solution

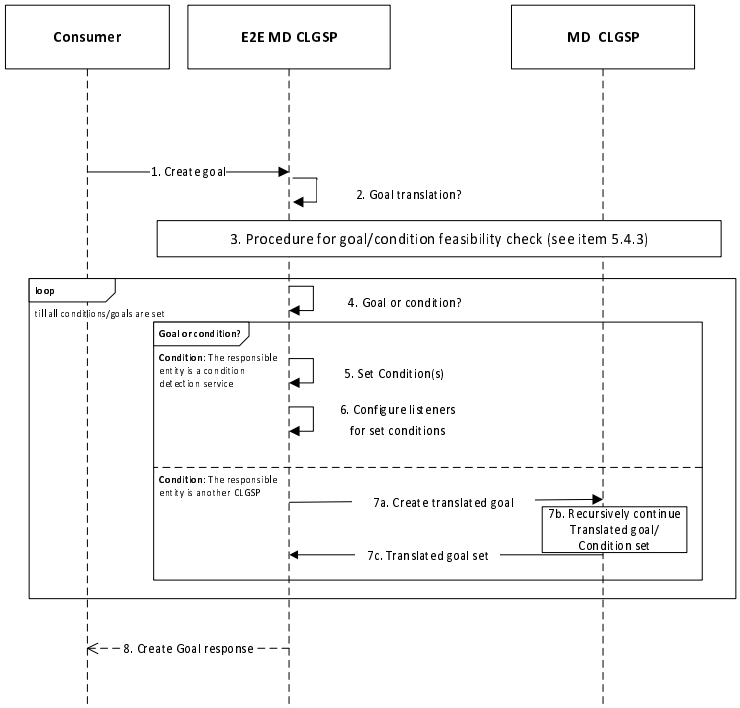

Figure 5.4.2.2-1: Solution for goal configuration

Table 5.4.2.2-1: Steps in solution in figure 5.4.1.2-1

Precondition: The consumer wants to configure a goal in the E2E MD **Target:** The corresponding translated goals and conditions are configured in the respective MDs.
Solution alternative: (Steps refer the sequence diagram in figure 5.4.2.2-1)
Step 1: The consumer configures a new goal in the E2E MD using the Closed Loop Governance Service Producer (CLGSP). For this capability Manage Closed Loop Goal as described in clause 9.2.2 in ETSI GS ZSM 009-1 [3] is used. Step 2: The E2E CLGSP translates the goal into a list of "translated goals" or conditions configurable in the various composing MDs. Step 3: Procedure for each goal/condition a feasibility check is performed as described in clause 5.4.3. If not successful, a failure report is sent to the consumer of the manage goals service. **Loop: For each translated goal/condition from step 2 do** Step 4: Check if entity is a goal or a condition **If condition** Step 5: The condition is created and activated in the appropriate CDSP. For doing this the capability Manage Conditions and Activate/deactivate conditions described in clauses 6.6.3.2.3 and 6.5.3.2.2 of ETSI GS ZSM 002 [2] is used. Step 6: Setting a condition also requires configuring the appropriate listener for the notification when the set condition is met. In this step the appropriate entity that will listen for such a notification is configured to subscribe to the condition notification from the condition detection service. **Else if translated goal** Step 7: Configure the translated goal in the appropriate MD CLGSP. The MD CLGSP may recursively repeat the steps in this procedure to set the translated goal. For this the capability Manage Closed Loop Goal as described in clause 9.2.2 in ETSI GS ZSM 009-1 [3] is used. **Endif** **End loop** Step 8: If all succeeds a positive acknowledgement is provided to the consumer.

5.4.3 CL Goal feasibility check

5.4.3.1 Description

To ensure service assurance an E2E MD may need to configure multiple closed loop goals in different MDs simultaneously. These multiple goal configuration may succeed in some MDs but fail in others, resulting in ineffective and inconsistent configuration of the goals in the operator network. Hence, the E2E MD should check all goals for feasibility prior to configuration in the MD. Each MD on receiving a check for the feasibility of a closed loop goal may perform some sanity checks on that goal. For example, check that the goal is technically possible to achieve and that it does not conflict with existing goals in the MD.

5.4.3.2 Proposed Solution

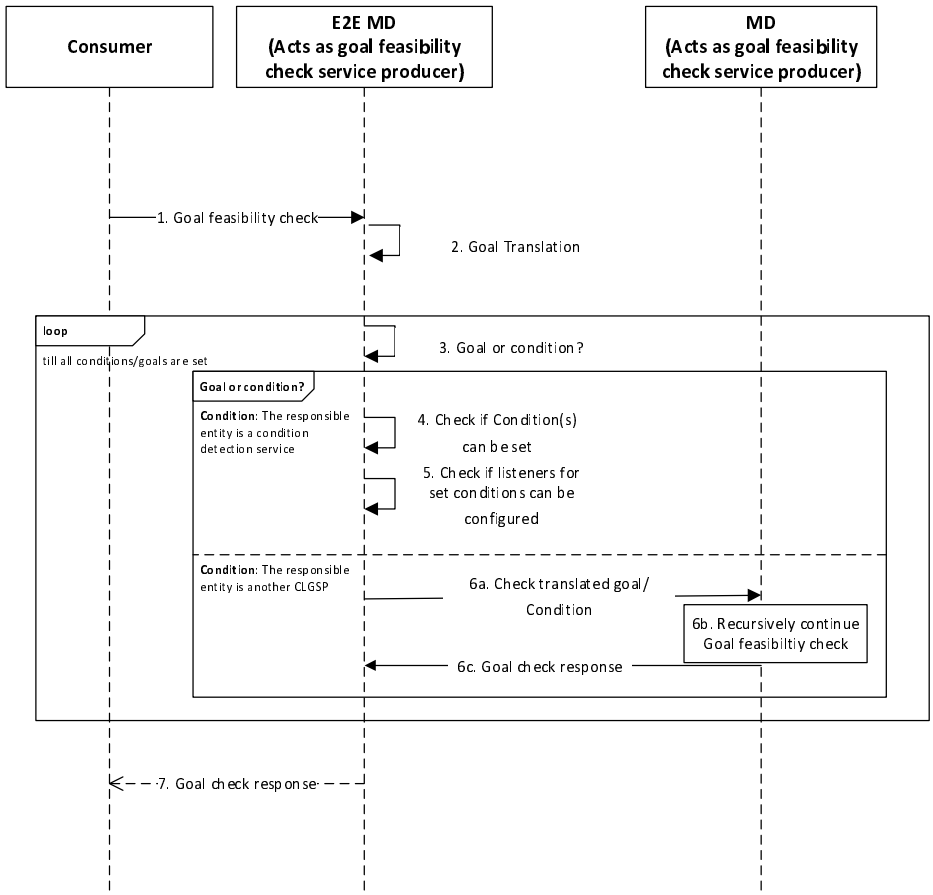

Figure 5.4.3.2-1: Solution for goal configuration

Table 5.4.3.2-1: Steps in solution in figure 5.4.3.2-1

Precondition: The consumer wants to check the feasibility of configuring a goal in the E2E MD **Target:** The E2E MD checks the feasibility of configuring the goal and relevant conditions in the E2E MD and other relevant MDs in the operator network and replies with a feasibility verdict.
Solution alternative (Steps refer the sequence diagram in figure 5.4.3.2-1)
Step 1: The consumer configures a new goal in the E2E MD using the Closed Loop Governance Service Producer (CLGSP). For this the capability Goal feasibility check as described in clause 6 is used. Step 2: The E2E CLGSP may now translate the goal to a of "translated goals" or conditions configurable in the various composing MDs. An example of a condition is threshold crossing for a given KPI (see clause 6.6.3.2.3 in ETSI GS ZSM 002 [2]). **Loop: For each translated goal/condition from step 2 do** Step 3: Check if entity in entity list from step 2 is goal or condition. **If condition** Step 4: The possibility of configuring the condition in the E2E MD is checked. Step 5: The possibility of configuring a listener to the set condition is checked. **Else if translated goal** Step 6: Check if the goal can be configured in the respective MD. This check triggers a recursive procedure within the respective MD identical to this procedure. **Endif** **End loop** Step 7: If all succeeds a positive acknowledgement is provided to the consumer.

5.4.4 Trigger based CL state change

5.4.4.1 Description

A network operator may not need to have CLs active and running all the time. For example, different CLs may be active during different periods of the day, or the execution of a CL may depend on the network usage. To automate this, a CL governance consumer should have the ability to associate conditions or triggers in the network with the transition of a CL state. Such associations will trigger the state transition of the associated CL. Examples of CL state transition include:

a) Activation of a control loop.

b) Deactivation of a control loop.

c) Pausing a control loop.

d) Suspension of a control loop.

e) Continuing a control loop.

Examples of triggers may include, but are not limited to:

a) Values of KPIs or attributes in the network, such as:

   i) Downlink throughput >5 Mbps (KPI).

   ii) Beam Tilt is set to 45°.

b) Events in the network, such as:

   i) New provisioning request received.

   ii) Managed entity deactivated.

c) Time of the day.

d) Other control loop state changes.

5.4.4.2 Proposed Solution

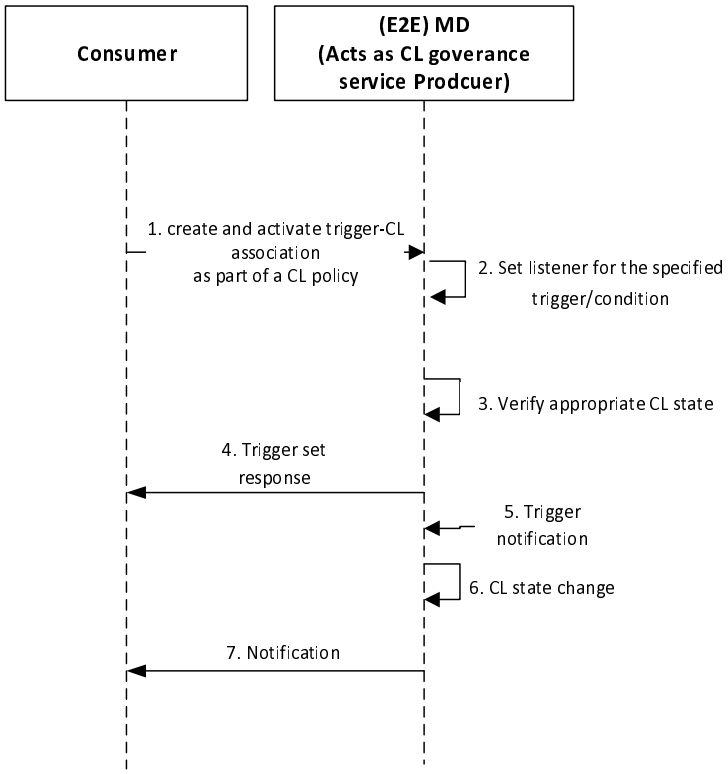

Figure 5.4.4.2-1: Solution for trigger-based CL state change

Table 5.4.4.2-1: Steps in solution in figure 5.4.4.2-1

Precondition: The consumer wants to enable a trigger-based CL State change. **Target:** A trigger is associated to a CL state change and is enabled such that when the condition of the trigger is detected in the network the CL state change is executed in the network. NOTE: "(E2E) MD" is used to signify either the E2E MD or just an MD.	
Solution alternative (Steps refer the sequence diagram in figure 5.4.4.2-1)	
Step 1:	The consumer configures and enables a trigger-based CL state transition in the (E2E) MD using the closed loop governance service producer (CLGSP). For this the capability manage closed loop policy as described in clause 9.2.2. of ETSI GS ZSM 009-1 [3] is used.
Step 2:	The (E2E) MD CLGSP may now set a condition in the network corresponding to the trigger. An example of a condition is threshold crossing for a given KPI. For this the manage conditions and activate/deactivate condition capabilities of the E2E service condition detection service as described in clause 6.6.3.2.3 in ETSI GS ZSM 002 [2] is used.
Step 3.	The (E2E) MD CLGSP verifies the correct state of the CL such that the requested CL state transition can happen. While CLs have a limited set of standardized states, the verification of the correct state is left for internal implementation.
Step 4:	The (E2E) MD CLGSP responds with the success or failure of the enable request.
Step 5:	Eventually, a condition is triggered in the network corresponding to an enabled trigger-based CL state change. The notification is published in the network using the Provide condition state change notifications capability of the E2E service condition detection service of clause 6.6.3.2.3 of ETSI GS ZSM 002 [2].
Step 6:	The (E2E) MD CLGSP is responsible for overseeing the state change of the CL. This is performed using the Manage CL Lifecycle capability as in clause 9.2.2 of ETSI GS ZSM 009-1 [3].
Step 7:	If notifications are enabled a notification of CL state change is provided to the consumer. This is performed using the Provide notification of CL goal change capability as in clause 6 of the present document.

5.4.5 Trigger based CL Goal change

5.4.5.1 Description

A network operator may want to trigger the optimization of different aspects of the network under different conditions. For example, a network operator may optimize resource consumption under low loads and may want to optimize QoS for user sessions under high loads. To automate such behaviour a CL governance consumer should have the ability to configure associations between various conditions, which, when met, will change the CL goal. This is an alternative way of addressing issue in clause 5.4.4 wherein the solution triggers a transition of the CL state, whereas here the solution updates the CL goal. In a deployed network both solutions may be used depending on the needs of the network.

5.4.5.2 Proposed Solution

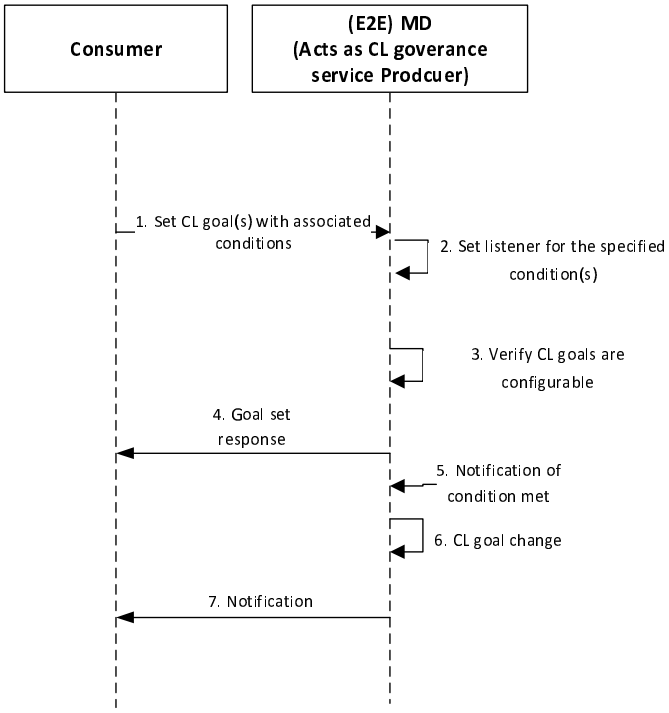

Figure 5.4.5.2-1: Solution for CL Goal change

Table 5.4.5.2-1: Steps in solution in figure 5.4.5.2-1

Precondition: The consumer wants to enable a trigger-based CL Goal change **Target:** A trigger is associated to a CL Goal change (and is enabled) such that when the condition of the trigger is detected the CL goal change is executed. NOTE: "(E2E) MD" is used to signify either the E2E MD or just an MD.	
Solution alternative (Steps refer the sequence diagram in figure 5.4.5.2-1)	
Step 1:	The consumer configures and enables a list of CL goals and the associated conditions that trigger their activation in the (E2E) MD using the Closed Loop Governance Service Producer (CLGSP). For this capability manage CL goal-condition association described in clause 6 of the present document is used. A default goal may be specified. The default goal is automatically used if a condition triggers the removal of an existing goal without specifying the next goal.
Step 2:	For each trigger in step 1 the (E2E) MD CLGSP may now set a corresponding condition in the network. An example of a condition is a threshold crossing over a given KPI. For this the manage condition and activate/deactivate conditions capabilities of the E2E service condition detection service as described in clause 6.6.3.2.3 in ETSI GS ZSM 002 [2] is used.
Step 3:	The (E2E) MD CLGSP verifies that the CL goal(s) is(are) correctly specified and can be configured in the CLs. Such a verification of the goal(s) could be performed using capability Goal feasibility check as described in clause 6.
Step 4:	The (E2E) MD CLGSP responds with the success or failure of the enable request.
Step 5:	Eventually, one of the set conditions is triggered in the network corresponding to a goal. The notification is published in the network using the Provide condition state change notifications capability of the E2E service condition detection service of clause 6.6.3.2.3 of ETSI GS ZSM 002 [2].
Step 6:	The (E2E) MD CLGSP is responsible for overseeing the goal change of the CL. This is performed using the Manage Closed Loop goal capability as in clause 9.2.2 of ETSI GS ZSM 009-1 [3].
Step 7:	If notifications are enabled a notification of CL goal change is pushed to the consumer.

5.4.6 M2O-CLs preparation and commissioning from multi-vendor stages

5.4.6.1 Description

Made-to-Order Closed Loops (M2O-CL), as defined in clause 7.4 of ETSI GS ZSM 009-1 [3], is a type of CLs assembled on demand by ZSM framework owner (or by other entities on behalf of the ZSM framework owner), using capabilities offered by the ZSM framework. Components of M2O-CLs originating from different ZSM framework vendors can be associated to a CL instance on demand. Therefore, it is important to define the capabilities needed to chain these different components together to prepare a M2O-CL for deployment.

5.4.6.2 Proposed Solution

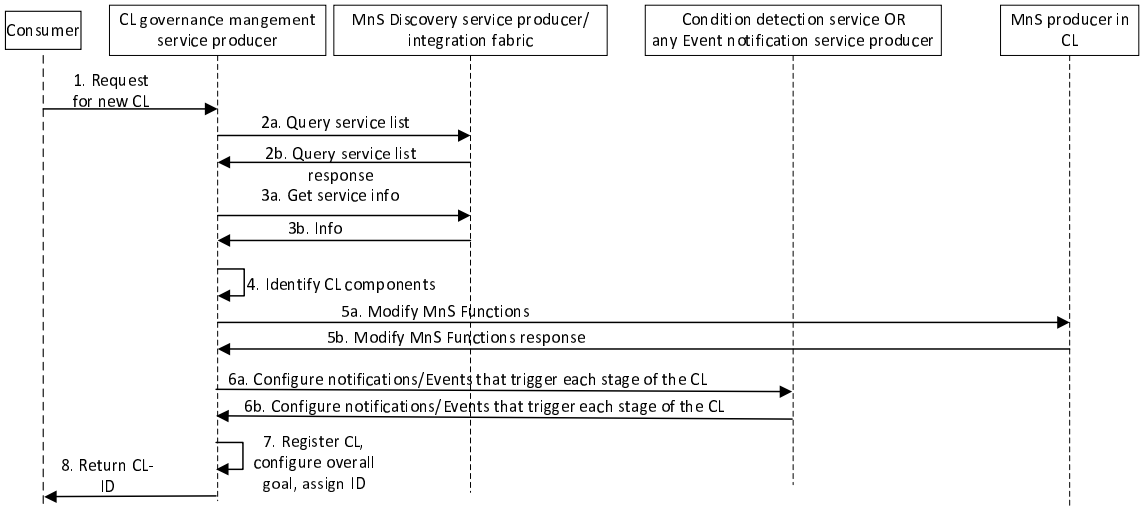

Figure 5.4.6.2-1: The steps in proposed solution

Table 5.4.6.2-1: Steps in solution in figure 5.4.6.2-1

Precondition: In an operator network, a M2O-CL is needed to monitor KPIs (KPI1, KPI2, etc.) and configure parameters (P1,P2, etc.) of managed entities (ME1,ME2, etc). The request for instantiating a new M2O-CL includes information to help the CLGMSP (CL Governance service producer) understanding which CL components are part of the M2O-CL (how this information is described is not in the scope of the present document). In this solution it is assumed that the CLGMSP receives sufficient information to construct a suitable M2O-CL. **Target:** a new M2O-CL is prepared and instantiated.
Solution alternative
Step 1: A consumer requests an M2O-CL by providing its description. This description maybe declarative or imperative in nature. In the imperative case the exact types of components or even the exact identifiers of components that form the closed loop may be provided. In the declarative case anywhere from the overall goal of the closed loop to the generic functionality of the components maybe provided. Furthermore, information description (declarative or imperative) includes details on how components may be chained together - including the conditions which determine the flows in those chains (see Condition Detection Service in clause 6.5.3.2.2 of ETSI GS ZSM 002 [2]). The description may include timeouts or time periods for various components of the closed loop. It may include functional and non-functional characteristics for the closed loop or parts of the closed loop chain - these characteristics may be used to decide on the closed loop components. To request the M2O CL the consumer may use the Request M2O CL capability of the CL governance service as described in clause 6 below.
NOTE 1: The following steps describe the situation in which the generic component functionality is provided in the CL description.
Step 2: CLGSP sends a request to the MnS Discover Service Producer the discover MnS implementations that form the components of the CL. For this the Query service list (described in clause 6.3.2.2 of ETSI ZSM GS 002 [2]) is used. The response includes where those services are located and address where to configure and access those management service implementations.
In case no match is found for a required component an error is returned.
Step 3: CLGSP may identify the exact functional and non-functional characteristics of each MnS producer that are returned in step 2. For this the Get service info capability of clause 6.3.2.2 of ETSI GS ZSM 002 [2] is used.
Step 4: CLGSP selects the CL component that meets the functional and non-functional characteristics with the required characteristics provided in step 1. This may be identified from the functional and non-functional characteristics of the CL component. Inputdatalist should match outputdatalists between subsequent CL components. In case no match is found for the required characteristics needed, an error is returned. This is an internal capability.
Step 5: The MnS producers that form the components of the CL are modified by the CLGMSP to correctly participate in the closed loop depending on the MnS. For example: The analytics service producer is modified to use the correct model. The performance service producer is modified to provide the correct KPIs. For these the appropriate configuration capabilities of the MnS are used.
Step 6: The conditions and events, including timeouts, durations and periods may be configured in this step. The flows in the CL along the different chains are configured in this step. For this an event notification providing capability, correct timeout, periods and durations or conditions and corresponding subscribers using the condition detection service (clauses 6.6.3.2.3 and 6.5.3.2.3 of ETSI GS ZSM 002 [2]).
NOTE 2: Steps 5 and 6 may be executed together.
Step 7: After identifying all components and creating the chains and the possible flows through them of the M2O-CL, the instance of Closed Loop is updated with information such as: closedLoopLifeCyclePhase = preparation, closedLoopComponentList = identified components and so forth, CL goal, other triggers using the CL Governance service in clause 9.2.1 of ETSI GS ZSM 009-1 [3].
Step 8: A response with the new CL instance ID and relevant state information is returned to the consumer.

6 Additional Capabilities

Table 6-1 shows capabilities additional to those specified in ETSI GS ZSM 002 [2] and ETSI GS ZSM 009-1 [3].

Table 6-1

Service name (and reference)	Additional Capability	Capability description
Closed loop governance service (clause 9.2.2 of ETSI GS ZSM 009-1 [3])	Goal feasibility check (M)	Check if a goal can be supported by an (E2E) MD. A timeout required after which the check is deemed to have failed, may be specified. If the feasibility check is successful, the ability to configure such a goal may only be valid for a limited duration. This time duration shall be provided together with the successful result. NOTE: "(E2E) MD" is used to signify either the E2E MD or just an MD.
Closed loop governance service (clause 9.2.2 of ETSI GS ZSM 009-1 [3])	Manage CL goal-condition association(s) (M)	Manage (create, read, update, delete, list) goal(s) of a Closed Loop in the respective management domain(s) and a corresponding condition that triggers the configuration or removal of the goal. Default goals may also be specified using this capability. This capability can be used for **conditional** delegation of goal(s) (as specified in clause 8.2.3) between different Closed Loops. Conditional delegation here means that the goal is only delegated if a pre-defined condition/notification is met.
Closed loop governance service (clause 9.2.2 of ETSI GS ZSM 009-1 [3])	Provide notification of CL goal change (M)	Provide a notification when the CL goal has been changed. Optionally, the cause for CL goal change may be provided. Examples of causes include configuration by an authorized consumer, trigger-based goal change and so on.
Closed loop governance service (clause 9.2.2 of ETSI GS ZSM 009-1 [3])	Request M2O CL (O)	Declares an M2O-CL providing a declarative or imperative description of it. Additional details required for constructing the M2O CL may be further specified.
Post-execution coordination service (clause 9.3.3 of ETSI GS ZSM 009-1 [3])	"Provide notification of conflicting actions" (M)	Provide notifications of potential conflicting action from different CLs when a conflict has been detected in the actions.
Post-execution coordination service (clause 9.3.3 of ETSI GS ZSM 009-1 [3])	"Manage closed loop actions"	Allow authorized entities to manage (R, U) Closed Loop actions.

History

Document history		
V1.1.1	June 2022	Publication