ETSI GR ZSM 017 V1.1.1 (2026-01)

GROUP REPORT

Zero-touch network and Service Management (ZSM); Closed-Loop Automation Security aspects

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
DGR/ZSM-017_CLA_Sec

Keywords
automation, closed control loop,
security requirements

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 IPR online database.

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™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

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

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

Introduction

The general ZSM security were studied and provided in ETSI GR ZSM 010 [i.1] and ETSI GS ZSM 014 [i.15], the autonomous, dynamic, and cross-domain nature of Closed Loops introduces a new and complex threat landscape within the ZSM framework. The present document covers security threat and risk analytics on the Closed Loop and Closed-Loop Automation within the ZSM framework, including the implementation of a single Closed Loop and the coordination/governance between multiple Closed Loops.

Several key security issues are identified according to security risk analytics, and potential solutions were proposed to mitigate the risks, which include:

- Trust issue of multiple Closed Loops during the coordination and build relationship between Closed Loops across multiple management domains.
- Access control for the coordination between different Closed Loops provided by multiple domain service producers of ZSM framework.

- Leverage Closed Loop security exposure mechanism to secure exposure of the management services between multiple Closed Loops within the ZSM framework.

1 Scope

The present document studies analysis of security risks related to Closed-Loop Automation (CLA) based on ETSI GS ZSM 009-1 [i.3], part 2 [i.8], part 3 [i.9], ETSI GR ZSM 010 [i.1], ETSI GS ZSM 014 [i.15] and ETSI GS ZSM 016 [i.12], as well as provides the gap analysis with ETSI GR ZSM 010 [i.1]. Based on the analysis conducted, the present report proposes new security capabilities for the ZSM framework architecture to support the mitigation of relevant security risks, especially those applicable to the coordination across Closed Loops from different management domains under the ZSM framework. Recommendations for future work are included in the present document.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI GR ZSM 010: "Zero-touch network and Service Management (ZSM); General Security Aspects".

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

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

[i.4] NIST SP 800-30 (Revision 1): "Guide for Conducting Risk Assessments".

[i.5] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[i.6] Recommendation ITU-T X.805 (10/2003): "Security architecture for systems providing end-to-end communications".

[i.7] MITRE Common Attack Pattern Enumeration and Classification (CAPEC) project.

[i.8] ETSI GS ZSM 009-2: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 2: Solutions for automation of E2E service and network management use cases".

[i.9] ETSI GR ZSM 009-3: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 3: Advanced topics".

[i.10] Benzaid C, Taleb T. ZSM security: Threat surface and best practices[J]. IEEE Network, 2020, 34(3): 124-133.

[i.11] ETSI GR ZSM 011 (V2.1.1): "Zero-touch network and Service Management (ZSM); Intent-driven autonomous networks; Generic aspects".

[i.12] ETSI GS ZSM 016 (V1.1.1): "Zero-touch network and Service Management (ZSM); Intent-driven Closed Loops".

[i.13] NIST SP 800-160v1r1: "Engineering Trustworthy Secure Systems".

[i.14] ETSI GR NFV-SEC 007 (V1.1.1): "Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments".

[i.15] ETSI GS ZSM 014 (V1.1.1): "Zero-touch network and Service Management (ZSM); ZSM security aspects".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

AAA	Authentication, Authorization and Account/Audit
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
CAPEC	Common Attack Pattern Enumeration and Classification
CDIF	Cross-Domain Integration Fabric
CL	Closed Loop
CLA	Closed-Loop Automation
CLC	Closed Loop Coordination
CLG	Closed Loop Governance
CLGSP	Closed Loop Governance Service Producer
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service attack
DIF	Domain Integration Fabric
DoS	Denial of Service
DPI	Deep Packet Inspection
E2E	End-to-End
E2ES	End-to-End Service
IAM	Identity and Access Management
IME	Intent Management Entities
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
KPI	Key Performance Indicator
LoA	Levels of Assurance
M2O-CL	Made-to-Order Closed Loop
MD	Management Domain
ML	Machine Learning
NFV	Network Function Virtualisation
OWASP	Open Web Application Security Project
RM-CL	Ready-Made Closed Loop
SDO	Standard Development Organization
SLA	Service Level Agreement
SLS	Service Level Specification

TRA	Threat and Risk Analysis
UEBA	User and Entity Behavior Analytics
VNF	Virtual Network Function

4 Security threats and risks analysis

4.1 Gap analysis with ETSI GR ZSM 010

4.1.1 Gap between ETSI GR ZSM 010 and the present document

In ETSI GR ZSM 010 [i.1], general approach was given to security threat and risk analysis for ZSM framework and some solutions were proposed to mitigate the security risks. According to the defined ZSM threat and risk analysis framework, the generic security threats and risk analysis for ZSM framework from assets perspective has been studied in ETSI GR ZSM 010 [i.1], including E2E Service management domain, E2E Service management function, E2E Service management service, etc. Security risks of Closed Loop and Closed-Loop Automation have not been analysed in detail.

As described in clause 7.1 of ETSI GS ZSM 002 [i.2], Closed Loops are composed of the building blocks defined in clause 6.1.2 of ETSI GS ZSM 002 [i.2] including management services, management functions, management domains, etc. Closed Loop is a type of control mechanism (refer to clause 6 of ETSI GS ZSM 009-1 [i.3]) to monitor and regulate a set of managed entities achieving a specific goal, which is composed by four stages: monitoring, analysis, decision and execution plus knowledge as its components. Closed-Loop Automation combined Closed Loop stages can be automatically processed to fulfill the Closed Loop's goal which is realized with the combination and chaining of management services (data, analytics, policy, orchestration, etc.). According to clause 5.2 [CL-general-5] in ETSI GS ZSM 009-1 [i.3], Closed Loop in a (E2ES) management domain or across management domains consists of different stages which are realized by one or more management functions/services across multiple management domains. In this scenario, the implementation of Closed Loop itself becomes more complex and the security risk analysis for Closed-Loop Automation will become more complicated. For example, E2E service data collection in E2E service management domain can be used in the Closed Loop monitoring stage and domain orchestration and control management services in another management domain may be used in Closed Loop execution stage. New security challenge will be introduced between two different trustworthiness management domains because the security capability and assurance of two management domains are different. Further, according to clause 5.2 [CL-general-15] in ETSI GS ZSM 009-1 [i.3], Closed Loops within the ZSM framework can collect data from multiple available and applicable data sources, including managed services, managed resources and Closed Loops. In the monitoring stage, it may collect data that is not within the scope of its authorization or collect too much data not needed for any function, resulting in data leakage and data privacy security issues.

Some general requirements about coordination, governance and interaction between Closed Loops (refer to [CL-general-3], [CL-general-4] and [CL-general-24] in clause 5.2 of ETSI GS ZSM 009-1 [i.3]) have been defined, Closed Loops stages/Closed Loops can be coordinated, governed and interacted with external entities (other Closed Loops and ZSM framework consumers) within a single management domain and multiple management domains. Thus, complex coordination, governance and interactions between Closed Loops across multiple management domains introduce new security challenges for ZSM framework. When the Closed Loop is in a hierarchical or peer relationship between service management domain and (E2E) service management domain, if the access policy (data policy and service policy) is improperly set, there is a security risk of unauthorized access to resources or service of CLs. Further, the exposure entitlements of CL's management services may change dynamically, if the configurations cannot dynamically adapt to such changes, it may cause inappropriate external visibility. As described in clauses 8.2.5.2 and 8.2.5.4 of ETSI GS ZSM 009-1 [i.3], some important interaction information (such as details on CL instance attributes involved in the interactions, action plans, etc.) are used in the Closed Loop Coordination (CLC) functionality. If there is no proper protection, it will be a security risk that important and sensitive data may be disclosed. Further, if the information sent or received by CL are stolen and tampered, CL may be unable to achieve the original goal using inaccurate information. Even worse, attackers may deplete the quantity of the resource available to service legitimate requests maliciously.

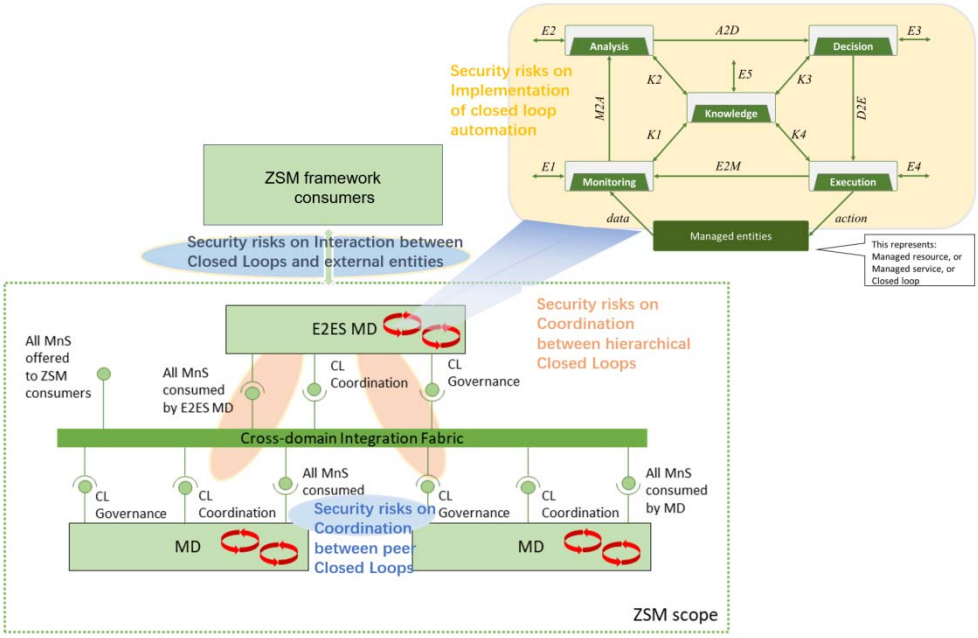

Figure 4.1.1-1: ZSM Closed-Loop Automation security risk analysis introduced in the present document

Figure 4.1.1-1 depicts the ZSM Closed-Loop Automation security risks analysis introduced in the present document. The security risk analysis can be performed from the implementation of a Closed Loop (clause 4.2) or from the coordination/governance between different Closed Loops across multiple management domains (clause 4.3).

To sum up, the present document provides new and specific security threats and risk analysis on Closed Loop and Closed-Loop Automation, which has not been covered by ETSI GR ZSM 010 [i.1] security study.

4.1.2 Relationship between ETSI GR ZSM 010 and the present document

The present document refers to the general methodologies, which are adopted in ETSI GR ZSM 010 [i.1], such as NIST 800-30 [i.4], ISO/IEC 27005 [i.5] and Recommendation ITU-T X.805 [i.6] for security Threat and Risk Analysis (TRA) of ZSM Closed Loop and Closed-Loop Automation. Closed Loops can be identified as assets in the ZSM framework which are composed of multiple assets including E2E Service management domain, E2E Service management function, E2E Service management service, Management Service management domain, etc. According to the clause 4.2 in ETSI GR ZSM 010 [i.1], security threats and risks for some assets have been studied in E2E service point of view including E2E Service management domain, E2E Service management function, E2E Service management service, Cross-Domain data service, Integration fabric and Collected data. Apart from security risk analysis for these assets, the present document analyses the security risk of ZSM Closed Loop and Closed-Loop Automation and focuses on the Closed Loop specific consequence of incident and potential countermeasures according to MITRE Common Attack Pattern Enumeration and Classification (CAPEC) [i.7].

The CL stages and functionalities (Closed Loop components) have been mapped to management functions based on the management services as defined the ETSI GS ZSM 002 [i.2] (refer to clause 7.3 of ETSI GS ZSM 009-1 [i.3]). The security threat and risk analysis for Closed Loop stages and coordination/governance of Closed-Loop Automation are performed according to the list of potential Deliberate threat category (refer to clause 4.1.4.1 of ETSI GR ZSM 010 [i.1]).

4.2 Threats and risk analysis on implementation of Closed-Loop Automation

4.2.1 Monitoring stage

According to clause 7.2.1 and clause 7.2.2 of ETSI GS ZSM 009-1 [i.3], the monitoring stage which is responsible for transferring, collecting and pre-processing data from managed entities or from external sources, provides information based on historical and/or streaming real-time data coming from various data sources. It also provides capabilities for tuning the data sources and data ingestion.

As described in clause 7.3 of ETSI GS ZSM 009-1 [i.3], the monitoring stage is realized, fully or in part, by the (domain or E2E) data collection management services from deployment view. Domain data collection services include event notification services, performance measurements streaming service, performance measurements collection service and log collection service (refer to clause 6.5.2 of ETSI GS ZSM 002 [i.2]). E2E service data collection services include E2E performance data reporting service (refer to clause 6.6.2 of ETSI GS ZSM 002 [i.2]).

In the monitoring stage, the relevant data (e.g. live performance and fault data of managed entities and managed services) is collected following the goals assigned to the Closed Loop. Besides, the sensitive information of Closed Loop (e.g. logs, outcomes derived in each CL stage) is collected for deriving insights of CL in the analysis stage. Since a large amount of sensitive data in different formats and coming from various sources are collected, stored and translated, data privacy is a main concern for (domain or E2E) data collection management services used in the monitoring stage. The confidentiality, integrity and availability of collected data at rest, in transit and in use is defended against potential data security threat and risk, such as data tampering, data leakage, illegal data acquisition, etc.

The security risks and threats of implementation of Closed Loop and Closed-Loop Automation using data collection management services above during monitoring stage are analysed as followed:

- Tamper or leak collected data: Data notifications related to faults, performance and security from the underlying managed entities and consumed managed services are provided in the performance measurements streaming service and performance measurements collection service. Closed-Loop Automation (CLA) uses these feedback information data to create automated processes, if the other managed entities or external attacker without required privilege gain and tamper collected data. On the one hand, the device, system, or network of Closed Loops within the ZSM framework may be unavailable because leak of sensitive information may bring disruption to the infrastructure resources and network. On the other hand, incorrect performance data can affect insights from monitoring data, leading to deviations or inability to achieve the goals of Closed-Loop Automation.

- Tamper log: Logs about system running, operation and security events are collected in the log collection service to enable health, security and performance monitoring of managed entities in the CL. If the logs are tampered with, the attack behaviors cannot be detected in a timely manner. When the logs including abnormal state changes information reported in the monitoring stage, the CLA may take wrong actions based on the tampered log.

- Authentication abuse or bypass: An attacker without authorized access to managed entities steals information about key performance indicators or resources to control the management domains including E2E management services. The attacker can perform the excessive consumption of resources, disrupting the process of CLA and causing the significant deviations or faults of the goal of CLA.

4.2.2 Analysis stage

As described in clause 7.2.1 of ETSI GS ZSM 009-1 [i.3], the analysis stage is responsible for deriving insights from available data from the monitoring stage as well as historical data. It also provides capabilities for tuning the analytics models and starting/terminating the analytics processes. Historical and real-time analytics insights deriving in the analysis stage are provided to the decision stage.

As described in clause 7.3 of ETSI GS ZSM 009-1 [i.3], the analysis stage is realized, fully or in part, by the (domain or E2E) analytics management services from deployment view. Domain analytics management services include analytics services, domain condition detection service and data optimization services (refer to clause 6.5.3 of ETSI GS ZSM 002 [i.2]). E2E service analytics management services include analytics services, E2E service quality management service and E2E service condition detection service (refer to clause 6.6.3 of ETSI GS ZSM 002 [i.2]).

In the analysis stage, domain analytics services provide domain-specific insights and predictions based on data collected by domain data collection services and other data. Since information of insights and predictions (e.g. analysis results, performance evaluation) have a significant impact for the decision stage, integrity and confidentiality of the information should be protected for the analysis stage to ensure the authenticity of information provided by (domain or E2E) data analytics services for the Closed Loop.

The security risks and threats of implementation of Closed Loop and Closed-Loop Automation using domain analytics management services above during analysis stage are analysed as followed:

- Tamper analysis results: Analytics services provide the anomaly detection service capabilities to detect anomalous conditions of CL using the collected fault, performance, usage and configuration data about the managed entity, manage (create, read, update, delete, list) analysis results, and analyse incident patterns and root cause to produce insights. When the abnormal analysis results are tampered with, it causes the managed services that subscribe to message notifications to receive incorrect results. The wrong results cannot trigger domain intelligence in decision stage to make appropriate decisions, causing deviations or faults of the goal of CLA.

- Tamper monitor condition: Domain condition detection service receives a set of conditions which can be defined on a case-by-case basis to be monitored continuously, and manage the conditions associated with a domain service model. The activation or deactivation of detection of conditions is specific to the network service instance and can be done per condition. An adversary tampers monitor condition, which impacts the analytics result in the analysis stage of CL. Besides, abnormal events (e.g. exceeding the threshold of the network resource utilization) cannot be reported to the CL, misleading the CL reaction (e.g. insufficient resources to execute Closed Loop in reality). Even worse, the operation of the entire Closed Loop is affected.

4.2.3 Decision stage

The decision stage which is responsible for deriving workflows from insights provided by the analysis stage, governs the behaviour of the system and decides which actions should be taken in face of issues detected in the analysis stage (refer to clause 7.2.1 of ETSI GS ZSM 009-1 [i.3]). In this stage, it provides action plans in form of workflows to managed entities, tune decision modules according to analysis insights.

As described in clause 7.3 of ETSI GS ZSM 009-1 [i.3], the decision stage is realized, fully or in part, by the (domain or E2E) intelligence management services from deployment view. Domain intelligence management services include AI model management service, deployed AI model assessment service, AI training data management service, knowledge base service and health issue reporting service (refer to clause 6.5.4 of ETSI GS ZSM 002 [i.2]). E2E intelligence management services include AI model management service, deployed AI model assessment service, AI training data management service, E2E health issue reporting service (refer to clause 6.6.4 of ETSI GS ZSM 002 [i.2]).

In the decision stage, intelligence services enable decision supporting, decision making and action planning via training AI models. The confidentiality of the AI model is one main concern for the Closed-Loop Automation. Besides, data security and privacy particularly for training data is another main concern in the decision stage.

The security risk and threats of implementation of Closed Loop and Closed-Loop Automation during the decision stage using (domain or E2E) intelligence management services are analysed as followed:

- AI models stolen: The AI model management service enables to manage AI models, an AI model can be updated on the basis of new input data periodically or at any time. An attacker steals AI models for the Closed-Loop Automation, rebuilds or copies the AI model, discovers the structure, function, and composition of the CL by using a variety of analysis techniques to determine how Closed-Loop Automation was constructed or operated. The vulnerabilities of constructions or operations can be exploited by the adversary to compromise the function and associated systems of the Closed-Loop Automation.

- Tamper evaluation results of AI model: Deployed AI model assessment service provides the result of the AI model assessment process, which is used to decide on the most appropriate actions to perform on the deployed AI model such as retrain, reconfigure, upgrade, replace, pause and terminate. Tampering the evaluation results can affect the operational decisions of AI models, leading to inaccurate matching between the model and reality and deviations in achieving Closed-Loop Automation goals.

- Tamper training data: The decision stage manages the training data used to train AI models. An adversary implants malicious samples or modify the training data that is required to train or re-train the AI models, resulting in incorrect predictions or decisions of the AI model in the future. The model is deviated from the representation of real data, bringing security issues in the deployment and operation of Closed-Loop Automation.

- Leakage of knowledge base: The knowledge base may contain problem causes derived from historical, operational and configurational data, as well as conclusions drawn from analysis of combinations of problem causes. If the information leaked, attackers may exploit information of known problems collected in the knowledge base to attack the process of Closed-Loop Automation, which may lead to the unavailability of associated service and its resources.

4.2.4 Execution stage

The execution stage is responsible for executing workflows towards managed entities within the ZSM framework. Execution occurs when the decision stage determines that an action is required (refer to clause 7.2.1 of ETSI GS ZSM 009-1 [i.3]). In this stage, it executes the workflows towards the managed entities. Optionally, it also provides information about historical and/or more recent actions that have been executed.

As described in clause 7.3 of ETSI GS ZSM 009-1 [i.3], the execution stage is realized, fully or in part, by the domain orchestration and control management services, when the CL is deployed within a management domain. Domain orchestration management services include domain orchestration service, feasibility check service, Managed services catalogue management service, testing service, domain inventory information service, domain inventory management service and domain topology information service (refer to clause 6.5.5 of ETSI GS ZSM 002 [i.2]). Domain control management services include resource configuration management service, resource lifecycle management services and configuration data generation service (refer to clause 6.5.6 of ETSI GS ZSM 002 [i.2]).

As described in clause 7.3 of ETSI GS ZSM 009-1 [i.3], since the E2E management domain does not interact directly with managed resources and thus does not specify Control management services, when the Closed Loop is deployed within the E2E service management domain, the execution stage is realized, fully or in part, by the E2E orchestration management services only. E2E orchestration management services include E2E service orchestration service, feasibility check service, managed services catalogue management service, E2E testing service, E2E services inventory information service, E2E services inventory management service and E2E services topology information service (refer to clause 6.6.5 of ETSI GS ZSM 002 [i.2]).

NOTE 1: The execution stage is realized by one or more management services of (E2E) orchestration management services, which is depending on the preferences and implementation of the ZSM framework owner.

In the execution stage, resource security control becomes a key consideration because the managed resources are used to achieve the goal of Closed Loop in the orchestration and control management services. Some key resource information that involves the entire network (e.g. domain inventory, service models, network topology) in the Closed Loop should be protected.

The security risks and threats of implementation of Closed Loop and Closed-Loop Automation using domain orchestration and control management services above during execution stage are analysed as followed:

- Resource leak exposure: Domain orchestration services consume control services to configure and modify infrastructure resources or consumed services. If resource leak is exposed then it may be exploited by adversary in the execution stage of Closed Loop, it leads to the malicious execution or depletion of infrastructure resources.

- Tamper inventory: The domain inventory includes available infrastructure resources as well as available (instantiated and active) managed services managed by the management domain. Each change to the inventory is triggered as a side effect of a control or orchestration service invocation on the managed entities of the domain. The domain inventory is maliciously tampered with, causing incapability/wrong-capability of the associated resources used in the Closed-Loop Automation.

NOTE 2: As described in clause 6.5.5.2.5 of ETSI GS ZSM 002 [i.2], the information of domain inventory can be provided at different abstraction levels to support different use cases: Information of domain inventory used for end-to-end management is abstract while information used for the domain specific management is more detailed.

- Tamper catalogue: Service models are contained in the catalogue, including sensitive information (e.g. supported coverage areas, supported Service Level Specification (SLS) levels, service templates). Some information of the service models is tampered with or malicious information is inserted into the catalogue, resulting in incorrect data or services used during the Closed Loop execution stage and affecting the inability to achieve the goals of the Closed-Loop Automation.

NOTE 3: As described in clause 6.5.5.2.1 of ETSI GS ZSM 002 [i.2], the domain service model is maintained in the managed services catalogue of the domain. An explicit domain service model may provide a complete description of all necessary infrastructure resources and consumed services, their topology, their configuration, their policies and their location in the network, etc.

- Domain topology information theft and utilization: Domain orchestration services utilize topology information (e.g. resources, resources utilization level, services, physical/virtualized nodes, physical and/or virtual links/network connections) to maintain the network services and virtualized resources managed by the management domain. In a Closed Loop, relevant configuration operations can be updated and performed in the execution stage in a timely manner based on topology information. The topology information is stolen and exploited by an adversary, leading to incorrect resource configuration or execution of incorrect operations managed by the Closed Loop. Further, it brings interruption and unavailability of associated services in the domain.

4.2.5 Composition of Closed Loops

As described in ETSI GS ZSM 009-1 [i.3], CL stage is the logical role to be played while the CL component is the entity identified to play the particular role(s). As described in clause 7.4 of ETSI GS ZSM 009-1 [i.3], two different types of Closed Loops including Made-to-Order Closed Loops (M2O-CL) and Ready-Made Closed Loops (RM-CL) are supported in the ZSM framework. The main differences from these two types of Closed Loops are composition of capabilities. M2O-CLs are assembled on demand by ZSM framework owners, or by other entities on behalf of the ZSM framework owners, using capabilities offered by the ZSM framework. RM-CLs are assembled by ZSM framework vendors prior to their use in the ZSM framework, using capabilities outside of the ZSM framework. The present clause gives security risk analysis for the different types of Closed Loops, outlines their commonalities and differences:

- M2O-CL

As described in the clause 7.4 of ETSI GS ZSM 009-1 [i.3], the ZSM lifecycle scope of M2O-CLs comprises the preparation, commissioning and operation phases. As described in ETSI GS ZSM 009-2 [i.8], it defines the capabilities needed to chain the different components together to prepare a M2O-CL for deployment. Components of M2O-CLs may come from different ZSM framework vendors and can be associated with a CL instance based on demand.

The security risks and threats for the internal and external interactions and capabilities of M2O-CLs should be considered.

The security risks and threats for internal interactions and capabilities of M2O-CLs are analysed as followed:

- Tamper goal of Closed-Loop Automation: A specific CL goal will be defined during the procedure of creation of a CL in the preparation phase. The attacker may attempt to gather and collect the sensitive information of the goal through a variety of methods including active querying and passive observation. By exploiting the weakness in the design or configuration of the target (e.g. managed network, deployed system, applied software), the adversary may directly tamper the goal of Closed-Loop Automation, manipulating and depleting one or more resources of the target in order to achieve a desired outcome.

- Collect and analyse components' information: Some sensitive information about CL components and stages (e.g. CL-component unique names or identifiers, CL-component inputs and outputs and CL-Step capabilities defined in clause 6.3 of ETSI GR ZSM 009-3 [i.9]) are used by a Closed Loop Controller (CLC) to compose M2O-CL. Additionally, data transformation might be required between the stages of M2O-CL to facilitate mapping the output of one stage to the input of subsequent stages. By exploiting weaknesses in the design or configuration of the target and its communications, an adversary is able to get more information than intended from the target, and the information obtained can be used to further infer potential weaknesses and vulnerabilities of components in CLs.

The security risks and threats for the external interactions and capabilities of M2O-CLs can refer to the clause 4.3 of the present document:

- RM-CL

As described in the clause 7.4 of ETSI GS ZSM 009-1 [i.3], RM-CLs are assembled by ZSM framework vendors prior to their use in the ZSM framework, using capabilities outside of the ZSM framework.

The vulnerabilities of RM-CL from outside of the ZSM could be exploited by the adversary to compromise the RM-CL itself, then attack other Closed Loops, finally endanger the whole ZSM framework and/or ZSM consumers.

The security risks and threats analysis for the external interactions and capabilities of the RM-CLs should be considered, which can refer to the clause 4.3 of the present document.

4.2.6 Threat analysis report

The present clause summarizes the security risk analysis on implementation of Closed-Loop Automation mentioned above and provides potential security countermeasures according to CAPEC [i.7] and ETSI GR ZSM 010 [i.1].

Table 4.2.6-1

Threat Id	Threat Cat Id	Adversarial Technique	Consequence of Incident	Potential countermeasure
Monitoring stage				
D8.3	D8	Authentication Abuse or bypass	Steal information and manipulate the system, cause excessive consumption of resources, disrupt the process of CLA, and cause the significant deviations or faults of the goal of CLA.	Apply software vulnerability validation, strong authentication
D9.1	D9	Tamper log	The attack behaviors cannot be detected in a timely manner. The CLA cannot take corrective actions without receiving the abnormal state changes information.	Data classification and labelling, integrity protection and strict access control
D9.3	D9	Tamper or leak collected data	Cause unavailability of the device, system, or network of Closed Loops within the ZSM framework and affect insights of analysis stage through tampered data	Data integrity protection and strict access control

Threat Id	Threat Cat Id	Adversarial Technique	Consequence of Incident	Potential countermeasure
Analysis stage				
D9.1	D9	Tamper monitor condition	Impact the analytics result, and mislead the CL reaction (e.g. insufficient resources to execute Closed Loop in reality).	Data integrity protection and strict access control
D9.3	D9	Tamper analysis results	The wrong analysis results cannot trigger domain intelligence in decision stage to make appropriate decisions, causing deviations or faults of the goal of CLA.	Data integrity protection and strict access control
Decision stage				
D7.1	D7	Leakage of knowledge base	Disrupt the process of CLA through known problem collected in the knowledge base or cause the unavailability of associated service and its resources of CLA.	Data encryption and access control
D9.3	D9	Tamper evaluation results of AI model	Affect the operational decisions of AI models (e.g. retrain, reconfigure, upgrade, replace, pause, terminate), and lead to inaccurate matching between the model and reality.	Data integrity protection and strict access control
D9.6	D9	Tamper training data	Incorrect predictions of the AI model through tampered training data.	Data integrity protection and strict access control
D9.7	D9	AI models stolen	Compromise the function and associated systems	Employ code obfuscation, encryption and access control on the target module
Execution stage				
D2.6	D2	Resource leak exposure	Malicious execution, resource depletion of infrastructure resources through leak until the target is reset, therefore reduce the resources available for legitimate services and degrading or denying services.	Apply software vulnerability validation
D7.1	D7	Domain topology information theft and utilization	Cause interruption and unavailability of associated services in the domain through topology information.	Data integrity protection and strict access control
D9.6	D9	Tamper catalogue	Affect the inability to achieve the goals of the Closed Loop through incorrect data or services automation.	Validate the authenticity and integrity of the service profile/descripted during service deployment/update, etc. Employ strong access control
D9.9	D9	Tamper inventory	Cause incapability/wrong-capability of the associated resources used in the Closed-Loop Automation	Employ strong access control
M2O-CL				
D7.4	D7	Collect and analyse components' information	The adversary is able to obtain information from the target that aids the attacker in making inferences about its security, configuration, or potential vulnerabilities	Data classification and access control, apply UEBA (see note).
D9.1	D9	Tamper goal of Closed-Loop Automation	Manipulating and depleting one or more resources of the target in order to achieve a desired outcome.	Data integrity protection and strict access control

NOTE: According to the definition from Gartner, User and Entity Behavior Analytics (UEBA) refers to providing profiling and anomaly detection based on various analysis methods, usually basic analysis methods (using signature rules, pattern matching, simple statistics, thresholds, etc.) and advanced analysis methods (supervised and unsupervised machine learning, etc.), using packaged analysis to evaluate users and other entities (hosts, applications, networks, databases, etc.), and discover potential events related to activities that are abnormal to user or entity standard profiling or behavior. The detection objects include abnormal access to the system by trusted internal or third-party personnel (user anomalies), or intrusion by external attackers bypassing security control measures (abnormal users).

4.3 Threats and risk analysis on coordination/governance of Closed-Loop Automation

4.3.1 Coordination between hierarchical Closed Loops

As described in clause 8.2.3 of ETSI GS ZSM 009-1 [i.3], hierarchical relationship is the case when one Closed Loop is authorized to control another Closed Loop regarding a defined set of aspects. The subordinate CLs are responsible for optimization and self-healing within their scope, while the superior CLs are responsible for the coordination and optimization within their scope. The subordinate CLs deployed in the E2ES MDs or in the MDs perform local optimizations which might not result in a global, end-to-end optimum or which might even be in conflict to each other. To this end the superior CLs can be able to coordinate the decisions of subordinate CLs. As described in clause 8.2.3 of ETSI GS ZSM 009-1 [i.3], two typical approaches of coordination between hierarchical Closed Loops are supported by ZSM framework, including Delegation and Escalation.

NOTE: As described in clause 8.2.3 of ETSI GS ZSM 009-1 [i.3], Delegation means that the superior CLs delegates respective goal(s) to the subordinate CLs, e.g. by setting the policies and/or the intents in a way that allow the subordinate CL to act autonomously. Escalation means that if a subordinate CL is not able to achieve the goal(s) assigned to it, it escalates the situation to the superior CL in the E2ES MD.

The confidentiality, integrity and availability of the important and sensitive data (e.g. interaction information, CL instance attribute details, CL action plan) between superior CLs and subordinate CLs should be protected against the security threats and risks to guarantee the accuracy and timeliness of information received from another CL, especially important in the hierarchical Closed Loop when controlling subordinate CLs (refer to the clause 8.2.2 of ETSI GS ZSM 009-1 [i.3]).

As described in clause 8.2.5 of ETSI GS ZSM 009-1 [i.3], Closed Loop Coordination (CLC) is a set of capabilities that allows multiple CLs running within the ZSM framework to be coordinated, with the main objective of improving their performance and the fulfilment of their goal(s).

In the present clause, the security threats and risks are analysed following the exemplary timeline describing the typical occurrence time (refer to the Figure 4.3.1-1).

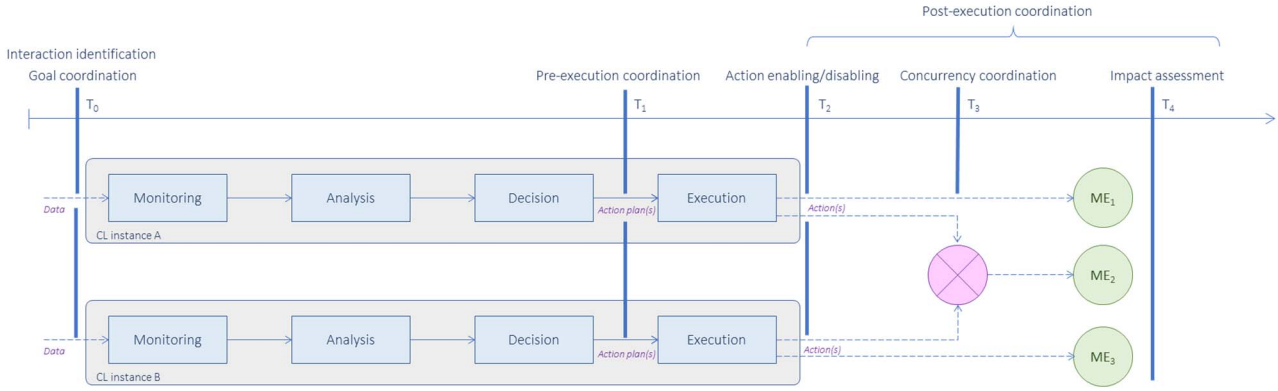

Figure 4.3.1-1: Exemplary Closed Loop Coordination timeline (Source: ETSI GS ZSM 009-1 [i.3])

Before time T0 in Figure 4.3.1-1, SLA/SLS may be translated to Closed-Loop Automation goals, then a specific CL goal will be defined during the procedure of creation of a CL in the preparation phase in the respective MDs according to the translated goals. Security threats and risks are analysed as followed:

- Tamper goal of Closed-Loop Automation: An adversary tampers changing the values of the parameters of the goal (e.g. closedLoopGoal) that is currently in use of the superior CL and the subordinate CL, it will result in the entire Closed-Loop Automation not achieving the original goal. The attacker may attempt to gather and collect the sensitive information of the goal through a variety of methods including active querying and passive observation. By exploiting the weakness in the design or configuration of the target (e.g. managed network, deployed system, applied software), the attacker may directly tamper the goal of Closed-Loop Automation, manipulating and depleting one or more resources of the target in order to achieve a desired outcome. As described in [i.10], a CL example shows a legitimate scenario where a fault event collected by the domain data collection services triggers the CL process by publishing the fault event, which will be consumed by the domain intelligence services. Then the domain intelligence services determine that the link is bad and requests the domain control services to change the router configuration to reroute the traffic on managed resources. An attacker may launch a deception attack and send a fake fault event to the domain data collection services, misleading the domain intelligence services and the domain orchestration services to decide and execute the wrong operation on the managed resources (e.g. scale the network resources or to instantiate new resources to handle the increased load). In this scenario, more resources will be allocated to solve this fake fault event, which can lead to exhaustion of infrastructure resources (e.g. DoS).

At time T0 in Figure 4.3.1-1, designed instances of the CLs are instantiated based on the specific CL goal. (E2E) Closed Loop Governance Service Producer (CLGSP) described in clause 9.2.2 in ETSI GS ZSM 009-1 [i.3] translates the goal into a list of "translated goals" or conditions configurable in the various composing MDs, and check all goals for feasibility prior to configuration in the MD. When new Closed Loops are instantiated, Closed Loops interactions identification determines and characterizes the interactions (e.g. information about the coordination between CL instances and details on CL instance attributes involved in the interactions) that may exist between the superior CL instance and the subordinate CLs (refer to clause 8.2.5.2 of ETSI GS ZSM 009-1 [i.3]). Security threats and risks are analysed as followed:

- Tamper management data: An adversary (internal attacker and external attacker) tampers management data (e.g. event, measurement, KPI, configuration file, log) of the superior CL, or the subordinate CL or both to change the behavior or reaction of the system.

- Illegal Interception: An adversary monitors and gathers the interactions streams to or from the superior CL services or the subordinate CL services for information gathering purposes, causing leak of sensitive information (e.g. the health status of the CL, the values of CL attribute(s), the status of goal fulfilment related to managed (created, updated) CL goals in the past) defined in clause 9.2.3 of ETSI GS ZSM 009-1 [i.3].

- Privilege Abuse: If access control mechanisms are missed or misconfigured for managed entity, an adversary (internal user without required privilege or external attacker) may get access to sensitive interactions information or functionality between the superior CL and the subordinate CL.

At time T1 in Figure 4.3.1-1, the pre-execution coordination service is used to configure control information (e.g. parameter for conflict detection, subscriptions to notifications) to detect conflicting action plans provided by multiple Closed Loops in the decision stage and select the most appropriate combination of action plans according to the evaluation (refer to clause 9.3.2 of ETSI GS ZSM 009-1 [i.3]). As shown in the Figure 4.3.1-1, the superior CL may need to retrieve the action plans from the subordinate CLs, check if there are any conflicting actions based on the information of action plans, and select non-conflicting action plans in the subordinate CLs. Security threats and risks are analysed as followed:

- Identity Spoofing: An attacker may attempt to forge the identity of the superior CL through knowledge of the inherent weaknesses of an authentication mechanism, and steals action plans of the subordinate CLs, causing the leakage of sensitive information (e.g. resource and asset used in the CL, service data). In addition, the adversary may use stolen information to launch attacks on infrastructure resources and managed services, disrupting the progress of Closed-Loop Automation.

- Content Spoofing: An adversary may intend to modify the content (e.g. action plans, transmitted data) at the source (e.g. modifying the source file for a web page) or in transit (e.g. intercepting and modifying a message between the sender and recipient), leading to false feedback, privacy violations, and other unwanted outcomes.

- Resource Location Spoofing: By spoofing the resource location of the Closed Loop, the adversary can cause an alternate resource to be used in the Closed-Loop Automation, often one that the adversary controls and can be used to help them achieve their malicious goals. For example, when a specific Management Domain (say MD-A) copes with the increase of demands e.g. a sudden increase of traffic or loads on managed entities, subordinate CLs in MD-A take action and report information (e.g. results of action taken by the CL in MD-A) to superior CLs in E2E service MD. In such cases, to mitigate the impact caused by the event, CLs in E2E service MD delegates roles (e.g. of Analytics or Decision) to lower CLs in other MDs (say MD-B). If receiving incorrect resource location information of the managed entities spoofed by the adversary, the lower CLs will perform wrong action over the managed entities, causing serious interruption for the E2E service.

At time T2 in Figure 4.3.1-1, action enabling or disabling typically occurs at this time. Coordination amongst Closed Loops may require disabling actions (actions are changes that a Closed Loop can perform over a managed entity such as configuring an attribute) of a Closed Loop (refer to clause 8.2.5.5.2 of ETSI GS ZSM 009-1 [i.3]). The Closed Loops execution management service provides the ability to pause the execution of a Closed Loop at a pause point which is defined during procedure of design in the preparation phase. In the case of the hierarchical Closed Loops, the pause/resume message sent by an authorized consumer may carry an instruction of what the subordinate CLs should be done upon the action of the superior CL. Security threats and risks are analysed as followed:

- Tamper message related data: Attackers impersonate authorized consumer identities or use man-in-the-middle attack to release or alter the pause/resume message. The pause/resume messages carry an instruction of what the subordinate CLs should do upon the action of the superior CL. If attacker tampers the messages, wrong information may result in an undesired operation on the superior CL and subordinate CLs.

At time T3 in Figure 4.3.1-1, concurrency coordination service ensures that the actions of CL instances that have managed entities in common are applied consistently and in accordance with the operational policies, rules, or decision criteria (refer to clause 8.2.5.5.3 of ETSI GS ZSM 009-1 [i.3]). As described in clause 5.3.2 of ETSI GS ZSM 009-2 [i.8]), some stored knowledge (e.g. configuration data, operational data, and historical data) of Closed Loops can be shared between the superior CL in E2E management domain and the subordinate CLs in management domain to enhance the functioning of Closed Loops across management domains. When an anomalous state (e.g. shutdown for maintenance of the specific management domain) is detected in the subordinate MD, the change is notified to the E2E management domain. Superior MD analyses the anomalous state and delegates a new MD to take over the responsibilities of the subordinate MD based on evaluating knowledge data of CL in the subordinate MD and from other MDs. Security threats and risks are analysed as followed:

- Shared Data Manipulation: The superior management domain may choose to share some knowledge data to help the subordinate MD accelerate the convergence speed of models/algorithms or enhance the accuracy of deriving insight and making decision when managing part of its service (refer to clause 5.3.2.2.1 of ETSI GS ZSM 009-2 [i.8]). An adversary exploits shared knowledge data of CL to affect normal operation of management service in the domain.

- Leakage of knowledge data: An adversary may attempt to collect the knowledge data (e.g. models/algorithms for insight derivation, list of root causes and the recommended solutions) shared during the transmission between different Closed Loops which can disturb the entire automation process of Closed Loops.

- Exploitation of Trusted Credentials/Identifiers: When the superior CL in E2E management domain shares the knowledge data from one subordinate CL1 in MD1 with a new subordinate CL2 in MD2 (refer to the clause 5.3.2 of ETSI GS ZSM 009-2 [i.8]), if an adversary attempts to attack the trusted credentials/identifiers (e.g. session ID, resource ID, cookie) during transmission, malicious actions can be performed to allow the adversary to obtain sensitive data, download/install malware on the system and pose as a legitimate user for social engineering purposes, and more, leading to an attacker's ability to break authentication, authorization, and audit controls on the system.

4.3.2 Coordination between peer Closed Loops

As described in clause 8.2.4 of ETSI GS ZSM 009-1 [i.3], peer Closed Loops in the E2ES MD or in MDs may benefit from exchanging information to cooperate in achieving a common objective. The peer CLs may perform local operations which might be in conflict to each other. Cooperation is a typical approach of coordination between peer Closed Loops which is supported by ZSM framework, which may be based on capabilities provided by the Closed Loop Governance service and the Closed Loop information reporting service (defined in ETSI GS ZSM 009-1 [i.3]). As described in clause 9.2.2 of ETSI GS ZSM 009-1 [i.3], a CL can request a peer CL to assist in the resolution of an issue, which is provided by Closed Loop Governance (CLG) service in each management domain, to solve an issue which a Closed Loop is not able to solve.

The confidentiality of sensitive data (e.g. Identity and Access Management (IAM) related data, tenant information, configuration and performance data related to the CL), integrity and availability of data (e.g. policy/intent specification, parameter tuning, action plans, actions in CL flows, system logs, outcomes derived in each CL stage, their goals, their models and their information, etc.) exchanged between peer CLs should be protected against the security threats and risks to guarantee peer CLs adjust their own policies and/or intents to achieve a common objective.

Compared with the security risks on coordination between hierarchical Closed Loops, analysis for the security risks on coordination between peer Closed Loops are more focused on the inter-influence between the Closed Loops. An attacker can launch an attack on one Closed Loop, causing it to malfunction. In turn, this can affect the normal operation of another Closed Loop. In addition, some security risks can be introduced into one Closed Loop that are then transmitted to another, affecting both simultaneously. These situations may all result in the failure to achieve the common objectives. It is a challenge to cooperate and implement security protection and measures against the security risks since peer Closed Loops exist independently and one Closed Loop is not responsible for the other, especially across different management domains.

In the present clause, the security threats and risks on coordination between peer Closed Loops are analysed as followed:

- Collect and analyse information: As described in clause 6.2.1 of ETSI GR ZSM 009-3 [i.9], CLs belonging to the same use case with a common goal may be composed as a group of interdependent (nested) CLs. Some CLs may coordinate themselves in a peer manner to detect and mitigate conflicting actions. Some sensitive information (e.g. individual goal of the CL, the predicted decision/action, accuracy/confidence of the prediction defined in ETSI GR ZSM 009-3 [i.9], Table 6.2.3-1) on the derived insights & workflows from the Decision stage of one CL are fed as an input to the Analytics stage of next (or all) lower or higher CLs. An attacker may collect the information through active querying and passive observation. By exploiting weaknesses in the design or configuration of the target and its communications, an adversary is able to get the target to reveal more information than intended. Information retrieved may aid the adversary in making inferences about potential weaknesses, vulnerabilities, or techniques that assist the adversary's objectives.

- Shared Data Manipulation: As described in clause 5.3.2 of ETSI GS ZSM 009-2 [i.8], some stored knowledge data (e.g. configuration data, operational data, and historical data) are shared during the transmission between peer Closed Loops. An adversary exploits shared knowledge data of peer Closed Loops to affect normal operation of management service in the management domain or disturb the entire automation process of peer Closed Loops.

- Identity Spoofing: An attacker may attempt to forge the identity of one peer CL through knowledge of the inherent weaknesses of an authentication mechanism, and steals action plans of the other CL, causing the leakage of sensitive information (e.g. resource and asset used in the CL, service data). In addition, the adversary may use stolen information to launch attacks on infrastructure resources and managed services, disrupting the progress of Closed-Loop Automation.

- Illegal Interception: An adversary monitors and gathers the interactions streams between peer Closed Loops for information gathering purposes, causing leak of sensitive information (e.g. the health status of the CL, the values of CL attribute(s), the status of goal fulfilment related to managed (created, updated) CL goals in the past) defined in clause 9.2.3 of ETSI GS ZSM 009-1 [i.3].

- Tamper data during transmission: An attacker may intercept and tamper with the sensitive information between peer Closed Loops, resulting in the conflicts between goals of peer Closed Loops, or causing the peer Closed Loops unable to adjust their own policies or intents in a timely manner.

4.3.3 Interaction between Closed Loops and external entities

4.3.3.1 Introduction

As defined in clause 8.1.1 of ETSI GS ZSM 009-1 [i.3], the external entities can manage the life cycle of CLs and configure their behaviour through Closed Loop Governance (CLG). CLs within management domains can be controlled by internal or external governance.

When internal/external governance is applied, the confidentiality, integrity and availability of the sensitive information (e.g. status, performance, polices, intents) between CLs and external entities should be protected against the security threats and risks to ensure the whole operation of Closed-Loop Automation runs normally.

In addition, according to ETSI GS ZSM 002 [i.2], management services with optional or conditional external visibility may not expose their capabilities to consumers located outside the management domain where the management service is produced. The CLs need to guarantee the external exposure of management services across management domains, which is controlled by the Management capability exposure configuration of ZSM framework integration fabric. When external governance is applied, the exposure entitlements of CL's management services may change dynamically (refer to clause 6.3.2.5 of ETSI GS ZSM 002 [i.2]), if the configurations cannot dynamically adapt to such changes, it may cause inappropriate external visibility of the management services.

As described in clause 8.1.5 of ETSI GS ZSM 009-1 [i.3], an external entity may interact directly with a CL or indirectly, via other CLs. The external entity is external to the CL, but could be a part of ZSM framework (e.g. human operator, external management system). Two types of interactions between Closed Loops and external entities are supported in the ZSM framework, including Interactions based on policies and Interactions based on intents. The present clause analyses the security threats and risks for these two types of interaction as followed.

4.3.3.2 Interactions based on policies

As defined in ETSI GS ZSM 009-1 [i.3], a policy defines a set of actions that an external entity requires a CL to perform when a given set of conditions are met. Two basic types of policy should be supported, resource policy and service policy (refer to clause 8.1.5.2 of ETSI GS ZSM 009-1 [i.3]), specifying a behavioural pattern that a CL should follow. Security threats and risks analysis for interactions based on policies between Closed Loops and external entities are analysed as followed:

- Tamper policies: As described in clause 7.2.1 of ETSI GS ZSM 009-1 [i.3], interactions at each stage of the CL lifecycle (monitoring, analysis, decision and execution) between CLs and external entities are conveyed through policy/intent specification. If an attacker tampers policy, it can lead to unexpected behavior or results of CL operation according to the incorrect policy, such as wrong allocation of resources or improperly set characteristics and control the externally observable behaviour of services and service instances, acted on by the CL.

- Identity Spoofing: If an adversary steals identity information and impersonates the identity of an authorized external entity, the adversary can obtain the sensitive resources or capabilities exposed from service management service to damage infrastructure resources and service producer or consumer in the (E2E) management domain, affecting the normal operation of the Closed Loop.

- Authentication Abuse or bypass: As described in clause 5.4 of ETSI GR ZSM 010 [i.1], potential authentication/authorization administration services and audit service are provided by integration fabric to support access control. If unauthorized/unauthenticated external entity exploits a flaw or weaknesses of authentication/ authorization mechanism to obtains access to management services in the CL, the adversary may steal sensitive information and manipulate the CL operation.

4.3.3.3 Interactions based on intents

As defined in clause 8.1.5.3 of ETSI GS ZSM 009-1 [i.3], an intent specifies wanted characteristics or behavior of a managed object or of a system composed of several managed objects. Intent may be an abstracted way to specify business or operational desired state of a system, without specifying how to achieve it. As described in ETSI GR ZSM 011 [i.11], the management domains may contain Intent Management Entities (IME), which can play the role of intent owner and/or intent handler and is capable of making and actuating decisions to fulfill intents. A Closed Loop could be implemented within an IME to execute the intent fulfilment. Security threats and risks analysis for interactions based on intents between Closed Loops and external entities are analysed as followed:

- Communication channel manipulation: An adversary manipulates a setting or parameter on communications channel in order to compromise its security. This can result in information exposure, insertion/removal of information from the communications stream, and/or potentially system compromise. For example, intents can vehicle information about the desires of the application such as connecting with peers, advertising services or content, and regulating network traffic. Thus, intercepting such information by an unauthorized entity can result in information exposure, compromise system security objectives (e.g. privacy, confidentiality) and launch of other attacks.

NOTE: As described in the clause 7.2.2.4 of ETSI GS ZSM 009-1 [i.3], "Setting" which is used for interactions between different CLs and between CLs and external entities in the customization flow may refer to, e.g. attributes of CL models, configurations that define how each CL stage works, etc. As described in the clause 8.1.3.4 of ETSI GS ZSM 009-1 [i.3], "Parameter" in the update & upgrade activity may refer to, e.g. changing data sources, KPIs being calculated, models, policies.

- Malformed intent: An unauthorized IME handler exploits and manipulates parameters of the accepted intent (e.g. bandwidth, latency defined in the clause 4.3.3.2 of ETSI GR ZSM 011 [i.11]) shared between multiple management domains to affect application behavior. A malformed intent sent to IME may result in an abnormal behavior of the domain orchestration service during the intent rendering. For instance, the domain orchestration service may be aborted or rebooted, leading to Denial of Service (DoS).

- Tamper intents: As described in Annex C of ETSI GR ZSM 011 [i.11], in an intent-based autonomous networks, intent owner (e.g. operators, vendors and users) specifies one or more intents stating what they want in terms of service features or "outcomes" generally. The IME can execute actions using CLs to handle the network resources to fulfil the requirements expressed by the intents (refer to clause 4.1.1 of ETSI GS ZSM 016 [i.12]). IMEs interact with the specific logic within a (E2E) management domain to translate an intent into detailed technical configurations. If an attacker impersonates the identity of intent owner and tampers the intent maliciously, it may result in insecure configurations being implemented on the managed resources or services. For example, a high level of security is mapped to a service chaining of a firewall, a DPI, and IPS VNFs. Meanwhile, a low level of security is translated to instantiation of only a firewall VNF. An intent expressed by intent-based service model (refer to the Annex D, clause D.4 of the ETSI GR ZSM 011 [i.11]) is sent to IME: "HTTP traffic from slice X to Internet has a high security level". Thus, if an attacker maliciously tampers the intent by changing the security level from "high" to "low", an undesirable security level will be set to slice X, making the slice vulnerable to security threats.

- API manipulation: As described in clause 5.2 of ETSI GR ZSM 011 [i.11], intent owner communicates the service intent via an Intent API to an intent handler. An adversary manipulates the use or processing of the API, resulting in an adverse impact upon the security of IME, such as unauthorized access to service and resource composed by CL, data disclosure, data loss or manipulation.

- Manipulate intent to make conflict: If an adversary deliberately tampers one or more intents to make the conflict (syntax-level conflict, action-level conflict and impact-level conflict described in clause 5.7.2 of ETSI GR ZSM 011 [i.11]) between other intents, resulting in an unintended and potentially harmful outcome for the network operation. Conflicts may arise within the context of a single Closed Loop or from the concurrent actions of more than one such Closed Loop.

4.3.4 Threat analysis report

The present clause summarizes the security risk analysis on coordination/governance of Closed-Loop Automation mentioned above and provides potential security countermeasures according to CAPEC [i.7] and ETSI GR ZSM 010 [i.1].

Table 4.3.4-1

Threat Id	Threat Cat Id	Adversarial Technique	Consequence of Incident	Potential countermeasure
Coordination between hierarchical Closed Loops				
D9.3	D9	Tamper goal of Closed-Loop Automation	The attacker tampers the goal of Closed-Loop Automation, manipulating and depleting one or more resources of the target	Data integrity protection and strict access control
D9.1	D9	Tamper management data	Cause disruption or loss of service, and prevent efficient reaction in case of exception in incident	Data integrity protection and strict access control
D7.1	D7	Illegal Interception	An adversary monitors and gathers the interactions streams to or from the superior CL services or the subordinate CL services for information gathering purposes, causing leak of sensitive information	Data encryption and access control

Threat Id	Threat Cat Id	Adversarial Technique	Consequence of Incident	Potential countermeasure
D8.4	D8	Privilege Abuse	Impact the analytics result, and mislead the CL reaction (e.g. insufficient resources to execute Closed Loop in reality)	Strong access control mechanism and policies, enforce configuration compliance
D1.2	D1	Identity Spoofing	An attacker may attempt to forge the identity of the superior CL through knowledge of the inherent weaknesses of an authentication mechanism, and steals action plans of the subordinate CLs, causing the leakage of sensitive information	Build adaptive trust model, adopt User and Entity Behavior Analytics (UEBA) to prevent potential APT, employ robust authentication processes (e.g. multi-factor authentication)
D1.1	D1	Content Spoofing	Causing malware exposure, financial fraud (if the content governs financial transactions), privacy violations, and other unwanted outcomes	Build adaptive trust model, adopt User and Entity Behavior Analytics (UEBA) to prevent potential APT, employ robust authentication processes (e.g. multi-factor authentication)
D1.3	D1	Resource Location Spoofing	Control alternative resource to achieve their malicious goals	Build adaptive trust model, adopt User and Entity Behavior Analytics (UEBA) to prevent potential APT, employ robust authentication processes (e.g. multi-factor authentication)
D9.1	D9	Tamper message related data	Cause disruption or loss of service, and prevent efficient reaction in case of exception in incident	Data integrity protection and strict access control
D3.2	D3	Shared Data Manipulation	An adversary exploits shared knowledge data of CL, affect normal operation of management service in the domain.	Apply software vulnerability validation. Data classify, label and isolation
R4		Leakage of knowledge data	Leak sensitive information of the Closed-Loop Automation	Data leak protection. Data classification, labelling and isolation
D8.1	D8	Exploitation of Trusted Credentials/Identifiers	Malicious actions can be performed to allow the adversary to obtain sensitive data, download/install malware on the system and pose as a legitimate user for social engineering purposes, and more, leading to an attacker's ability to break authentication, authorization, and audit controls on the system	Best practice suggested by Open Web Application Security Project (OWASP) should be adopted
Coordination between peer Closed Loops				
D7.4	D7	Collect and analyse information	The attacker tampers the goal of Closed-Loop Automation, manipulating and depleting one or more resources of the target	Data classification and access control, apply UEBA
D3.2	D3	Shared Data Manipulation	Affect normal operation of management service in the management domain or disturb the entire automation process of peer Closed Loops	Apply software vulnerability validation. Data classify, label and isolation
D1.2	D1	Identity Spoofing	Cause leakage of sensitive information, launch attacks on infrastructure resources and managed services, disrupt the progress of Closed-Loop Automation	Build adaptive trust model, adopt User and Entity Behavior Analytics (UEBA) to prevent potential APT, employ robust authentication processes (e.g. multi-factor authentication)
D7.1	D7	Illegal Interception	Leak of sensitive information	Data encryption and access control
D9.4	D9	Tamper data during transmission	Cause the conflict between the goals of Closed Loops or adjust untimely	Strong mutual authentication, integrity protect during data transfer

Threat Id	Threat Cat Id	Adversarial Technique	Consequence of Incident	Potential countermeasure
Interaction between Closed Loops and external entities				
Interactions based on policies				
D9.11	D9	Tamper policies	An attacker undermines the integrity of policy, cause the policy is not implemented correctly， lead to unexpected behavior or results of CL operation	Data integrity protection and strict access control
D1.1	D1	Spoofing	An adversary steals identity information and impersonates the identity of an authorized external entity, service management service was deceived to expose sensitive resource or capability， attacker use the information to damage infrastructure resources and service producer or consumer	Build adaptive trust model, adopt User and Entity Behavior Analytics (UEBA) to prevent potential APT, employ robust authentication processes
D8.3	D8	Authentication Abuse or bypass	Unauthorized external entity exploits a flaw or weaknesses of authentication mechanism in the authentication of CL, steals information and manipulates the CL operation	Apply software vulnerability validation, strong authentication
Interactions based on intents				
D2.7	D2	Communication channel manipulation	This can result in information exposure, insertion/removal of information from the communications stream, and/or potentially system compromise	Correctly configure the security service, and capable to integrate with existing Authentication, Authorization and Account/Audit (AAA) system
D3.2	D3	Malformed intent	This can result in invalid trust assumptions, corruption or stolen of additional data through the normal operations of the other users of the shared data, or even cause a crash or compromise of the sharing applications	Apply software vulnerability validation. Data classify, label and isolation, monitor and detect abnormal behaviours
D9.3	D9	Tamper intents	An attacker impersonates the identity of intent owner and tampers the intent maliciously, insecure policies being implemented and configurated on the managed resource or service	Data integrity protection and strict access
D2.4	D2	API manipulation	An adversary manipulates the use or processing of the API, resulting in an adverse impact upon the security of Intent Management Entities (IME)	Best practice suggested by Open Web Application Security Project (OWASP) and OWASP API should be adopted
D3.2	D3	Manipulate intent to make conflict	This can result in waste and unavailability of system resources, disruption of service and performance degradation.	Apply strict access control

5 Potential security solutions

5.1 Closed Loop trust management for coordination between Closed Loops

5.1.1 Issue description

According to the security threat and risk analysis in clauses 4.3.1 and 4.3.2 (e.g. D1.1, D1.2, D1.3, D3.2), frequent interaction and dynamic changes between Closed Loops across different management domains introduced new challenges to make trust evaluation for the CL within the ZSM framework.

For the hierarchical coordination between Closed Loops in resource constrained environments as a use case (refer to the Figure 6.5-1 of ETSI GR ZSM 009-3 [i.9]), the central CL and the remote CL generate diverse trust-related metrics (e.g. performance KPIs, security logs, behavioral patterns), but these metrics vary in format, granularity, and relevance across management domains, complicating unified trust evaluation. Trust policies and assurance levels differ between management domains, leading to potential conflicts when these two CLs interact or share data. In addition, the trust level of CL can change from time to time as the change in CL behaviors (e.g. configuration of policies, rules, triggers and priorities for the Closed Loops), the change of environmental conditions (e.g. cyberattacks comes from the remote/edge location which has constrained resources to deploy security functions such as firewall and anti-DDoS), the change of SLA violations (e.g. degraded security assurance because of unexpected limitation of central-remote framework). A compromised CL in one domain could propagate malicious actions to peer or subordinate CLs in another management domain if trust evaluation fails to detect anomalies in real time. The trust evaluation for the CL is essential to ZSM framework to deliver corresponding capabilities to ensure CLs act reliably, securely, and in compliance with policies in the framework.

NOTE: In ZSM context, trust relationship between Closed Loops is a belief that a Closed Loop meets certain expectations and can, therefore, be relied upon. A trustworthy Closed Loop requires sufficient evidence (in other words, it refers to trust-related metrics mentioned in the present document) to support its trustworthiness claims (refer to NIST SP 800-160v1r1 [i.13] Engineering Trustworthy Secure Systems). The trust level of CL can be characterized and established based on specific Levels of Assurance (LoA) defined in the clause 5 of ETSI GR NFV-SEC 007 [i.14] according to the nature of the requested service, the threats being considered, and the applicable policies at all levels, from legal requirements to commercial SLAs.

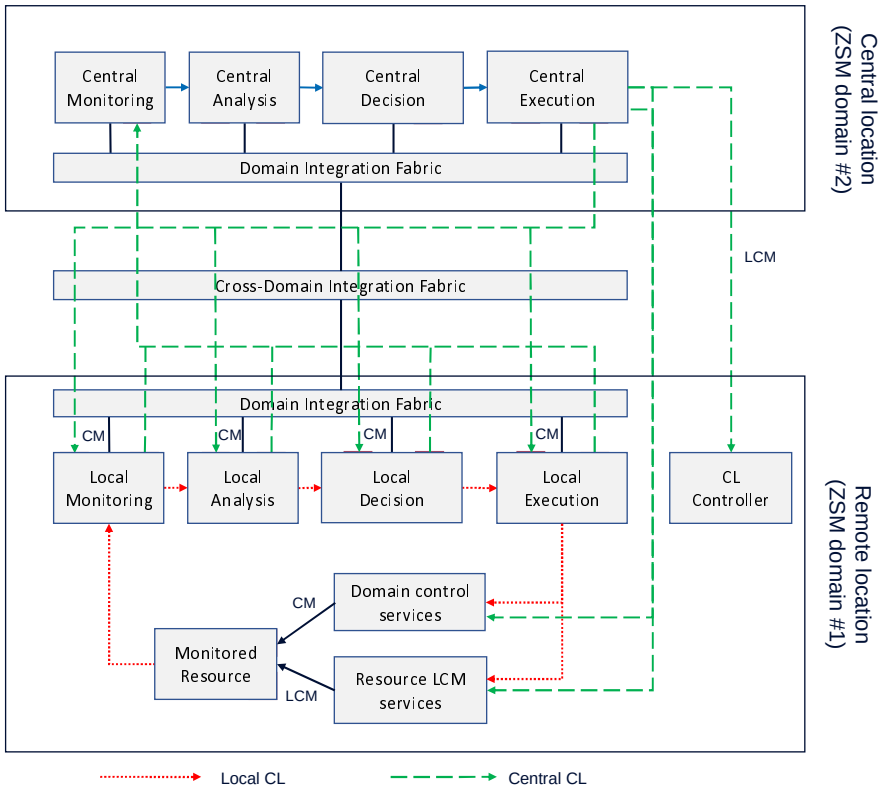

Figure 5.1.1-1: Hierarchical Closed Loop architecture (Source: ETSI GR ZSM 009-3 [i.9])

5.1.2 Potential proposed solutions

5.1.2.1 High Level description of the proposed solution

Dynamic Closed Loop trust model is proposed as a possible solution to establish trust relationship between CLs across different management domains. Both subordinate Closed Loops or peer Closed Loops need to be evaluated by trust-related metrics collected by the four stages (Monitoring, Analysis, Decision and Execution) in the Closed-Loop Automation within the ZSM framework. Then the superior Closed Loop as an external CL supervision can select the appropriate subordinate Closed Loops based on the trust level of this subordinate Closed Loop or peer Closed Loop to coordinate to fulfill the goal efficiently.

5.1.2.2 Procedures of the proposed solution

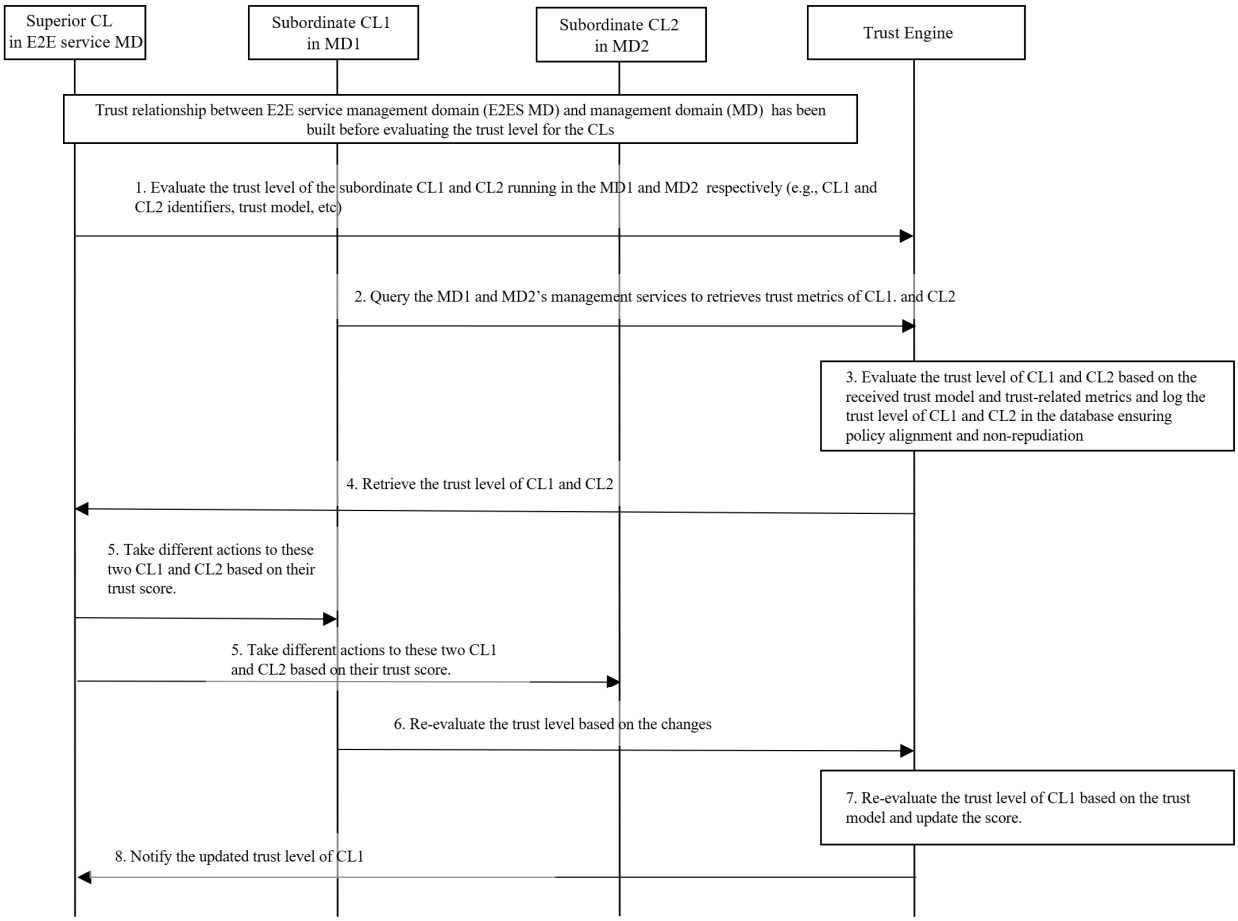

Figure 5.1.2.2-1: Evaluate the trust level of CLs between management domains

Pre-condition:

- Trust relationship between E2E service management domain (E2ES MD) and management domain (MD) has been built before evaluating the trust level for the CL based on the trust model (which can be based on trust management services defined in clause 5.1 of ETSI GS ZSM 014 [i.15]).

NOTE 1: The superior CL in the E2E management domain needs to be authorized to request trust evaluation for the subordinate CL in another management domain.

NOTE 2: Refer to the definition of ETSI GR ZSM 010 [i.1], trust model describes ways in which organizations can obtain the levels of trust needed to form partnerships, collaborate with other organizations, share information, or receive information.

- An E2E Service is deployed in the E2ES MD with a set of Closed Loops deployed within the same management domain or different management domains. It is assumed that Closed Loops CL1 and CL2 are respectively running within each management domain MD1 and MD2.

Steps:

1. When the superior CL may detect a potential SLA violation (e.g. latency spike in MD1) during the procedure to fulfill the target, the superior CL in the E2E service management domain sends trust evaluation requests (e.g. CL1 and CL2 identifiers, trust evaluation model, etc.) to evaluate the trust level of the subordinate CL1 and CL2 running in the MD1 and MD2 respectively to the Trust Engine.

NOTE 3: The Trust Engine is an entity to provide trust evaluation based on the trust model to build trust relationship between Closed Loops, which can be connected with the Trust Management Services defined in Clause 5.1 of ETSI GS ZSM 014 [i.15].

2. The Trust Engine queries the MD1 and MD2 management services (e.g. Trustworthiness evidence collection service defined in the clause 5.1. 2.1 of ETSI GS ZSM 014 [i.15]) to retrieve trust-related metrics of CL1 and CL2.

3. The Trust Engine evaluates the trust level of CL1 and CL2 based on the received trust evaluation model and trust-related metrics. Then it logs the trust level of CL1 and CL2 in the database ensuring policy alignment and non-repudiation (e.g. using permitted blockchain ledger to support the policy alignment and using digital signatures to sign the metrics to ensure non-repudiation).

EXAMPLE 1: The Trust Engine collects the metrics "CL1 reports 3 anomaly alerts in 24 hours and latency spikes (200 ms)" and "CL2 uptime (95 %), security logs (0 breaches), and response latency (50ms)". A federated ML model deployed in the Trust Engine can analyse the metrics "CL1's trust score = 40/100 (anomalies, Common Vulnerabilities & Exposures (CVE) exposure)." and "CL2's trust score = 90/100 (high uptime, no anomalies)." and outputs highlight "CVE exposure" as the primary factor lowering CL1's score.

4. The superior CL retrieves the trust level of CL1 and CL2 from the Trust Engine (e.g. the blockchain ledger).

5. The superior CL in the E2E service management domain can decide to take different actions to these two CL1 and CL2 based on their trust score.

EXAMPLE 2: The superior CL in the E2E service management domain can isolate the CL1 of MD1 to a quarantined network segment based on the low trust score and delegate CL2 of MD2 the granted access to traffic routing.

6. The CL1 of MD1 requests to re-evaluate the trust level to the Trust Engine based on the changes (e.g. uses its orchestration service to patch the CVE).

7. The Trust Engine re-evaluates the trust level of CL1 based on the trust evaluation model and updates the score to the blockchain ledger.

8. The Trust Engine notifies the updated trust level of CL1 to the superior CL of E2E service MD.

5.1.3 Potential requirements on Closed Loop trust management related capability

Capability-5.1.3-1: The ZSM framework should support dynamic, context-aware Closed Loop trust management to ensure secure coordination between Closed Loops (CLs) operating within or across management domains.

Capability-5.1.3-2: The ZSM framework should support the capability to collect trust-related metrics from Closed Loops and managed entities.

NOTE 1: Trust-related metrics include e.g. performance KPIs, security logs, behavioral patterns, security incidents, vulnerabilities of Closed Loop components.

Capability-5.1.3-3: The ZSM framework should support the capability to deploy models to evaluate the trust level of Closed Loops.

NOTE 2: Deploying models include e.g. decision trees, federated learning, to evaluate CL's behaviors and impact.

Capability-5.1.3-4: The ZSM framework should support the capability to trigger automation remediation based on trust levels of Closed Loops.

NOTE 3: Automation remediation includes e.g. isolate a compromised CL, reroute tasks to high-trust CLs.

Capability-5.1.3-5: The ZSM framework should support the capability to log trust evaluations of Closed Loops to provide non-repudiation.

NOTE 4: Ensuring non-repudiation including, e.g. the trust evaluations are signed with digital signature.

Capability-5.1.3-6: The ZSM framework should support the capability to re-evaluate the trust level of Closed Loops based on the changes of Closed Loops.

Capability-5.1.3-7: The ZSM framework should support the capability to notify the updated trust level of Closed Loops based on the changes of Closed Loops to the superior CL or other entities.

5.2 Closed Loop access control for coordination between Closed Loops

5.2.1 Issue description

According to the security threat and risk analysis in clauses 4.3.1 and 4.3.2 (e.g. D1.2, D7.1, D7.4, D8.4, D9.1, D9.2), unauthorized interactions between Closed Loops (CLs) can occur due to improper access policies, and cross-domain complexities. An adversary could impersonate trusted CLs to bypass authentication (e.g. forging credentials to escalate privileges), or exhausting management resources (e.g. controlling and executing CL illegally). A subordinate CL in a low-trust domain gains unauthorized access to a superior CL's action plans, tampering with workflows to disrupt end-to-end service delivery. Insufficient granularity of Closed Loop access control policies (e.g. granting full control to all peer CLs) can enable lateral movement for attackers. CLs' management services (e.g. orchestration, analytics) may expose sensitive capabilities to unauthorized CLs if access policies are misconfigured or failed to adapt to runtime changes (e.g. new vulnerabilities, SLA violations). Unauthorized interactions between CLs pose critical risks in multi-domain ZSM framework.

Furthermore, the trust relationship between Closed Loops across different management domains could be dynamically changed along the change of CL behaviors which can refer to the clause 5.1 of the present document. Closed Loop access control mechanism should adapt the change of trust relationship between Closed Loops across different management domains.

5.2.2 Potential proposed solutions

5.2.2.1 High Level description of the proposed solution

Closed Loop access control mechanism is proposed as a potential solution to provide dynamic authentication and authorization during cross-domain coordination between Closed Loops. The consumer of the superior Closed Loop in E2E service management domain and subordinate Closed Loop in management domain is authenticated based on their own agreed authentication policy or the security context, respectively. After authentication, the consumer of the superior Closed Loop can be granted permission based on access policies assigned to the consumer and the subordinate Closed Loop can be authorized based on security context of subordinate Closed Loop in MD. Finally, the superior and subordinate Closed Loops can cooperate to finish some specific tasks to fulfill the common goal. If some anomalies of Closed Loops have been detected, an authorized auditing service consumer can request ZSM framework to audit the consumer of superior Closed Loop for accounting through retrieving and analysing data related to the consumer of superior Closed Loop.

5.2.2.2 Procedures of the proposed solution

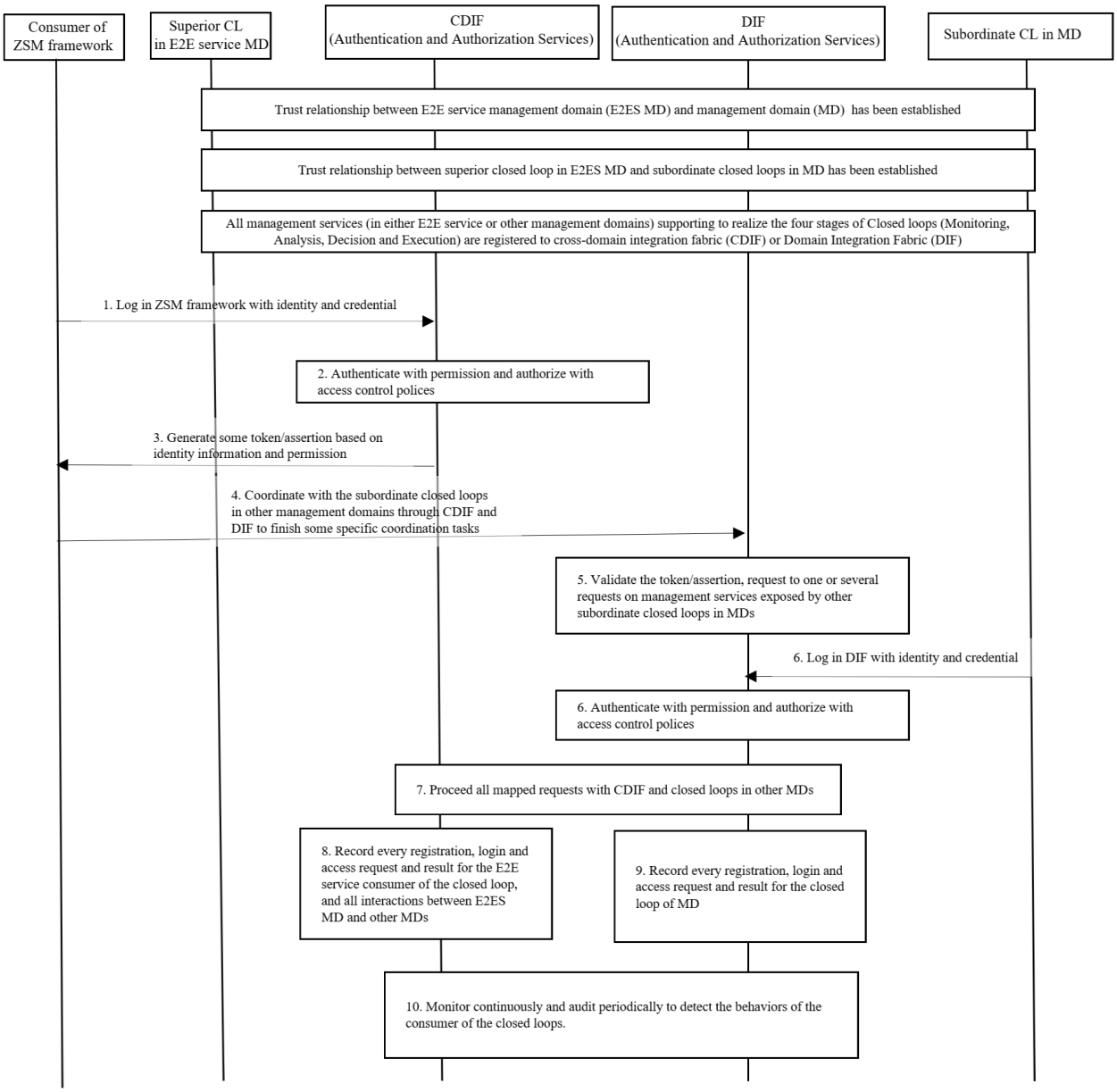

Figure 5.2.2.2-1: Access control for ZSM framework consumer of Closed Loops between management domains

Pre-condition:

- Trust relationship between E2E Service Management Domain (E2ES MD) and Management Domain (MD) has been established.
- Trust relationship between superior Closed Loop in E2ES MD and subordinate Closed Loops in MD has been established which can be referred to the clause 5.1 of the present document.
- All management services (in either E2E service or other management domains) supporting to realize the four stages of Closed Loops (Monitoring, Analysis, Decision and Execution) are registered to Cross-Domain Integration Fabric (CDIF) or Domain Integration Fabric (DIF) in the ZSM framework.

Steps:

1. ZSM framework consumer of superior Closed Loop within E2ES MD logs in ZSM framework with identity and credential. The CDIF, which may provide cross-domain authentication administration service (refer to the clause 5.2.2.1 of ETSI GS ZSM 014 [i.15]), can authenticate the consumer based on agreed authentication policy, as well as other security context of the identity (e.g. time, place, security status of the identity).

2. After authentication, the CDIF requests permission of the consumer of the superior Closed Loop. The CDIF may use authorization administration service (refer to the clause 5.2.2.3 of ETSI GS ZSM 014 [i.15]) to assign the related policies to the consumer based on the classification (e.g. security level, applied industry, region, security status) of management services registered by multiple domains on CDIF and classification/clearance of the consumer (e.g. SLA, industry, region), as well as security context of the consumer (e.g. time, location, security status, mission/reason), and grants permission to the consumer of the Closed Loop according to the access control policies.

3. CDIF generates some token/assertion based on identity information and permission to the ZSM framework consumer of the superior Closed Loop within E2ES MD.

4. The consumer of the superior Closed Loop within E2ES MD can coordinate with the subordinate Closed Loops in other management domains through CDIF and DIF to finish some specific coordination tasks (e.g. sharing knowledge across Closed Loops, pre-action conflict management between Closed Loops which refers to the clauses 5.3.2 and 5.3.4 of ETSI GS ZSM 009-2 [i.8]).

5. After having validated the token/assertion, the superior CL in the E2E service MD maps the E2E service request to one or several requests on management services exposed by other subordinate Closed Loops in MDs.

6. The subordinate Closed Loop in MD logs in DIF if there is no authentication session existed. The DIF uses authentication administration service (refer to the clause 5.2.2.1 of ETSI GS ZSM 014 [i.15]) to authenticate the subordinate Closed Loop based on Closed Loop specific authentication policy, as well as other security context of the Closed Loop. Then checks access control policies assigned to the subordinate Closed Loop, and generates token/assertion based on security context of subordinate Closed Loop in MD (e.g. time, location, security status, mission/reason, trust score). In addition, the DIF exposes allowed management services (may include service access point, operation, resource, etc.) to the subordinate Closed Loop.

7. After proceeding all mapped requests with CDIF and Closed Loops in other MDs, the superior Closed Loop in E2ES MD returns result to the E2E consumer.

8. CDIF records every registration, login and access request and result for the E2E service consumer of the Closed Loop, and all interactions between E2ES MD and other MDs in common data service.

9. DIF records every registration, login and access request and result for the Closed Loop of the MD in domain data service.

10. CDIF and DIF monitor continuously and audit periodically to detect some behaviors of the E2E service consumer for the Closed Loops against security-related criteria based on the data related to the consumer of superior Closed Loop. If the anomalies of the E2E service consumer have been detected, it is not allowed to be executed in the management domain. If the consumer of superior Closed Loop fails subsequently in monitoring or audits, it is quarantined to mitigate the risk.

5.2.3 Potential requirements on Closed Loop access control management related capability

Capability-5.2.3-1: The ZSM framework should support dynamic identity management (e.g. create, read, update and delete identity) for Closed Loop across multiple management domains.

Capability-5.2.3-2: The ZSM framework should support dynamic authentication policy management (e.g. create, read, update and delete policies) for the consumer of Closed Loops across multiple management domains.

Capability-5.2.3-3: The ZSM framework should support capability to authenticate Closed Loop based on authentication policy.

Capability-5.2.3-4: The ZSM framework should support dynamic authorization/access control policy management (e.g. create, read, update, delete) for the consumers of Closed Loops across multiple management domains.

Capability-5.2.3-5: The ZSM framework should support the capability to grant the least-privilege permissions for Closed Loops required for their assigned roles.

Capability-5.2.3-6: The ZSM framework should support the capability to grant access permissions to a Closed Loop for a specific task only for the exact duration and revoke the permissions automatically when completing the task.

Capability-5.2.3-7: The ZSM framework should support the capability to enforce access policies in real time, adapting to changes in Closed Loop trust scores or environmental risks.

Capability-5.2.3-8: The ZSM framework should support the capability to log all access attempts of Closed Loops to provide non-repudiation.

Capability-5.2.3-9: The ZSM framework should support the capability to audit and isolate Closed Loop violating access policies.

5.3 Closed Loop security exposure for coordination between Closed Loops

5.3.1 Issue description

According to the security threat and risk analysis in clauses 4.3.3 and 4.3.4 (e.g. D9.11, D1.1, D2.4), the dynamic and autonomous nature of Closed Loops introduces significant risks related to the unintended exposure of their management services and internal data.

Within the ZSM framework, management services produced by a Closed Loop (CL) may have optional or conditional external visibility (refer to ETSI GS ZSM 002 [i.2]). The exposure entitlements of a CL's management services can change dynamically based on its operational state, trust level, or the context of a coordination request (e.g. a CL may expose more capabilities during a critical incident response). If the security exposure configurations cannot dynamically adapt to such changes, it may lead to two primary risks. On one hand, a CL may inadvertently expose sensitive management services (e.g. orchestration, inventory management) or data (e.g. action plans, topology information) to unauthorized CLs or external entities. This provides a larger attack surface for adversaries to exploit (e.g. D7.1, D9.9). On the other hand, a CL may fail to expose necessary services for legitimate coordination, hindering the ability of peer or superior CLs to achieve a common objective. This can lead to failed automation, SLA violations, and inefficient resource utilization.

Furthermore, the definition of "authorized exposure" may conflict with cross management domains, leading to security gaps or operational blockages. A compromised CL can also maliciously manipulate its own exposure profile to lure other CLs into interacting with it, facilitating attacks.

5.3.2 Potential proposed solutions

5.3.2.1 High Level description of the proposed solution

A dynamic Closed Loop security exposure is proposed to continuously adjust the external visibility of a CL's management services based on a real-time assessment of security context, including the CL's trust level, the sensitivity of the requested service, the role/identity of the consuming entity, and the ongoing operational situation. The policy enforcement and decision service which can be part of the management capability exposure configuration service (refer to the clause 6.3.2.5 of ETSI GS ZSM 002 [i.2]) could evaluate the request to consume the management services utilizing a CL according to the dynamic exposure policy of the consumer of CL and handle policy enforcement and decision-making for the exposure of management services according to the evaluation.

5.3.2.2 Procedures of the proposed solution

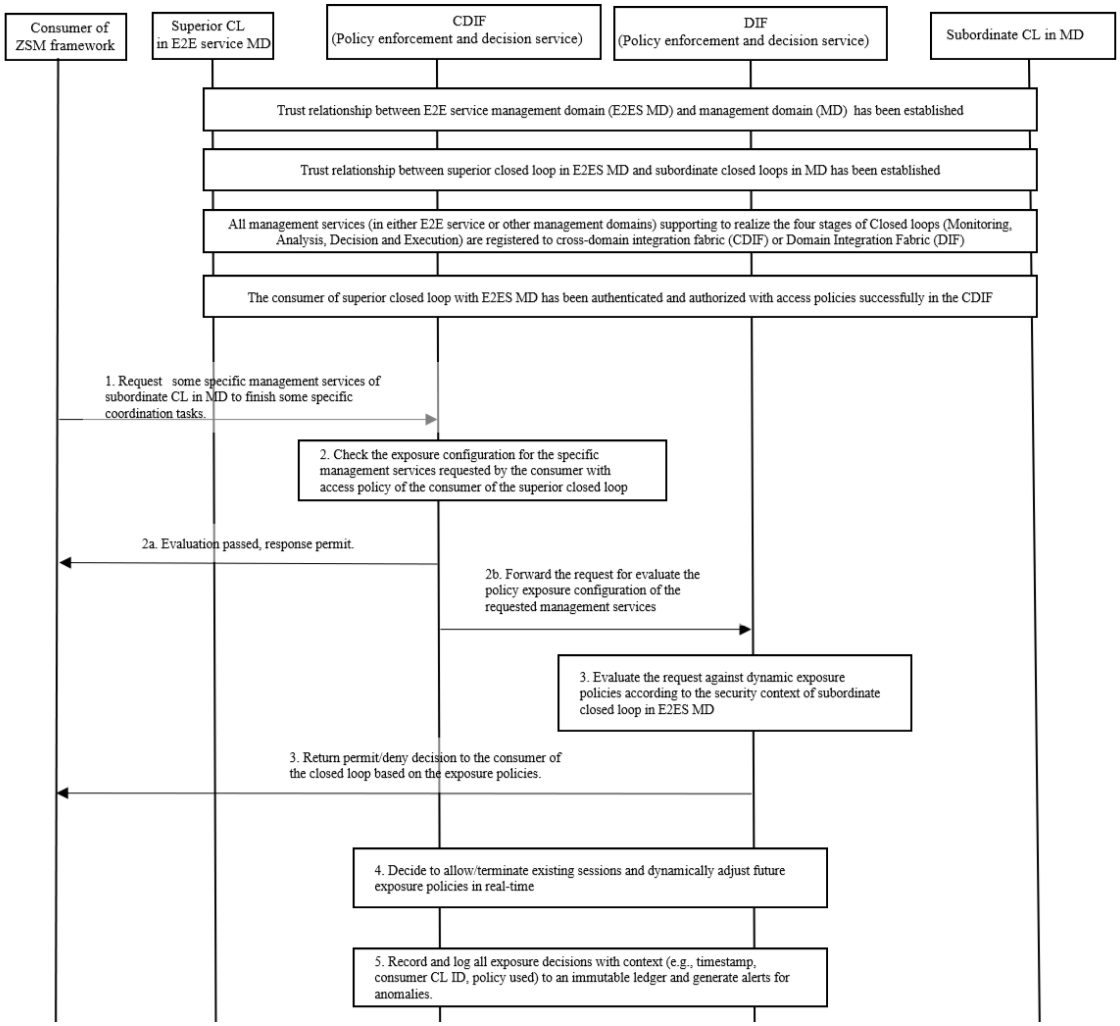

Figure 5.3.2.2-1: Security exposure for ZSM framework consumer of Closed Loops between management domains

Pre-condition:

- Trust relationship between E2E Service Management Domain (E2ES MD) and Management Domain (MD) has been established.
- Trust relationship between superior Closed Loop in E2ES MD and subordinate Closed Loops in MD has been established.
- All management services (in either E2E service or other management domains) supporting to realize the four stages of Closed Loops (Monitoring, Analysis, Decision and Execution) are registered to Cross-Domain Integration Fabric (CDIF) or Domain Integration Fabric (DIF) in the ZSM framework.
- The consumer of superior Closed Loop with E2ES MD has been authenticated and authorized with access policies successfully in the CDIF which can be referred to the Closed Loop access control procedures of clause 5.2 of the present document.

Steps:

1. The ZSM framework consumer of superior Closed Loop within E2ES MD requests some specific management services of subordinate CL in MD to finish some specific coordination tasks.

2. The CDIF by using policy enforcement and decision service checks the exposure configuration for the specific management services requested by the consumer with access policy of the consumer of the superior Closed Loop:

   2a. If the evaluation has passed, CDIF will proceed to response permit decision to the consumer of superior Closed Loop within E2ES MD and consume the specific management services.

   2b. Otherwise, the CDIF forwards the request to DIF for evaluate the policy exposure configuration of the requested management services of CL

3. The DIF using policy enforcement and decision service can evaluate the request against dynamic exposure policies according to the security context of subordinate Closed Loop in E2ES MD (e.g. time, location, security status, mission/reason, trust score) and return permit/deny decision to the consumer of the Closed Loop based on the exposure policies.

EXAMPLE: The dynamic exposure policies could be "inventory-information-service can be exposed to hierarchical CLs only if their trust score is over 80 and no ongoing security incident is declared". The evaluation for the trust score of the CL can be referred to the clause 5.1 of the present document.

4. If the trust level of CL-Consumer drops or a security incident is detected during an active session, the policy enforcement and decision service of CDIF and DIF can decide to allow/terminate existing sessions and dynamically adjust future exposure policies in real-time.

5. CDIF and DIF can record and log all exposure decisions with context (e.g. timestamp, consumer CL ID, policy used) to an immutable ledger and generate alerts for anomalies.

5.3.3 Potential requirements on Closed Loop security exposure related capability

Capability-5.3.3-1: The ZSM framework should support the capability to dynamically control the external exposure of a Closed Loop's management services based on real-time context.

Capability-5.3.3-2: The ZSM framework should support the capability to define exposure policies based on the security context of the consumers of Closed Loops across multiple management domains.

Capability-5.3.3-3: The ZSM framework should support the capability to automatically revoke or reduce service exposure permissions upon the security context of the consumer of the Closed Loops across multiple management domains.

Capability-5.3.3-4: The ZSM framework should support the capability to reconcile and enforce exposure policies of Closed Loops across different management domains.

Capability-5.3.3-5: The ZSM framework should support the capability to dynamically re-evaluate the external exposure of Closed Loops' management services based on the changes of Closed Loops.

Capability-5.3.3-6: The ZSM framework should support the capability to securely discover which management services are available for Closed Loop to consume from other Closed Loops based on exposure policies.

Capability-5.3.3-7: The ZSM framework should support the capability to log all exposure control decisions for auditability and non-repudiation.

Capability-5.3.3-8: The ZSM framework should support the capability to trigger alerts for administrative review upon the repeated denial of Closed Loops' management services exposure requests to indicate misconfiguration or a reconnaissance attack.

6 Recommendations

6.1 The summary of the present document

The present document did security threat and risk analysis for the Closed Loop and Closed-Loop Automation within ZSM framework, listed key issues/risks of the implementation of a single Closed Loop across its monitoring, analysis, decision and execution stages and the coordination/governance between multiple Closed Loops including hierarchical, peer, and external entity interactions, proposed potential solutions to mitigate the risks for the different Closed Loops across multiple management domains, and raised potential requirements on ZSM framework to support the security capabilities.

6.2 Potential future work based on the present document

Several key issues are studied in the present document and potential solutions and security capability requirements were discussed. Potential future work based on the study are listed below:

- Closed Loop specific access control is essential to interaction or exchange information between Closed Loops, therefore need to enhance the ZSM security framework to specify dynamic, context-aware access control mechanisms tailored for interactions between Closed Loops, both within and across management domains.
- To assure security of AI/ML enabled Closed Loop and Closed-Loop Automation provided by ZSM framework, ZSM framework would provide capability to mitigate AI/ML related security risks involving Closed Loops in combination with AI/ML, intents, policies, etc.
- As discussed in the present document, the process of trust evaluation and policy decision is essential for the interactions and coordination between Closed Loops, see clauses 5.1.2.2 and 5.3.2.2. More details about this process needs to be standardized.
- The security decisions capability of AI-driven Closed Loops (e.g. AI agent implementing the Closed-Loop Automation capability) is the key aspect to mitigate the security incidents automatically. However, some important issues (e.g. why a CL was deemed untrustworthy, what specific behavior triggered a security countermeasure and how a security policy was derived) need to be identified to guarantee human-understandable, transparent and interpretable explanations for the security decisions of AI-driven Closed Loops in the ZSM framework.
- Work on AI security is ongoing in several SDOs (e.g. ETSI SAI, ITU, ISO/IEC, OWASP, MITRE ATLAS) and various AI models have been developed in several open-source projects. Further work can be done to identify new AI models and how existing models can be combined to detect novel, multi-stage attacks that target the entire Closed Loop lifecycle.
- Potential security capabilities identified in clauses 5.1.3, 5.2.3 and 5.3.3 of the present document need to be revisited and evaluated if some normative work can be done in the future. These potential capabilities may be refined in ETSI GS ZSM 009-1 [i.3] and ETSI GS ZSM 014 [i.15] or new security specification if they are identified as real security requirements, or removed if they are duplicated or invalid according to the assessment.

Annex A:
Change history

Date	Version	Information about changes
November 2023	0.0.1	Initial Draft: agreement on the skeleton and initial content
May 2024	0.0.2	Included contribution: - ZSM(24)000048r1_ZSM017_Gap_Analysis_with_ZSM010
August 2024	0.0.3	Included contribution: - ZSM(24)000049r4_ZSM017 Threats and risk analysis on implementation of closed loop automation
November 2024	0.0.4	Included contributions: - ZSM(24)0000102r4_ZSM017 Threats and risk analysis on coordination between hierarchical Closed Loops - ZSM(24)000155r1_ZSM017 Threats and risk analysis on coordination between peer Closed Loops
December 2024	0.0.5	Included contributions: - ZSM(24)0000103r5_ZSM017 Threats and risks analysis on interaction between Closed Loops and external entities
June 2025	0.0.6	Included contributions: - ZSM(25)000040r1_ZSM017 Closed-loop trust management for coordination between closed loops
October 2025	0.0.7	Included contributions: - ZSM(25)0000193_ ZSM017 Closed-loop security exposure for coordination between closed loops - ZSM(25)000172r2_ ZSM017 Closed-loop access control for coordination between closed loops
October 2025	0.0.8	Included contributions: - ZSM(25)000211 ZSM017 Closed-loop security aspect introduction - ZSM(25)000213 ZSM017 Closed-loop security aspect recommendations
November 2025	0.0.9	Included contributions: - ZSM(25)000234 ZSM017_editorial_changes_for_final_draft
January 2026	1.1.1	First published version

History

Version	Date	Status
V1.1.1	January 2026	Publication