ETSI GS ZSM 012 V1.1.1 (2022-12)

Zero-touch network and Service Management (ZSM); Enablers for Artificial Intelligence-based Network and Service Automation

Disclaimer

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

Reference
DGS/ZSM-012_AI_Enablers

Keywords
artificial intelligence, automation, network

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

Introduction

The goal of ZSM is to enable zero-touch automated network and service management in a multi-vendor environment. Current techniques (e.g. rule-based management) require significant involvement of the operator. In order to achieve zero-touch automation, the involvement of the operator in network management tasks must be reduced. One way to achieve this is through Artificial Intelligence (AI). Through the union of AI and network and service management, the effort of network management operations can be significantly reduced. AI can be applied to several high potential areas such as:

- Network planning, optimization, and Service provisioning.
- Service assurance by prediction, anomaly detection, and correlation of events.
- Transforming the operator experience in adapting control and supervision interactions through machine reasoning, human/AI interaction, and scalability.

- Certain security aspects e.g. AI-based threat detection and mitigation.
- Intent fulfilment, e.g. learn what actions are more efficient and impactful to realize intents in given contexts with self-evaluation and self-measurement capabilities.

To maximize the full potential of AI in network and service automation, enabling seamless AI integration and evolution from operation to mission autonomy is required. Moreover, a comprehensive set of AI enablers should be specified to increase the scope of interoperability and to ensure that AI is trusted and capable of delivering - continuously and reliably - required business targets. Such enablers include capabilities to:

- Ensure the infrastructure supports the AI application execution requirements and constraints.
- Provide access to the right data, at the right place, and at the right time.
- Support AI techniques to interpret, recommend and act, while shifting operators' role towards formulation of higher-level declarative behavioural requirements and goals for the AI solutions.
- Govern the operation of AI applications.
- Support coordination for AI solutions.

1 Scope

The present document specifies extensions and new capabilities (so-called "AI enablers") for the ZSM framework reference architecture providing support for the automation of management functionalities and operations based on Artificial Intelligence (AI), applicable to end-to-end and per management domain. The set of AI-enabling capabilities is specified as management services, complementing the existing management services defined in ETSI GS ZSM 002 [2]. The focus is on AI-related areas such as data (including data handling and analytics), action, interoperation, governance and execution environment. Furthermore, the use and integration in the ZSM framework of externally provided AI-based capabilities are taken into account. Security and privacy aspects of AI-enabled network and service automation are taken into account, where the details would be addressed in a Security related WI.

The present document considers AI-related scenarios defined in ETSI GS ZSM 001 [1], as well as new scenarios, in order to derive AI-specific requirements. The present document also documents deployment aspects of the above scenarios to validate the applicability of the AI enablers. Related work from standard development organizations, open-source projects and other sources are considered and re-used, where applicable, in the development of the specifications.

2 References

2.1 Normative references

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

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

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

The following referenced documents are necessary for the application of the present document.

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

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

2.2 Informative references

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

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

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

[i.1] European Commission (21/04/2021): "Proposal for a Regulation laying down harmonised rules on artificial intelligence".

[i.2] Kamiran, Faisal, Asim Karim, and Xiangliang Zhang: Reject Option Classification: "Decision theory for discrimination-aware classification". In 2012 IEEE 12th International Conference on Data Mining, pp. 924-929. IEEE, 2012.

[i.3] ETSI GR ZSM 013: "Zero-touch network and Service Management (ZSM); Automation of CI/CD for ZSM services and managed services".

[i.4] 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.5] ETSI GR ZSM 009-3: "Zero-touch network and Service Management (ZSM); Closed-Loop Automation; Part 3: Advanced topics".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

explainable Machine Learning: Machine Learning model that can explain its decisions to humans in a comprehensible manner

fair Machine Learning: Machine Learning model which ensures biases in the data and/or model inaccuracies do not result in unwanted preferences towards individuals or groups

Quality of Trustworthiness (QoT): metric that describes or measures the trustworthiness aspects in Machine Learning

NOTE 1: Trustworthiness aspects may include explainability, fairness, robustness, etc.

NOTE 2: ML QoT may apply for ML data or ML model.

robust Machine Learning: Machine Learning model that is resilient to adversarial attacks (e.g. data poisoning, model leakage), that can handle unintentional errors (e.g. missing data, data drift), that have safeguard mechanisms (e.g. fallback to rule-based algorithms) put in place to deal with unexpected outcomes and that are reproducible

trustworthy Machine Learning: Machine Learning model that respects applicable laws, regulations, ethical principles, values, and is robust from a technical perspective while considering its social environment (see [i.1])

NOTE 1: The proposed EU regulation [i.1] for Machine Learning divides Machine Learning systems into three categories:

i) unacceptable-risk Machine Learning systems;

ii) high-risk Machine Learning systems; and

iii) limited- and minimal-risk Machine Learning systems.

NOTE 2: Based on those risk levels, the proposed EU regulation for Machine Learning has put forward a set of seven key requirements that Machine Learning systems should meet for them to be considered trustworthy:

i) human agency and oversight;

ii) technical robustness and safety;

iii) privacy and data governance;

iv) transparency;

v) diversity, non-discrimination, and fairness;

vi) accountability; and

vii) societal and environmental well-being (see [i.1]).

The details on each of those seven requirements are presented in annex C.

3.2 Symbols

Void.

3.3 Abbreviations

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

ACK	Acknowledge
AI	Artificial Intelligence
AIML	Artificial Intilligence and Machine Learning
AIOp	Aritificial Intelligence Operations
API	Application Interface
AppLCM	Application Life Cycle Management
CI/CD	Continuous Integration/Continuous Development
CPU	Central Process Unit
DataOp	Data Operations
DevOp	Development Operations
DML	Decentralized Machine Learning
E2E	End to End
E2ESMD	End to End Service Management Domain
EU	European Union
FFS	For Future Study
FL	Federated Learning
GDPR	General Data Protection Regulation
KPI	Key Performance Index
MD	Management Domain
ML	Machine Learning
MnS	Management Service
QoE	Quality of Experience
QoS	Quality of Service
QoT	Quality of Trustworthiness
RAN	Radio Access Network
RL	Reinforcement Learning
SL	Supervised Learning
SMD	Service Management Domain
WI	Work Item

4 Enabling areas

4.1 Overview

This clause specifies enabling areas to support the broad use of AI in a multi-vendor network and service management environment. These enablers relate to each other and together facilitate the use of AI in achieving zero touch network and service management automation. As depicted in Figure 4.1-1, the areas that are important to facilitating and enabling AI based management and automation are:

- Execution: The execution enabling area is critical for supporting deployment and operation of AI/ML applications. It addresses specific execution requirements e.g. computational requirements, time constraints.
- Data: Data is the lifeblood of AI/ML empowered automation. Providing data access across domains, ensuring the integrity and trustworthiness of the data and whether the data satisfies the required training and inference needs are of high importance for AI/ML applications to ensure correct management and orchestration decisions.
- Action: AI/ML applications play a crucial role in providing optimal control decisions and recommendations. These outputs may target machines, network entities, management domains, or other management functions and understanding AI/ML outputs is important to correctly apply these decisions.

- Governance: The governance enabling area is crucial for ensuring the trustworthiness of AI/ML applications by designing them to respect applicable laws, regulations, ethical principles, and values and be robust from a technical perspective while considering its social environment.
- Inter-AI: The Inter-AI enabling area focuses on supporting the functionalities and interactions between AI/ML applications and application components.

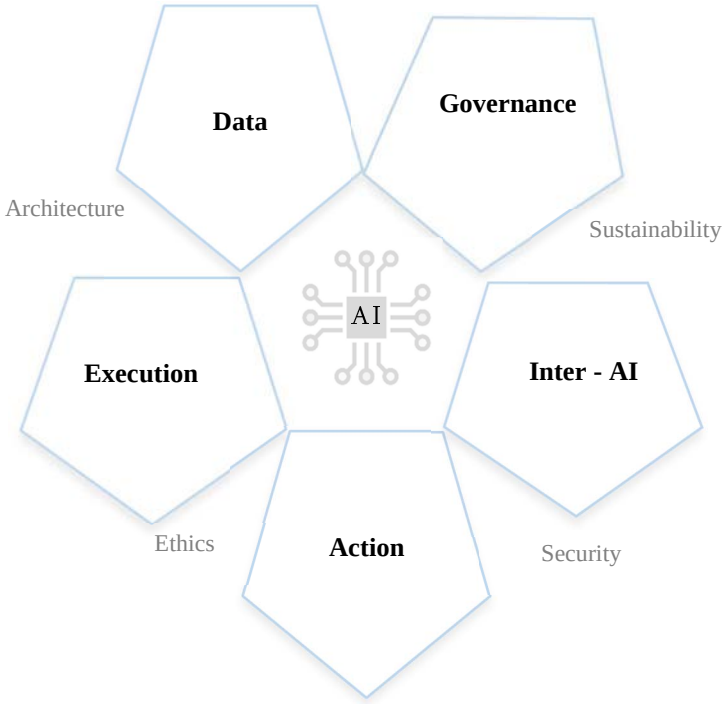


Figure 4.1-1: AI Enabling Areas

4.2 Enabling area: Execution

4.2.1 Description

The execution enabling area is critical for the deployment and operation of AI/ML applications in an operator's network empowered by AI/ML. Each AI/ML application has specific execution requirements that change depending on the operational environment where it is deployed (e.g. on-cloud, on-premises, etc.). These requirements range from computational requirements to time constraints. Matching the AI/ML application with the correct environment/infrastructure capable of meeting these requirements is very important to the successful operation of the application.

Moreover, AI/ML applications can be deployed in multiple locations, layers, and domains of the network. For example, in an operator's network, an AI/ML application may be deployed in the core or RAN. Depending on the use-case and specific solution, one deployment option might be favourable than others. Supporting all possible deployment options, as well as providing a level of coordination across domains (E2E) between different AI/ML applications, is paramount to the possible integration of a wide range of AI/ML applications with different operational, executional, and deployment specific requirements.

Finally, AI/ML applications may have different learning types. For example, a supervised learning application may need historical data sets for training purposes. Once this training is complete, deployment of the application is possible expecting accurate performance. Another example is unsupervised learning and Reinforced learning applications. These type of AI/ML applications learn by experience (e.g. performing actions and observing the effect on the environment). Depending on the use-case and solution specific implementation, an AI/ML application may have one learning type or another. It is of value to the operator's network to be able to support a wide range of possible learning types as well as provide a controlled environment where reinforcement learning based solutions can optimize their performance before being deployed in an operational environment. These controlled environments are usually referred to as Sandboxes and are typically used for testing purposes. Sandboxes are further discussed in ETSI GR ZSM 013 [i.3] Automation of CI/CD for ZSM services and managed services.

4.2.2 Requirements

The following requirements need to be fulfilled by the ZSM framework to enable the above-described aspects of AI/ML empowered network and service automation:

Req-1: ZSM framework shall support the capability to deploy AI/ML instances in a controlled testing environment (sandbox). The sandbox can be a dedicated part of the network, test network, simulation environment or a digital twin of the network.

Req-2: ZSM framework shall support the capability for the seamless integration of AI/ML applications within the ZSM fabric. AI/ML applications should be able to operate smoothly in a single domain or cross domains (E2E) through a properly defined and flexible AppLCM.

Req-3: ZSM framework shall support the capability to instantiate, integrate, chain, decommission and aggregate Data/action pipelines.

Req-4: ZSM framework shall support the capability to dynamically orchestrate and manage data/action pipelines.

4.2.3 Provided management services

4.2.3.1 ML model validation service

The ML model validation service is used to assess the performance or the trustworthiness of the trained ML model under specified conditions (e.g. operational requirements) before deployment. The trained ML models may be validated based on different aspects using a predefined sandboxing environment. Moreover, the validation of ML models may continue after the deployment, if necessary.

NOTE: The aspects of validation may be assessment of ML model performance, ML model trustworthiness or trade-off between ML model performance (e.g. accuracy, utilization of network resources) and ML model trustworthiness (e.g. explainability), etc.

Table 4.2.3.1-1: ML model validation service

Service name		ML model validation service
External visibility		Optional
Service capabilities		
	Request ML model validation (O)	Trigger model validation in predefined sandboxing environment based on defined performance and trustworthiness requirements
	Provide result of the ML model validation (O)	Provide information on ML model validation results

4.2.3.2 Sandbox Configuration Service

The sandbox configuration service enables the consumer to configure sandbox environment and provide reports on the tasks executed with and inside the sandbox, sandbox usage and status. Sandboxing environment supports different types of tasks.

Examples for tasks supported by sandbox:

- Online learning (exploration) in case of reinforcement learning.
- Validation and testing during training as well as inference.

Table 4.2.3.2-1: Sandbox configuration service

Service name		Sandbox configuration Service
External visibility		Optional
Service capabilities		
	Manage sandbox (M)	Manage (create, read, update, delete, list) sandbox environment Update allows to modify configuration parameters of the sandbox environment including CPU, memory, etc.
	Request sandbox report (M)	Request sandbox report on the tasks executed with the sandbox, sandbox usage and status. The request may specify aspects to report on e.g. memory usage, CPU status, task status, etc.
	Provide sandbox report (M)	Provide sandbox report on the tasks executed with the sandbox, sandbox usage and status according to the specification in the request

4.3 Enabling area: Data

4.3.1 Description

In an automated network and service management environment empowered by AI/ML, Data plays a crucial role. Providing data access across domains while satisfying the required data for training and inference ensures correct management and orchestration decisions. Moreover, the integrity and trustworthiness of the data are of high importance before distribution.

To reduce the load on an Operator's network as well as the management framework, data collection techniques can be optimized. This can be done through aggregation of data sources and supporting data pools for enabling the re-use of collected data by multiple AI/ML instances. Moreover, this elevates the need to provide consumers with direct access to data sources. In addition, the correct description of data in the form of metadata facilitates discovery of required data by AI/ML instances or other authorized consumers. More expressive descriptions, containing aspects such as type of data, version, and sampling frequency as well as AI/ML aspects such as labelled vs unlabelled and data statistics, ensures an easier search of required data.

Data privacy and security aspects are paramount for an automated network management environment. Providing data access only to authorized entities/consumers is critical for data governance. Additionally, anonymization and encryption of domain data provides a needed extra layer of privacy for domain specific data. Finally, observing region specific data privacy laws and regulations is important.

4.3.2 Requirements

The following requirements need to be fulfilled by the ZSM framework to enable the above-described aspects of AI/ML empowered network and service automation:

Req-1: ZSM framework shall support the capability to aggregate and reuse multiple data sources to ensure an efficient data distribution mechanism.

Req-2: ZSM framework shall support the capability to collect data, based on AI/ML model data requirements, through qualitative criteria or prediction capabilities.

Req-3: ZSM framework shall support the capability to automatically process collected data in a way that increases data quality and trustworthiness.

Req-4: ZSM framework shall support the capability to provide access to and distribute data under requirements in the same domain and across multiple domains.

NOTE 1: The requirements can be consistency requirements, time requirements such as low latency, real-time, etc.

Req-5: ZSM framework shall support the capability to describe data sets using metadata representation.

NOTE 2: The metadata representation can include data type, version, sampling frequency, labelled/unlabelled data, etc.

Req-6: ZSM framework shall support the capability to pre-process data sets according to the AI/ML model specific requirements.

NOTE 3: The AI/ML model specific requirements can be feature extraction, data labelling, etc.

Req-7: ZSM framework may support region specific laws regarding data privacy during data distribution across domains.

4.4 Enabling area: Inter AI

4.4.1 Description

The Inter-AI enabling area focuses on supporting the functionalities and interactions between AI/ML applications and application components. First, supporting a variety of AI/ML deployment schemes enables the use of AI/ML applications with different requirements and constraints. For example, one AI/ML solution may be completely centrally located while another solution may be distributed across multiple locations/domains. Each of these solutions will have use-case specific constraints deciding the exact deployment schemes (e.g. latency constraints). Another example is Federated learning, in which multiple AI/ML applications are being trained in multiple domains and then aggregated in a central location. Supporting AI/ML specific information exchange such as model parameter and training information enables operators to deploy and make use of AI/ML solutions based on Federated learning.

A very effective method to reduce the load on the operator and the management environment is to reuse existing knowledge and exploit task and domain similarity for different or similar use-cases. For example, an AI/ML application in one domain providing a solution for a specific use-case might have insight and knowledge that can be exploited by another AI/ML application in another domain providing a solution for a similar use-case.

Additionally, Multiple AI/ML applications may cooperate to solve a common problem or provide a common ML enabled solution. For example, the output of one AI/ML application can be used as input to another AI/ML application (i.e. forming a chain or sequence of interlinked modular ML applications). Alternatively, multiple ML models might provide the same type of output in parallel, and their outputs may be merged (e.g. using weights).

Enabling such and other examples of AI/ML application cooperation requires a level of coordination on the domain or E2E level to ensure consistency and concurrency. Finally, it is critical to provide means of proper authentication and trust for access control to AI/ML applications operations.

Some network scenarios require the adaptation of AI/ML applications based on domain information and data to obtain a domain specific AI/ML application. Using transfer learning methods, pre-trained AI/ML applications can be used as starting point for obtaining a domain specific AI/ML application. This method reduces training time and computational resources needed which facilitates rapid deployment of AI applications.

Additionally, due to continuous change of the network and environment, model performance of AI applications may deteriorate over time. Therefore, AI application performance monitoring and evaluation is very important. Furthermore, it is crucial to monitor network and environment statistics to detect potential data drifts (i.e. data distribution changes over the time) and model reality changes. When the performance decreases or when data drift is detected, the AI/ML application should be retrained based on the newly collected data samples.

4.4.2 Requirements

The following requirements need to be fulfilled by the ZSM framework to enable the above-described aspects of AI/ML empowered network and service automation:

Req-1: ZSM framework shall support the capability to manage and orchestrate cross domain AI/ML application training schemes ranging from fully centralized to fully distributed while satisfying different training requirements.

NOTE 1: Example for distributed learning is federated learning. The training requirements can be training data, model parameter transfer, etc.

Req-2: ZSM framework shall support the capability to enable and automate the required workflow for training and inference across different types of AIML solutions while providing access only to authorized consumers.

Req-3: ZSM framework should support the capability to provide (multi-vendor) representation of network state at the required granularity depending on the use-case.

NOTE 2: Network state can be described using slice state, service state, etc. Required granularity of the representation can be in the form of time series data, discrete data log, etc.

Req-4: ZSM framework should support the capability to evaluate domain similarity for sharing and adaptation of knowledge representation between management domains or between AI/ML applications.

NOTE 3: Examples of sharing and adaptation of knowledge can be transfer learning methods, metadata, interfaces and coordination for knowledge sharing.

Req-5: ZSM Framework should support the capability to adapt initial versions of AI/ML applications to domain specific information and data.

Req-6: ZSM Framework should support the capability to retrain the AI/ML application in case of performance degradation or model reality change.

Req-7: ZSM Framework should support the capability for an AI/ML application to improve its AI/ML model performance by interacting with the network or its equivalent and learning from the interaction in runtime.

NOTE 4 Such an interaction can be performed with the live network, sandbox environment, test network or a digital twin of the network.

Req-8: ZSM Framework should enable and coordinate domain-specific as well cross-domain cooperation between AI/ML applications/components as part of common ML enabled solutions.

4.4.3 Provided management services

4.4.3.1 FL configuration management service

The FL configuration management service enables the consumer to configure the federated learning related properties for ML models and management functions that participate in federated learning in the same or different management domain or E2E service management domain.

NOTE: Examples for federated learning configuration related to data characteristics, training termination conditions, performance, trustworthiness, model characteristics, node selection criteria, etc.

Below are some examples of the federated learning related configuration:

- The Federated learning aggregation entity needs to specify the characteristics (e.g. statistics) of the data to be used and ML model to be trained by the participating management functions.
- The Federated learning aggregation entity needs to define the conditions for terminating the training of the ML model by the participating management functions.
- The Federated learning aggregation entity needs to define the requirements related to performance of the ML model or trustworthiness of the data to be used or ML model to be trained, by the participating management functions.

Table 4.4.3.1-1: FL configuration management service

Service name		FL configuration management service
External visibility		Optional
Service capabilities		
	Manage Federated Learning configuration(M)	Manage configuration of data or ML model training characteristics for Federated learning

4.5 Enabling area: Action

4.5.1 Description

In a zero-touch network and service management environment, AI/ML applications play a crucial role in providing optimal control decisions and recommendations. These outputs may target machines, network entities, management domains, or other management functions. To this end, understanding AI/ML outputs is important in order to correctly apply these decisions or recommendations provided by the AI/ML application. Moreover, in an AI assisted network and service management environment, these recommendations may target human operators who would find it helpful to understand AI/ML outputs. Unfortunately, AI/ML application outputs is not standardized, and it differs depending on the application and/or use-case specific solution. For example, using a python made AI/ML application with library A may result in an output syntax different than an application using library B. Therefore, it is helpful to the operator that AI/ML outputs are supported by descriptive information providing details on understanding the accompanying decision/recommendation. These details support the interpretability of AI/ML application's outputs and enrich them with context information to help better translate recommendations/decisions into network actions and commands.

4.5.2 Requirements

The following requirements need to be fulfilled by the ZSM framework to enable the above-described aspects of AI/ML empowered network and service automation:

Req-1: ZSM framework shall support the capability to manage and orchestrate the use of AI/ML applications in inference, including the coordination between multiple AI/ML applications.

Req-2: ZSM framework shall support the capability to trigger appropriate actions based on AI/ML inference output.

Req-3: ZSM framework shall support the capability to provide metadata and descriptive information on the outputs of AI/ML applications.

4.6 Enabling area: Governance

4.6.1 Description

The governance enabling area is crucial for ensuring the trustworthiness of AI/ML applications deployed in the ZSM framework by designing them to respect applicable laws, regulations, ethical principles and values and be robust from a technical perspective while considering its social environment. Based on the risk level (e.g. unacceptable, high, limited) of the use case, the trustworthiness requirements of an AI/ML application may vary. Therefore, the operator shall have means to set the level of trustworthiness required (e.g. via high-level declarative goals) for an AI/ML application which the ZSM framework shall be able to satisfy. For example, if the trustworthiness requirement is to explain (human-readable) the decisions made by an AI/ML application to the operator, then the ZSM framework shall ensure that the AI/ML application is able to generate local explanations for its decisions. ZSM framework consumer also needs the means to impact (e.g. via setting rules) specific behaviour(s) of the AI/ML application so that the AI/ML application can behave accordingly. Other trustworthy requirements may include but not limited to fairness, robustness, privacy, security, safety, reliability, and traceability. It is worth to mention that robustness and security of an AI/ML application may be influenced by intrinsic design and implementation of the AI/ML application, threat surface in training and deployment environment and planned countermeasures to maintain robustness and resilience against potential adversarial attacks. These aspects are for further study and would be addressed in an ETSI ZSM Security WI.

Moreover, the ZSM framework shall also ensure the trustworthiness of decentralized AI/ML applications by considering the coordination between individual management domains and E2E service management domain. Additionally, the ZSM framework should ensure the trustworthiness for any type of AI/ML application (e.g. supervised learning, unsupervised learning, reinforcement learning).

4.6.2 Requirements

The following requirements need to be fulfilled by the ZSM framework to enable the above-described aspects of AI/ML empowered network and service automation:

Req-1: ZSM framework shall support the capability to explain and interpret the outputs and decisions of AI/ML applications. This applies locally (e.g. single decision/output) or globally (e.g. the entire behaviour of the application).

Req-2: ZSM framework shall support the capability for explaining the data used to train AI/ML applications.

Req-3: ZSM framework shall support the capability to detect, understand and mitigate bias in data and AI/ML applications, as well as ensure fairness both on the individual level and the group level (e.g. groups defined by protected attributes receiving similar outcomes).

Req-4: ZSM framework shall support the capability to be robust against adversarial threats and defend against adversarial attacks such as evasion, poisoning, and extraction.

Req-5: ZSM framework shall support the capability to be robust against missing or erroneous data, prevent introducing bias, and avoid reduction in performance caused by missing or erroneous data.

Req-6: ZSM framework shall support the capability to have a Fall-back mechanism between Trustworthy AI, non-trustworthy AI and non-AI solutions to ensure safety.

4.6.3 Provided management services

4.6.3.1 ML Data trust management service

The ML data trust management service enables the consumer to manage the trustworthiness of data (training, inference) required for ML models based on the desired level of ML data trustworthiness.

NOTE: Examples for desired level of ML data trustworthiness are: low explainability, high fairness, very high robustness.

Below are some examples for managing the trustworthiness of data:

- Training data samples can be augmented with labelled explanations thus enabling the model to be trained to provide explanations for their predicted outcomes based on the desired ML training data explainability level.
- Training data samples can be assigned (lower or higher) weights to mitigate bias or unfairness towards certain groups based on the desired ML training data fairness level.
- Based on the desired ML data robustness level, noise can be added to the data samples to protect them from data poisoning attacks.
- Based on the desired ML training data robustness level, adversarial samples can be added to the training data set to perform adversarial training to prevent from adversarial attacks.
- Based on the desired ML data robustness level, missing data can be added using a selected data imputation method.

Table 4.6.3.1-1: ML data trust MnS definition

Service name		ML data trust management service
External visibility		Optional
Service capabilities		
	Data Trust Configuration Request (M)	Manage (create, read, update, delete, list) the trustworthiness related configurations of the ML data according to the desired level of trustworthiness of ML data

4.6.3.2 ML Data Trust Evaluation Service

The ML data trust evaluation service allows to measure the trustworthiness of ML data (training, inference) and to detect trustworthiness degradations.

NOTE 1: Examples of measurements of trustworthiness are explainability metric, fairness metric, robustness metric.

NOTE 2: Examples of detected degradations are fairness degradation in data, robustness degradation in data, explanation quality degradation in data, based on the desired level of ML data trustworthiness configured in the ML data trust management service.

Table 4.6.3.2-1: ML data trust evaluation service definition

Service name		ML data trust evaluation service
External visibility		Optional
Service capabilities		
	Manage subscriptions (O)	Manage (create, read, update, delete, list) subscriptions to the trust evaluations on the data. The subscription may include a particular trustworthiness metric along with their crossed reporting threshold
	Request analysis results (C)	Trigger data trustworthiness analysis process
	Provide analysis results (C)	Provide data trustworthiness analysis results

4.6.3.3 ML Model Trust Management Service

The ML model trust management service enables to manage the trustworthiness of ML models based on the desired level of ML model trustworthiness.

NOTE: Examples for desired level of ML model trustworthiness are low explainability, high fairness, very high robustness.

Below are some examples for managing the trustworthiness of ML models:

- ML models may be configured to generate e.g. text-based explanations, examples-based explanations, contrastive explanations, etc., for their predicted outcomes based on the desired ML model explainability level.
- ML models may be configured to modify their predicted labels (e.g. based on confidence values) to ensure favourable outcomes to unprivileged groups and unfavourable outcomes to privileged groups based on the desired ML model fairness level (see [i.2]).
- ML models may be configured to add noise to their predictions to obfuscate labels and/or confidence information to protect from model inversion or inference or extraction attacks based on the desired ML model robustness level. Additionally, the ML models may be further configured to exhibit technically robust operations to minimize potentially negative impact to the network performance. This may be by defining fallback operations (e.g. switching from ML to non-ML based solutions) in situations such as applying ML in "live"/operational networks or during exploration/learning phase in Reinforcement Learning, etc.
- Based on the desired ML model robustness level, model reality drift detection and adaptation methods can be configured.
- This is also applicable in the case of ML models cooperation, e.g. within a sequence of interlinked or chain of ML models or where multiple ML models provide the same type of output in parallel.

Table 4.6.3.3-1: ML model trust MnS definition

Service name		ML model trust management service
External visibility		Optional
Service capabilities		
	Manage Model Trust Configuration (M)	Manage the configuration of trustworthiness of ML model by providing the desired level of trustworthiness for ML model

4.6.3.4 ML Model Trust Evaluation Service

The ML model trust evaluation service allows to measure the trustworthiness of deployed ML models and detecting ML model trustworthiness degradation.

NOTE 1: Examples of measurements of ML model trustworthiness are explainability metric, fairness metric, robustness metric.

NOTE 2: Examples of detected degradations are fairness degradation in ML model, robustness degradation in ML model, explanation quality degradation in ML model based on the desired level of ML model trustworthiness configured in the ML model trust management service.

Table 4.6.3.4-1: ML model trust MnS definition

Service name		ML model trust evaluation service
External visibility		Optional
Service capabilities		
	Manage subscriptions (O)	Manage (create, read, update, delete, list) subscriptions to the trust evaluations on the ML model. The subscription may include a particular trustworthiness metric along with their crossed reporting threshold
	Request analysis results(C)	Trigger model trustworthiness analysis process
	Provide analysis results (C)	Provide model trustworthiness analysis results

4.6.3.5 ML Fallback Management Service

The ML fallback management service enables the consumer to configure and trigger the fallback mechanism to other models or solutions when degradation is detected in the ML models.

NOTE 1: Examples of detected degradations are degradation of model performance and required QoT of model/data.

NOTE 2: Fallback solutions can be ML or non-ML solutions.

Table 4.6.3.5-1: ML fallback management MnS definition

Service name		ML fallback management service
External visibility		Optional
Service capabilities		
	Manage fallback configuration (M)	Manage (create, read, update, delete, list) associations between conditions and the fallback actions when degradation is detected. Degradation is detected using "Condition detection" capability as described in clauses 6.5.3.2.2 and 6.6.3.2.3 in ETSI GS ZSM 002 [2].
	Trigger Fallback(M)	Trigger fallback actions based on the fallback configuration

4.7 Common provided management services for ML

4.7.0 Introduction

ETSI GS ZSM 002 [2] defines standard management services and capabilities both on the MD and E2E SMD levels in clauses 6.5 and 6.6 respectively. To achieve ML enabled Zero touch network and service automation, some of the management services and capabilities defined in ETSI GS ZSM 002 [2] shall be enhanced to support ML specific aspects and requirements. Moreover, an extended analysis of ETSI GS ZSM 001 [1] documented scenarios on analytics and ML, as shown in Annex D, demonstrates the need for ML specific enhancements to existing management services and capabilities.

In the following, enhancements to some of the management services and capabilities previously defined in ETSI GS ZSM 002 [2] are defined.

4.7.1 ML Event Notification Service

As described in ETSI GS ZSM 002 [2], clause 6.5.2.2.1 the event notification service provides a generic event notification service. The ML specific events notification service have the same set of capabilities as the generic event notification service but provides notifications related to ML events.

Examples for ML specific events are:

- ML QoT threshold crossing for example fairness metric threshold, robustness metric threshold and explainability metric threshold.
- ML model performance during inference for example performance degradation event.
- ML model training evaluation threshold crossing for example accuracy, mean square error.

Table 4.7.1-1: ML Event Notification MnS definition

Service Name	External visibility	Service Description	Events Reported
ML performance and trustworthiness events service	C	ML performance and trustworthiness events service provides notifications about model performance and QoT monitoring events	ML performance and trustworthiness events
ML training events service	C	ML training events service provides notifications about ML training evaluation	Events related to ML training
NOTE: In the presence of AI/ML then the service capabilities should be supported.			

4.7.2 ML Log Collection Service

As described in ETSI GS ZSM 002 [2], clause 6.5.2.2.4 the log collection service provides a generic log collection service. The ML log collection service is derived from and has the same set of capabilities as the generic log collection services and collects ML specific logs.

Example of ML specific log collections are:

- Explanations on the behaviour of the ML models or reasons for the predicted outcomes from the ML models or both. The ML log collection service provides explanations originating from the managed ML models either via streaming using the management communication service of the integration fabric or in batches to the authorized consumer. The information provided includes parameters such as ML model identifier producing the explanation, the timestamp of the explanation and the content/identifier of the explanation.
- ML model training and retraining events (information on data set used, observed changes).

4.7.3 ML Feasibility Check Service

As described in ETSI GS ZSM 002 [2], clauses 6.5.5.2.2 and 6.6.5.2.2 the feasibility check service provides a generic service to check whether the service is deployable at proposed service level. The ML feasibility check service has the same capability as the generic service and performs feasibility checks of ML specific aspects and is used in ML specific use cases.

Examples of ML specific feasibility checks are:

- ML trustworthiness requirements (e.g. required QoT).
- Management functions supporting ML training e.g. local training for ML federated learning.

Table 4.7.3-1: ML feasibility check MnS definition

Service name		ML Feasibility Check Service
External visibility		Optional
Service capabilities		
	Check ML performance and trustworthiness feasibility (C)	Check whether the ML performance and trustworthiness requirements can be supported by the E2E service management domain or management domain
	Check ML training feasibility (C)	Check whether the ML training requirements can be supported by E2E service management domain or management domain
NOTE: Either one of the service capabilities should be provided if this service is supported.		

4.7.4 ML Data Processing Service

As described in ETSI GS ZSM 002 [2], clause 6.4.2.3 the data processing service provides a generic execution environment for data processing. This service allows performing data analysis and data processing based on provided processing instructions.

This service can be used in ML specific use cases.

EXAMPLE 1: Possible use case: the data used for ML model training and inference can be processed to derive information on model reality and to detect changes in model reality, e.g. in terms of data statistics.

EXAMPLE 2: The Feature extraction, data labelling and grouping details of the data is used for ML model training or inference. Feature extraction prepares data for the input to both training and inference. Labelling provides the ground truth to check the output of both the training and inference. The ground truth is collected together with the input as historical data for future use which can be processed to prepare the input for both training and inference.

4.7.5 ML Training Reporting Service

The ML training reporting service enables the consumer to configure and provide reports on the performance evaluation of the ML model in the training phase and provides reports on the training. Specific metrics related to training evaluation may be monitored. The reported training evaluation metrics may be a sub-set of supported training evaluation metrics.

NOTE: The training evaluation metrics describe the performance of the ML model in training phase. Examples for training evaluation metrics may be accuracy/precision/recall/F1-score/MSE/MAE/confusion matrix of the ML model in training phase.

Table 4.7.5-1: ML training reporting service

Service name		ML training reporting service
External visibility		Optional
Service capabilities		
	Manage subscriptions (C)	Manage (create, read, update, delete, list) subscriptions to the training results report that describes the outcomes of the training
	Configure training reporting (C)	Configure the monitoring of training evaluation metrics and reporting of training results
	Request training report (O)	Request ML model training evaluation metrics and training results report
	Provide training report (O)	Provide ML model training evaluation metrics and training results report

4.7.6 ML model cooperation management service

As described in ETSI GS ZSM 002 [2], clauses 6.5.4.2.1 and 6.6.4.2.1 the AI model management service enables to manage ML models. An ML model can be updated based on new input data periodically. Further extensions of this service are needed to address the specifics of ML models cooperation, e.g. within a sequence of interlinked or chain of ML models or where multiple ML models provide the same type of output in parallel. ML model cooperation management service is derived from AI model management service to address the needed extensions.

Examples of ML model cooperation specifics are:

- ML model cooperation where the output of one ML model can be used as input to another ML model forming a sequence of interlinked ML models i.e. chain of ML models.
- ML model cooperation where multiple ML models provide the same type of output, for services or solve problems, in parallel, and their outputs may be merged (e.g. using weights).

Table 4.7.6-1: ML model cooperation MnS definition

Service name		ML model cooperation management service
External visibility		Optional
Service capabilities		
	Manage ML model cooperation (M)	Manage (create, read, update, delete, list) the ML model cooperation, e.g. chaining of ML models - mapping the output of one model to the input of another model, or how the model outputs shall be merged

Annex A (normative): Scenarios

A.1 Trustworthy Machine Learning for Network and Service automation

A.1.1 Description

This scenario describes the operations associated with managing trustworthiness of Machine Learning (ML) services in the ZSM framework.

A.1.2 Rationale and Challenges

ML is one of the tools/methods to achieve the target of zero-touch network and service automation. As such, new requirements and related management services were introduced to support ML algorithms in the ZSM framework (see ETSI GS ZSM 001 [1], clause 6.4.2 and ETSI GS ZSM 002 [2], clauses 6.5.4 and 6.6.4). However, the introduction of ML algorithms (e.g. neural network) also results in various technological challenges involving ethical, lawful and robustness aspects that need to be addressed by the ZSM framework. These challenges include lack of explainability with respect to ML decisions, bias in ML algorithms, missing data to train the model, data & model poisoning attacks, etc. Therefore, depending on the risk-level of the use case (e.g. critical infrastructure is a high-risk use case), it is necessary to design trustworthy (as defined in clause 3.1) ML services addressing the needs of various telco stakeholders (e.g. vendors, operators, regulators, end-users, etc.).

A.1.3 ZSM scenario details

The above-mentioned challenges affect several stakeholders (e.g. operator, vendor, regulator) within the ZSM framework. Therefore, it is necessary to ensure the trustworthiness of ML services deployed in the network which can be achieved by:

1) Providing means in the ZSM framework for ZSM authorized entities to request and receive detailed explanations for decisions made by ML services to understand their effect on the network behaviour.

2) Enabling the operator to configure fairness, robustness, and other trustworthiness requirements for the ML services that the ZSM framework should consider.

3) Providing operators with the technical capabilities to support multiple levels of trustworthiness.

Additionally, it is necessary to understand that there may be a trade-off between ML performance (e.g. accuracy, utilization of network resources) and ML trustworthiness (e.g. explainability) which needs to be accounted for by the ZSM framework. Stricter trustworthiness measures might reduce ML performance (e.g. more explainable ML algorithm might result in lower accuracy in model predictions and increase the utilization of network resources in order to realize the level of trustworthiness required). Moreover, backward compatibility is important to ensure the continuation of smooth operations while increasing the amount of trustworthiness measures in the network. Therefore, the integration of trustworthy ML services in the ZSM framework shall be accomplished gradually without any interruption of service or operations in the operator's network.

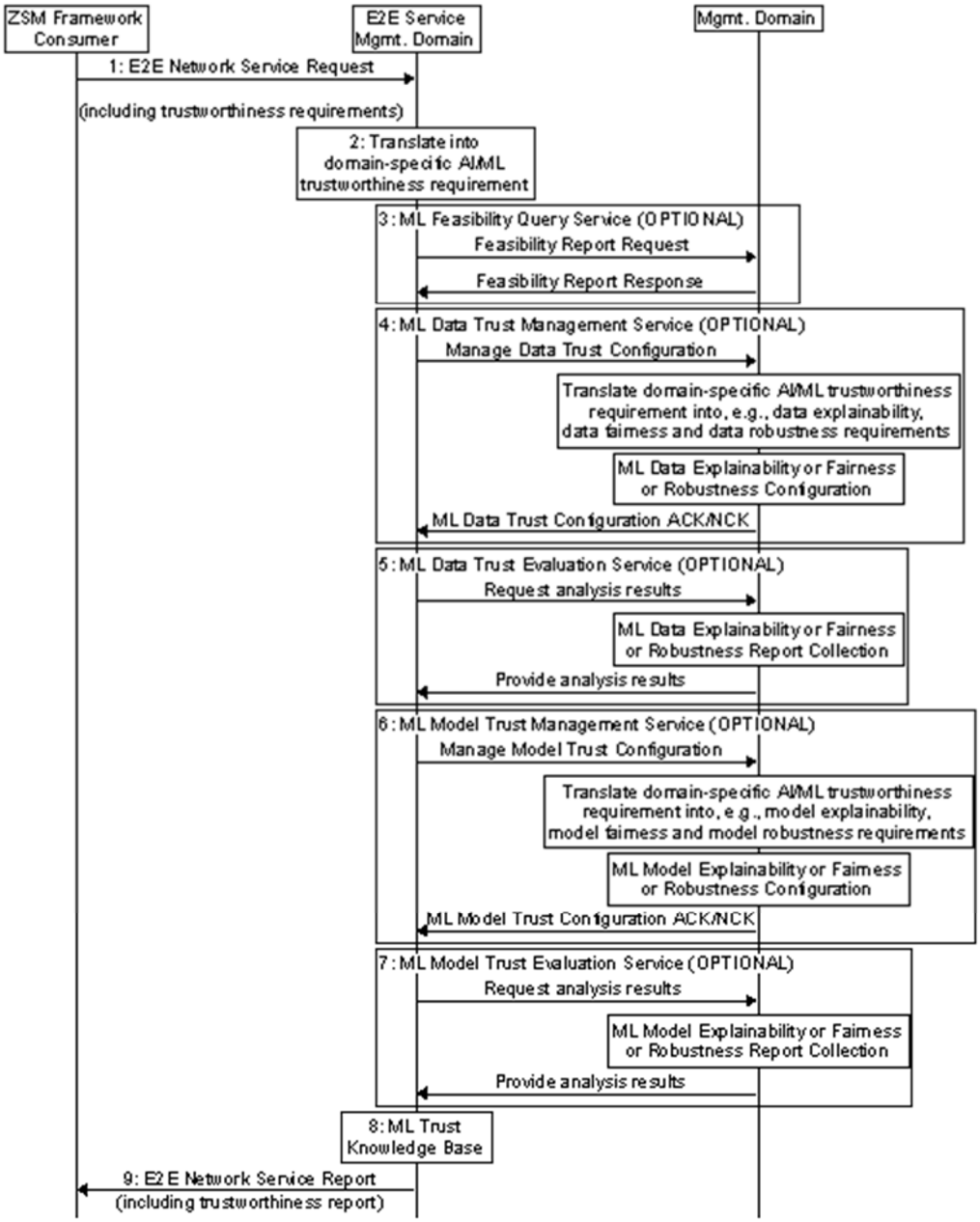


Figure A.1.3-1: Trustworthy ML workflow in ZSM framework

Step 1: ZSM Framework Consumer requests for an end-to-end network service with the desired end-to-end network service requirements (including trustworthiness requirements).

Step 2: Depending on the risk level of the end-to-end network service, E2E Service Management Domain translates the end-to-end network service requirements (including trustworthiness) into domain-specific service requirements (including trustworthiness). If ML models are utilized for optimizing an end-to-end network service, then E2E Service Management Domain also translates the end-to-end network service ML trustworthiness requirements into domain-specific service ML trustworthiness requirements (e.g. domain-specific ML Quality of Trustworthiness). One example of such a translation is shown in Table A.1.3-1. The domain-specific service ML trustworthiness requirements may be translated further into ML explainability, ML fairness and ML robustness requirements either by E2E service management domain or induvial management domains. Table A.1.3-2 shows example classes for ML QoT.

Table A.1.3-1: Example Translation from Cross-Domain ML Quality of Trustworthiness to domain-specific ML Quality of Trustworthiness

Cross-Domain ML QoT	Example network service	Domain 1	Domain 2	Domain X
Class 1	Autonomous Driving	ML QoT Class 1	ML QoT Class 1	ML QoT Class 2
. . .	. . .	. . .	. . .	. . .
Class N	Video Streaming	ML QoT Class N-5	ML QoT Class N	ML QoT Class N

Step 3: The E2E Service Management Domain uses capability *Feasibility Report Request for trustworthiness to* the Management Domain, to discover the network resource capabilities or constraints to realize required QoT of ML model. The request may include the information on the ML model but also further information to describe the request, e.g. for which ML model phase (e.g. training, inference) the request relates to, etc. The Management Domain uses capability *Feasibility Report Response for trustworthiness* to the E2E Service Management Domain to indicate whether the realization of required QoT of ML model is feasible or not according to available network resources. Further related information, such as ML model phase or indication on temporal or spatial validity of the response may be included.

Step 4: The E2E Service Management Domain uses capability *Manage Data Trust Configuration* to the Management Domain to notify about the translated domain-specific service ML trustworthiness requirements (e.g. domain-specific ML Quality of Trustworthiness) required to be met in the domain-specific ML model. The Management Domain may translate the domain-specific service ML data trustworthiness requirements into ML data explainability or ML data fairness or ML data robustness requirements (one example of such a translation is shown in Table A.1.3-2). Optionally, the E2E Service Management Domain may directly translate and send the required ML data explainability or ML data fairness or ML data robustness corresponding to the domain-specific ML model. Based on the derived requirements, Management Domain configures corresponding ML data explainability or ML data fairness or ML data robustness methods or metrics in the domain-specific ML model. The Management Domain uses capability *ML Data Trust Configuration ACK/NCK* to the E2E Service Management Domain to indicate whether the previous operations were successful or not.

Table A.1.3-2: Translation from Domain-specific ML Quality of Trustworthiness to explainability, fairness and robustness requirements

Domain-specific ML QoT	Example network service	Explainability	Fairness	Robustness
Class 1	Autonomous Driving	High	High	High
. . .	. . .	. . .	. . .	. . .
Class N	Video Streaming	Low	Medium	Medium

Step 5: The E2E Service Management Domain uses capability *Request Analysis Results* to the Management Domain containing the reporting/subscription configuration for the domain-specific ML model. Optionally, the E2E Service Management Domain may directly request ML data explainability report or ML data fairness report or ML data robustness report corresponding to the domain-specific ML model. If one or more reporting characteristics (e.g. periodic or on-demand) is met, the Management Domain collects ML data trustworthiness reports (e.g. data explainability metrics, data fairness metrics, data robustness metrics) from the domain-specific ML model.
The Management Domain uses capability *Provide Analysis Results* to the E2E Service Management Domain as per the reporting configuration specified in *Request Analysis Results.*

Step 6: The E2E Service Management Domain uses capability *Manage Model Trust Configuration* to the Management Domain (e.g. domain-specific ML Trust Engine) to notify about the translated domain-specific service ML trustworthiness requirements (e.g. domain-specific ML Quality of Trustworthiness) required to be met in the domain-specific ML model. The Management Domain may translate the domain-specific service ML model trustworthiness requirements into ML model explainability or ML model fairness or ML model robustness requirements (one example of such a translation is shown in Table A.1.3-2). Optionally, the E2E Service Management Domain may directly translate and send the required ML model explainability or ML model fairness or ML model robustness corresponding to the domain-specific ML model. Based on the derived requirements, Management Domain configures corresponding ML model explainability or ML model fairness or ML model robustness methods or metrics in the domain-specific ML model. The Management Domain uses capability *ML Model Trust Configuration ACK/NCK* to the E2E Service Management Domain to indicate whether the previous operations were successful or not.

Step 7: The E2E Service Management Domain uses capability *Request Analysis Results* to the Management Domain containing the reporting/subscription configuration for the domain-specific ML model. Optionally, the E2E Service Management Domain may directly request ML model explainability report or ML model fairness report or ML model robustness report corresponding to the domain-specific ML model. If one or more reporting characteristics (e.g. periodic or on-demand) is met, the Management Domain collects ML model trustworthiness reports (e.g. model explainability metrics, model fairness metrics, model robustness metrics) from the domain-specific ML model. The Management Domain uses capability *Provide Analysis Results* to the E2E Service Management Domain as per the reporting configuration specified in *Request Analysis Results*.

Step 8: The E2E Service Management Domain stores the collected ML data trust reports and ML model trust reports in the ML Trust Knowledge Base.

Step 9: The E2E Service Management Domain may provide a report (including ML data trust and ML model trust related information) to the ZSM Framework Consumer corresponding to the end-to-end network service.

A.1.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to facilitate the integration of Trustworthy ML as a service into a zero-touch automation environment including different trustworthy ML methods.

NOTE 1: Trustworthy ML methods can be Fair ML, Robust ML, explainable ML, etc.

Req-2: ZSM framework shall support the capability to measure and provide trustworthy ML metrics.

Req-3: ZSM framework shall support the capability to provide explanations for ML-based decisions.

Req-4: ZSM framework should support stepwise introduction of Trustworthy ML based management, allowing a mixed environment of trustworthy and non-trustworthy ML algorithms.

NOTE 2: Stepwise - the introduction of trustworthy ML based management in a series of stages offering backward compatibility with non-trustworthy ML as well as non-ML services.

A.2 Decentralized Machine Learning for Network and Service Automation

A.2.1 Description

This scenario describes the operations associated with managing decentralized Machine Learning (ML) services in the ZSM framework.

A.2.2 Rationale and Challenges

ML is one of the tools/methods to achieve the target of zero-touch network and service automation. As such, new requirements and related management services were introduced to support centralized ML services in the ZSM framework (see ETSI GS ZSM 001 [1], clause 6.4.2 and ETSI GS ZSM 002 [2], clauses 6.5.4 and 6.6.4). However, in cross-domain network & service automation, individual Management Domains (MDs) might not want to share their raw/complete data with other MDs or E2E Service MD due to several reasons: confidentiality, privacy, ethical, regulatory (e.g. GDPR), etc. Hence, training efficient centralized ML services in E2E Service MD becomes very challenging. This poses a trade-off between performance (e.g. accuracy) and data governance (e.g. privacy) in the operator's environment when using ML services for Cross-domain use cases. This needs to be addressed by the ZSM framework as it is necessary to support decentralized (e.g. Federated Learning) ML services to ensure data governance in ML models.

A.2.3 ZSM scenario details

The above-mentioned challenges can be addressed by enabling decentralized learning in proactive cross-domain use cases within the ZSM Framework, (e.g. Federated Learning with E2E Service Management Domain taking the role of FL aggregator and underlying Management Domains taking the role of distributed nodes) as shown in Figure A.2.3-1. This allows for training ML models in individual MDs without centralizing the data in E2E Service Management Domain in addition to capturing the shared knowledge of all participating management domains by aggregating their model parameters, regardless of the disparity between their data distributions. This can lead to a better performing global model compared to the model trained using only the individual management domain data.

Moreover, the introduction of decentralized ML algorithms results in various other technological challenges involving ethical, lawful, and robustness aspects that need to be addressed by the ZSM framework through designing trustworthy (as defined in clause 3.1) decentralized ML services. These challenges include lack of explainability with respect to decentralized ML services, bias in decentralized ML algorithms, missing data in training nodes, security when exchanging model parameters between central and distributed nodes and so on. On the other hand, it is necessary to understand that there may be a trade-off between decentralized ML performance and trustworthiness of decentralized ML services which needs to be accounted for by the ZSM framework. Therefore, the integration of trustworthy decentralized ML services in addition to the existing centralized ML services in the ZSM framework shall be accomplished gradually.

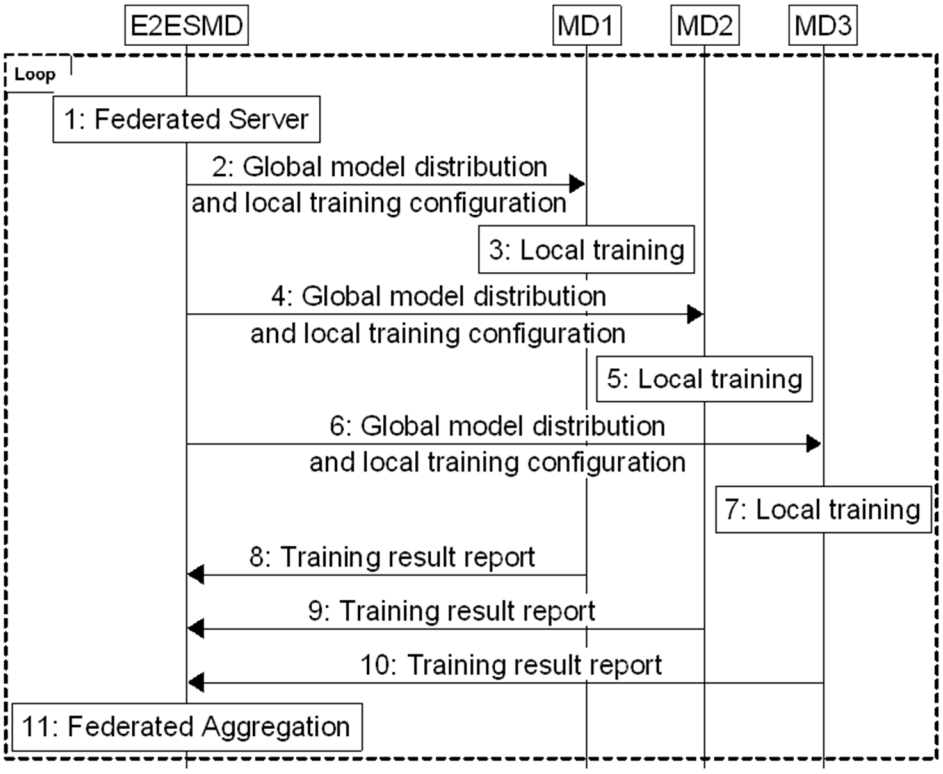


Figure A.2.3-1: Federated Learning Workflow in ZSM framework

A.2.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to facilitate the integration of decentralized ML as a service into a zero-touch automation environment.

Req-2: ZSM framework shall support the capability to measure and provide metrics of trustworthiness in decentralized ML service.

Req-3: ZSM framework shall support the capability to provide explanations for decisions made by decentralized ML service.

Req-4: ZSM framework should support stepwise introduction of decentralized ML based management, allowing centralized and decentralized ML services to work in parallel.

A.3 AI/ML model validation - pre-deployment/post-deployment validation and model reality monitoring

A.3.1 Description

This scenario describes the AL/ML model validation, pre/post deployment AI/ML model validation and model reality monitoring associated with AI/ML services in the ZSM framework.

A.3.2 Rationale and Challenges

AI/ML is one of the tools to achieve the target of zero-touch network and service automation. As such, new requirements and related management services were introduced to support AI/ML algorithms in the ZSM framework (see ETSI GS ZSM 001 [1], clause 6.4.2 and ETSI GS ZSM 002 [2], clauses 6.5.3, 6.5.4 and 6.6.4). The ZSM framework defines the generic service for Deployed AI model assessment service (Domain/E2E Intelligence) which relies on the result of Deployed AI model performance evaluation service (Domain/E2E Analytics) and determines the need for AI model update or replacement. However, such services need additional AI/ML specific enhancements in order to ensure the achievement of required AI/ML model performance. For example, AI/ML model validation prior to deployment is important to assess its performance after the deployment. Additionally, long-term validation of the deployed model, as well as monitoring and detecting the changes in the model reality, e.g. in terms of input data statistics, provides an indication of potential model performance degradation and the need for further model update and validation.

A.3.3 ZSM scenario details

The performance of the AI/ML model may change due to many reasons, e.g. change of the model reality by means of changed data input statistics, deployment of the model in a reality which differs from design and training reality, etc. The AI/ML model performance change may lead to unexpected or undesired effects on the network operation. Therefore, it is highly important to perform the validation of AI/ML model to evaluate the model performance, as well as to assure achievement of required AI/ML service performance within the ZSM framework. Thus, the validation of the AI/ML model may be carried out prior, as well as after the model deployment.

Due to the AI/ML models' learning and adapting to the reality prior to deployment, e.g. from training data, it is very difficult or even impossible to estimate a-priori the achievable performance of the model after the deployment, e.g. in the operational reality. Thus, to evaluate AI/ML model's true usability and performance, the AI/ML model may be evaluated in a sandbox environment, prior to the actual deployment. After successful evaluation, the AI/ML model is deployed in the operational reality.

However, the operational reality may change after the model deployment, e.g. the statistics of the input data may change. This may lead to changes (typically degradation) of the AI/ML model performance. Therefore, further (long-term) validation of the model is needed. The long-term validation of the model means determining performance measures during operation and comparing those to the expected performance. Model validation during operation may be done using different approaches (e.g. manual checks, using an oracle model, etc.)

A.3.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to derive information on AI/ML model reality.

NOTE 1: The derived information can be in terms of used data statistics.

Req-2: ZSM framework shall support the capability to monitor and detect changes in AI/ML model reality.

Req-3: ZSM framework shall support the capability to validate AI/ML model prior to deployment using different approaches.

NOTE 2: The validation approach can be model performance assessment in a sandboxing environment.

Req-4: ZSM framework shall support the capability to validate AI/ML model performance after deployment using different approaches.

A.4 Anomaly Management using AI/ML based closed loop

A.4.1 Description

This scenario describes the use of Machine Learning (ML) technologies in a closed loop for the anomaly management in ZSM framework.

A.4.2 Rationale and Challenges

ETSI GS ZSM 002 [2], clause 6.5.3.2.1 defines anomaly detection service, as part of the Domain Analytics that provides capabilities to detect anomalous conditions using the collected fault, performance, usage, and configuration data about the managed entity. A related scenario - "Automated service healing capability for handling infrastructure failures" is described in ETSI GS ZSM 009-2 [i.4], clause 5.1.3 (scenario 3) which uses the anomaly detection service to detect fault conditions in E2E management domain. Similarly ETSI GR ZSM 009-3 [i.5], clause 5 describes the application of ML technology that can be incorporated in to various control loop stages such as:

- ML-based monitoring, analysis, decision making and optimized actions.

Therefore, referring to these specifications management of anomalies using an AI/ML based closed loop is a relevant scenario to be considered.

Anomaly conceptually is an unusual, unexpected event, observation, or items significantly different from what is allowed or expected. Here the concept of anomaly is not limiting representation of fault scenarios alone, but observations which deviate from the other observations as to arise suspicions. For example, change of traffic metrics because of a popular event (e.g. New Year eve, sports event). Such anomalous metric may not necessarily cause the network to operate in a faulty manner. So anomaly management using an AI/ML based cognitive closed loop has wider application, not limiting to fault scenarios, as it provides right mechanism for addressing different operational stages in an autonomous fashion. Leveraging AI/ML enablers enhance the anomaly management closed loop by automating critical decisions and actions.

ETSI GR ZSM 009-3 [i.5], clause 6 describes the use of Analytics models assisted/enabled by AI/ML in closed loop for analytics capabilities. While ETSI GR ZSM 009-3 [i.5] focus on the closed loop cognitive capabilities, it is important to note the challenges involved in using AI/ML Models as enablers in closed loop with the help of the scenario detailed here. Some of the challenges associated with use of ML Models in closed loop are listed below:

1) Dynamic selection of on-demand data sources based on the analytics flow - for example in anomaly management, closed loop may require selection of the data sources dynamically for determining the root cause when an anomaly is detected or when it determines that the data is not sufficient for finer analysis.

2) Detection of the ML capability for producing conclusive or confident results by checking model's intrinsic confidence metric - in anomaly management this may be required for checking if the ML Model is generating false-positives or false-negatives which trigger unwanted actions.

3) Ability to compare the distribution of input data to model on the field with the training data used by ML model to check if there is data drift - in anomaly management this may be required to ensure the behaviour of ML model is consistent with the operational goal.

4) Ability to check if a given model is sufficient for analytics/decision or another model/another data source may be required - in anomaly management this may be required to detect new patterns of anomalies which cannot be determined by an existing model using its training data.

5) Ability to control the ML based analytics models so that the operational flow of the closed loop can be diverted based on operational needs - in anomaly management this may be required to manage the operational flow of the closed loop based on the operational reality.

6) Ability to explain and interpret the results produced by AI/ML Models in a closed loop at a later point in time - in anomaly management this may be required to revisit or audit the decisions or analytics results produced by an AI/ML model and validate associated control flow of the closed loop.

A.4.3 ZSM scenario details

Anomaly management using an AI/ML based closed loop involves closed loop analysis, where in an event or metric detected in the E2E or domain management system can be evaluated against a known/allowed metric range or event pattern. Such known/allowed metric range or event pattern can be used for training the AI/ML models. Additionally AI/ML models can be used for identifying the potential root causes or appropriate actions to mitigate the anomaly or recover from fault condition caused due to anomaly.

The closed loop used for anomaly detection can leverage the AI/ML enabled Analytics Models in different stages such as:

- Monitoring: Dynamic selection of data sources using an AI/ML Model based on the analytics capability required for anomaly detection - for example few input data with coarse analytics result or large input data with finer analytics results.
- Detection: AI/ML Model used for identifying the anomaly against allowed metrics range or event pattern. This involves monitoring of the metrics or events by a trained AI/ML Model for detection of anomalies which are deviations from the allowed range.
- Root Cause Analysis: AI/ML Model used for identifying the root cause of anomalies. Here ML Models are trained based on historical events, metrics or associated root cause scenarios or uses online training to update the ML model based on new patterns of anomalies and related causes.
- Mitigation action selection: AI/ML Model used for selecting the right dynamic action based on the operational reality.
- Conflict resolution: AI/ML Model used for Pre and Post Execution Co-ordination of closed loop actions based on the knowledge base and operational reality.
- Recovery from the fault: If the anomaly results in a fault, AI/ML model can be used to identify the right resolutions.
- Health reporting: AI/ML model can be used in health reporting based on classification of the anomaly condition or patterns detected in anomaly over a period of time.

A.4.4 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to dynamically select on-demand data sources as determined by a closed loop for AI/ML Model training.

Req-2: ZSM framework shall support the capability to determine the ability of the AI/ML model to produce conclusive and confident results by analysing the metrics associated with the model.

NOTE 1: List of metrics to be analysed can be defined as part of the metadata associated with AI/ML model. Examples of metrics that may help to determine the capability of predicting conclusive and confident results are - Accuracy, Precision, F1-Score, Root Mean Square Error, Mean Absolute Error, etc.

Req-3: ZSM framework shall support the capability to control AI/ML Models used in a closed loop based on the dynamic operational requirements or AI/ML Model reality.

NOTE 2: Examples of control capability that may be enabled on AI/ML Models in closed loop are activation/deactivation of AI/ML Model, pause/restart of analysis, scheduling of analysis at particular time window, filter and bypass analysis for specific samples of data, diversion of analysis to a human operator or alternate applications, etc.

Req-4: ZSM framework shall support the capability to determine changes in the data over time, provided as input to the AI/ML Model that helps to identify appropriate training or model enhancement requirements.

Req-5: ZSM framework shall support the capability to determine if a model is sufficient for an analytics requirement or an alternate model or data source is required.

NOTE 3: Example of capability to check if a model is sufficient may be to analyse the input data for accuracy (such as error, missing data), implausible values in data, wrong sequence of data and data drift. The data quality check helps to identify if a particular ML Model is sufficient for analysis or an alternate model or data source is required. In distributed AI/ML processing used for optimum performance and security, the operational goals (such as performance, security, coverage) drive the need for multiple/distributed ML models or sequence of interlinked ML models. Checking the AI/ML metadata (AI/ML Model capabilities and characteristics - such as ability to split and consolidate the distributed analysis results, ability to maintain intermediate results in interlinked ML Model sequence) against the operational and AI/ML Reality helps to determine if an ML Model is sufficient or additional/alternate, ML Models are required.

Req-6: ZSM framework shall support the capability to interpret or explain the results produced by the AI/ML Model with required traceability in association with the AI/ML reality or operational reality at different time intervals.

A.5 ML model cooperation - modular approach

A.5.1 Description

Multiple ML models may cooperate to solve a common problem or provide a common solution, as described in the present document Inter AI Enabling area (clause 4.4). There are different ways in which the ML models may cooperate. An example of ML model cooperation is the case where the output of one ML model can be used as input to another ML model forming a sequence of interlinked ML models i.e. chain of ML models. Another example of ML model cooperation is the case where multiple ML models provide the same type of output in parallel, and their outputs may be merged (e.g. using weights). Such ML models may be regarded as components of a single ML enabled solution. The modular approach in building a single ML enabled solution facilitates ML model reusability and replacement, as well as modular evolvement, improvements, and changes of individual ML components.

A.5.2 Rationale and Challenges

ML is one of the tools to achieve the target of zero-touch network and service automation. As such, new requirements and related management services were introduced to support ML algorithms in the ZSM framework (see ETSI GS ZSM 001 [1], clause 6.4.2 and ETSI GS ZSM 002 [2], clauses 6.5.3, 6.5.4 and 6.6.4). The present document introduces the Inter-AI enabling area with a focus on supporting the functionalities and interactions between ML applications and application components. In the case of modular approach in building ML enabled solutions the interactions between the ML components needs to be enabled. Furthermore, the functionalities that allow management of such a single ML enabled solution, e.g. derivation of metrics related to ML enabled solution based on monitored metrics of individual ML components, collection and exposure of the knowledge related to ML enabled solution, etc.

The framework described in ETSI GS ZSM 002 [2] defines various services for handling individual ML model aspects, e.g. performance evaluation, knowledge database, etc. Moreover, further related services were introduced within the present document, e.g. trust evaluation, log collection service for explainability, etc. However, such services need additional enhancements to enable and coordinate the interactions between different ML components in an ML enabled solution. Such enhancements may include orchestration aspects such as aggregation of the monitored performance and trustworthiness metrics of individual ML components that form part of a single ML enabled solution. Moreover, they may include management aspects such as configuration of ML enabled solution specific data collection.

A.5.3 Related requirements for ZSM

Req-1: ZSM framework shall support the capability to enable and coordinate domain-specific as well cross-domain cooperation between ML components as part of single ML enabled solution.

A.6 A Federated Learning scenario for Network and Service Automation

A.6.1 Description

This scenario describes an approach of Federated Learning (FL) within management domain in the ZSM framework.

A.6.2 Rationale and Challenges

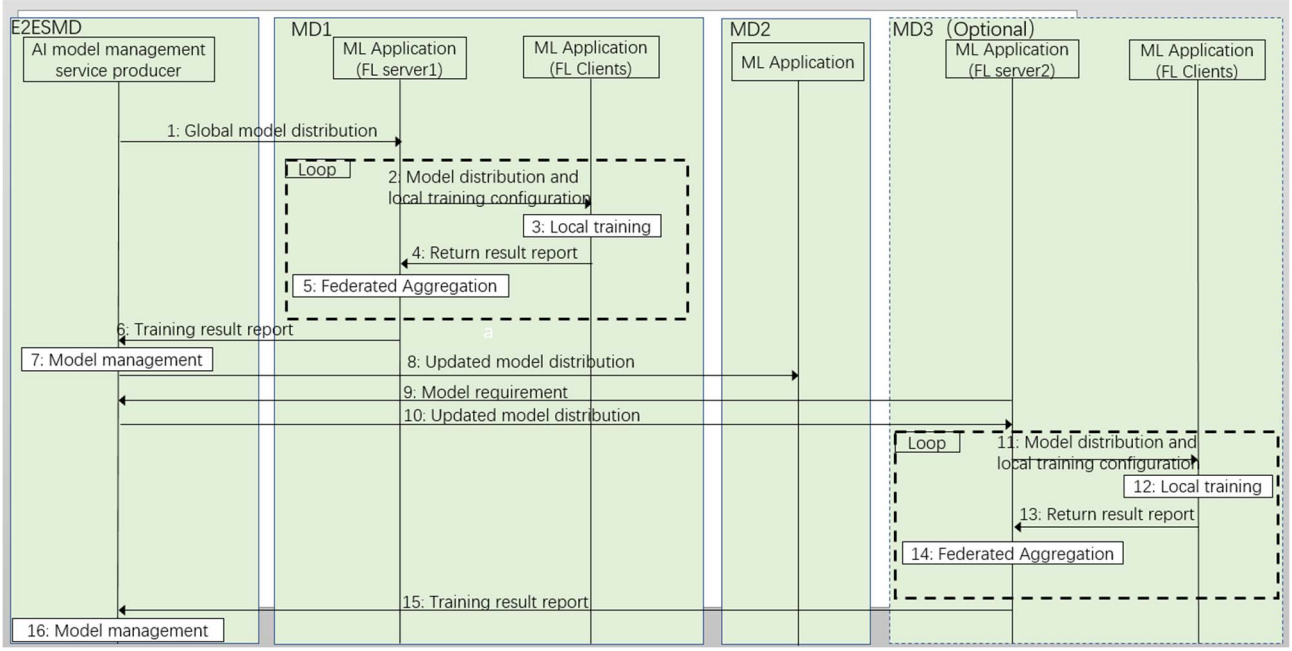
In order to achieve the cross-domain sharing problem, Decentralized Machine Learning (DML) services is introduced in clause A.2 of the present document.

In some cases, the FL Server (located in E2ESMD) and FL clients (located in MDs) need to communicate with each other many times to achieve a given target accuracy. This high communication load may be a bottleneck for the training process. In other cases, due to applicable privacy or security regulations it may happen that intermediate ML model or the model parameters update information cannot be shared outside of the MD. These need to be addressed in ZSM framework.

A.6.3 ZSM scenario details

The high-communication load and privacy/security challenges mentioned above can be resolved if a FL server function/application exists in the MD, and using the E2E AI model management service (as defined in clause 6.6.4.2.1 of ETSI GS ZSM 002 [2]) provided by E2ESMD to manage ML models used in the FL process.

The Federated learning process and knowledge sharing across MDs can be shown in Figure A.6.3-1. The AI model management service provides a global ML model instance to be trained locally within the management domain. After local training or retraining using training data generated by the AI training data management service (as defined in clause 6.5.4.2.3 of ETSI GS ZSM 002 [2]), the trained parameters will be fed back to the FL server for federated learning aggregation inside the management domain. In this case, the real-time decisions, e.g. event detection in the management domain can use the ML models with a very low latency. Meanwhile, the FL training result report can be sent to the E2ESMD. Finally, the AI model management service can make sure that FL servers in one management domain can take advantage of FL training results from other management domains.



NOTE 1: Step 1 and step 6 are optional. Accordingly, initial global model used in FL process may be created by E2ESMD based on knowledge from other MDs or not.

NOTE 2: The training result report contains trained model specification and/or its parameters together with training performance results.

Figure A.6.3-1: Federated Learning Workflow in ZSM framework

A.6.4 Related requirements for ZSM

Req-1: ZSM framework should support the capability to share and manage knowledge across management domains.

NOTE: In this scenario, knowledge represents FL training results shared by MDs with the E2ESMD and models provided by E2ESMD for FL process in MDs. The exact definition of knowledge is out of scope of the present document.

Annex B (informative): Terminology

Trustworthy Machine Learning: The proposed EU regulation for Machine Learning has put forward a set of seven key requirements that the Machine Learning systems should meet for them to be considered trustworthy. The details on each of those seven requirements are as follows (as described in [i.1]):

1) Human agency and oversight: AI systems should empower human beings, allowing them to make informed decisions and fostering their fundamental rights. At the same time, proper oversight mechanisms need to be ensured, which can be achieved through human-in-the-loop, human-on-the-loop, and human-in-command approaches.

2) Technical Robustness and safety: AI systems need to be resilient and secure. They need to be safe, ensuring a fallback plan in case something goes wrong, as well as being accurate, reliable, and reproducible. That is the only way to ensure that also unintentional harm can be minimized and prevented.

3) Privacy and data governance: Besides ensuring full respect for privacy and data protection, adequate data governance mechanisms also be ensured, taking into account the quality and integrity of the data, and ensuring legitimized access to data.

4) Transparency: The data, system and AI business models should be transparent. Traceability mechanisms can help achieving this. Moreover, AI systems and their decisions should be explained in a manner adapted to the stakeholder concerned. Humans need to be aware that they are interacting with an AI system, and should be informed of the system's capabilities and limitations.

5) Diversity, non-discrimination, and fairness: Unfair bias should be avoided, as it could have multiple negative implications, from the marginalization of vulnerable groups, to the exacerbation of prejudice and discrimination. Fostering diversity, AI systems should be accessible to all, regardless of any disability, and involve relevant stakeholders throughout their entire life circle.

6) Accountability: Mechanisms should be put in place to ensure responsibility and accountability for AI systems and their outcomes. Auditability, which enables the assessment of algorithms, data and design processes plays a key role therein, especially in critical applications. Moreover, adequate an accessible redress should be ensured.

7) Societal and environmental well-being: AI systems should benefit all human beings, including future generations. It should hence be ensured that they are sustainable and environmentally friendly. Moreover, they should consider the environment, including other living beings, and their social and societal impact should be carefully considered.

Annex C (informative): Analysis of ETSI GS ZSM 001

C.1 Methodology of analysis

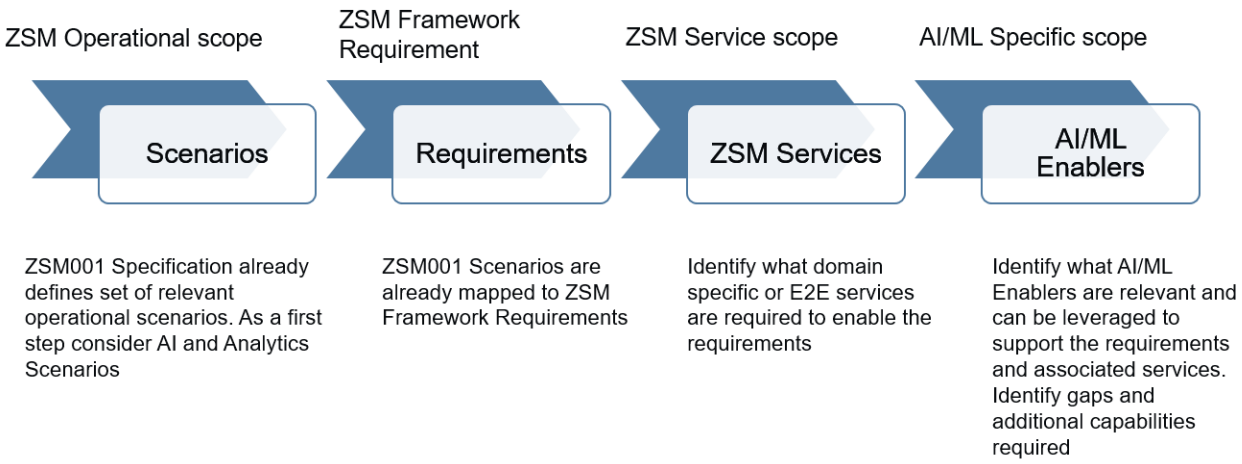


Figure C.1-1: Methodology of analysis

The methodology shown in Figure C.1-1 is intended for mapping existing operational scenarios in ETSI GS ZSM 001 [1] with AI/ML. Enabling areas highlighted as part of the present document. The requirements associated with these scenarios are already identified and documented in ETSI GS ZSM 001 [1].

Since ZSM follows a Service Based Architecture, it is critical to identify service impact before directly mapping to AI/ML enabling areas. The methodology investigates the potential services that can be associated with each of the requirements and analyses gaps in terms of enhancements required for services or additional capabilities that need to be scoped as part of the AI/ML enabling areas.

EXAMPLE: Clause 6.4 of ETSI GS ZSM 001 [1] covers the Analytics and Machine Learning Scenarios and associated requirements. Based on the proposed methodology a mapping of associated ZSM services are identified first and then AI/ML enabling areas related to the identified services are analysed based on the context of scenarios for the fitment and sufficiency of scope.

ETSI GS ZSM 001 [1] defines different groups of scenarios focusing on different topics. In the context of the present document the scenario group "Analytics and Machine Learning Scenarios" is of particular importance. However, not all the services are AI/ML relevant and associated requirements have been derived considering the AI/ML concepts. This group emphasizes the scenarios such as network predictive analytics, which drive the need for analytics, Machine Learning and AI capabilities in the ZSM framework. In order to enable such scenarios, the functional requirements such as collection of historical data, access to continuous up-to-date network data, etc. need to be fulfilled.

Due to the high relevance of this scenario group to the present document context, it is planned to apply the proposed methodology to the "Analytics and Machine Learning Scenarios". Apart from identifying the gaps in terms of enhancements required for services or additional capabilities that need to be scoped as part of the AI/ML enabling areas, it is planned to identify further (potentially missing requirements) for realizing the AI/ML scenarios.

C.2 Purpose of the analysis

The methodology defined above primarily serve following purposes:

- To identify the relevant operational scenarios, associated requirements, as well as further, potentially missing ZSM requirements, impacted ZSM services, as well as further, potentially missing ZSM services and how the AI/ML enabling areas may enhance or support those scenarios.

- To identify additional operational scenario and associated requirements that may be possible with the advent of AI/ML enabling areas.
- To identify the required enhancements in the services to support the AI/ML enabling areas.

EXAMPLE: AI or Data Operational requirements.

- To identify the gaps in the enabling areas such as Data, Action, Governance, Inter-AI, etc.

C.3 Example of mapping: ZSM Scenario - Requirements - Service - AI/ML enablers

Table C.3-1: ZSM Scenario-Requirements-Service-AI/ML enablers

ETSI GS ZSM 001 [1] Scenario	Requirements	ZSM Services	AI/ML enablers
Access to up-to-date telemetry data	Collect up-to-date telemetry data	Data Collection Data Services Data Analytics	Data Monitoring (for discrepancies in data) Policies (for Governance) AIOps (or a subset - say DataOps which manages Data pipelines)
	Common access to the collected up-to-date telemetry data		
	Enforcing a data governance scheme for the common access to telemetry data		
	Store telemetry data (or to steer their appropriate storage)		
	(Pre-)process and filter the telemetry data, and to perform cross-domain data aggregation		
	Check/validate the integrity of telemetry data		
	Manage the distribution of telemetry data, and keep distributed data consistent		
	Provide telemetry data to the data consumer according to the data consumer's requirements		

C.4 ETSI GS ZSM 001 AI/ML Scenarios: ZSM Scenario - Requirements - Service

Table C.4-1: ZSM scenario-Requirements-Service

ETSI GS ZSM 001 [1] Scenario	ZSM Requirements - ZSM framework should (support the capability to/for):	ZSM Services
Access to up-to-date telemetry data	1. Collect up-to-date telemetry data (such as performance data, KPIs, and alarms). 2. Common access to the collected up-to-date telemetry data, in a domain and cross-domain. 3. Enforcing a data governance scheme for the common access to telemetry data. 4. Store telemetry data (or to steer their appropriate storage). 5. Pre-process and filter the telemetry data, and perform cross-domain data aggregation. 6. Check/validate the integrity of telemetry data, e.g. of distributed data stores/replication. 7. Manage the distribution of telemetry data, keep distributed data consistent. 8. Provide telemetry data to the data consumer according to the data consumer's requirements.	Data Services Domain/E2E service Data collection

ETSI GS ZSM 001 [1] Scenario	ZSM Requirements - ZSM framework should (support the capability to/for):	ZSM Services
Machine learning for network & service automation	1. Support the management of composite services. 2. Support interfaces that facilitate the integration of Machine Learning-as-a Service frameworks into a zero-touch automation environment. 3. Allow for ways of measuring KPIs. 4. Support stepwise introduction of ML based management (allow mixed environment) of traditional and ML algorithms while the maturity of and confidence in ML assets increase. **Needed Requirements** 5. Allow for ways of measuring AI/ML specific KPIs (e.g. AI/ML training-inference performance KPIs). 6. Support Inter AI/ML interfaces that facilitate AI/ML specific information exchange (e.g. model parameter, model policy updates, AI/ML performance measurements, etc.). 7. Support mapping between AI/ML inference output and network/service/resource orchestration and control. 8. Support testing/training AI/ML models (SL, RL) in controlled testing environments (sandboxes) to enable online learning. 9. Support the possibility to switch back to non-AI/ML solution/service as a fall-back mechanism.	Data Services Domain/E2E service Data collection Domain/E2E service Intelligence Domain/E2E service Analytics **Needed Services/service Enhancements** **AI training data management services** Feature extraction and storage Data labelling and grouping **Deployed AI Model performance evaluation service** Root cause analysis for detected performance degradation from a supported list of causes (e.g. model drift, data bias, context change, etc.) **AI model management and orchestration services** E2E/Domain or Cross-Domain model aggregation (federation) Model selection services and Fall-back mechanisms Model updates and model parameter transfer **E2E service Orchestration** Orchestration and control based on AI inference outputs e.g. (AI recommendations to policy mapping) Sandboxing and AIML online learning services
Predictive analytics	1. Store historical data that is needed for the prediction and make it accessible to the analytics. 2. Introduce data analytics for predicting KPI changes and failure conditions. **Needed Requirements** 3. Prepare the data as input to training/inference according to the requirements of the AI/ML model.	Data Services Domain/E2E service Data collection Domain/E2E service Analytics **Needed Services/service Enhancements** **AI training data management services** Feature extraction and storage Data labelling and grouping

ETSI GS ZSM 001 [1] Scenario	ZSM Requirements - ZSM framework should (support the capability to/for):	ZSM Services
Real time monitoring and analysis	1. Set conditions (KPIs or policy conditions) that need to be monitored. 2. Monitor the state of the managed resources. 3. Detect undesired conditions and trigger appropriate actions. **Needed Requirements** 4. Clearly define supported appropriate actions in response to undesired conditions (e.g. of different types - command, recommendation- and granularity -on network resource, services, network area, entire network-).	Domain/E2E service Data collection Domain/E2E service Analytics Domain/E2E service Orchestration **Needed Services/service Enhancements** **E2E service Orchestration** Orchestration and control based on AI inference outputs e.g. (AI recommendations to policy mapping)
Proposal for analytics domains and concepts for interaction	1. Passive access to continuous up to date traffic in the network or service topology for an authorized consumer via relevant streaming APIs. 2. Provide the current logical and physical topology of a network and service for an authorized consumer within ZSM framework. 3. Support the ability for the authorized consumer within a management domain to relay a specific request for telemetry, trace or traffic to another management domain. Responding management domain should be able to decline requests for telemetry, trace or traffic based on policy, security, operational or other considerations. 4. Support capabilities to evaluate and report the QoS of a network or a service over either a specific duration of time or continuously over the service usage in near-real-time. 5. Identify the root cause of a network or service degradation. The root cause provided should be deterministic. 6. Evaluate and report the QoE of a service or a network service over either a specific duration of time or continuously over the service usage. **Needed Requirements** 7. Support capabilities to evaluate and report AI/ML model QoS on average or per model/version, over a specific duration of time or continuously over the AI/ML solution usage in near-real-time. 8. Identify the root cause of an AI/ML solution/ service performance degradation. The root cause provided should be deterministic.	Data Services Domain/E2E service Data collection Domain/E2E service Analytics Domain/E2E service Control **Needed Services/service Enhancements** **Deployed AI Model performance evaluation service** Root cause analysis for detected performance degradation from a supported list of causes (e.g. model drift, data bias, context change, etc.)

ETSI GS ZSM 001 [1] Scenario	ZSM Requirements - ZSM framework should (support the capability to/for):	ZSM Services
AI for network and service automation	1. Collection of data from all managed entities that are necessary to perform automated network and service management based on AI. 2. Ensure that data is available not only inside management domains but also outside them so that such data can be available to any authorized consumer belonging to one operator. **Needed Requirements** 3. Prepare the data as input to training/inference according to the requirements of the AI/ML model. 4. Support Inter AI/ML interfaces that facilitate AI/ML specific information exchange (e.g. model parameter, model policy updates, AI/ML performance measurements, etc.).	Data Services Domain/E2E service Data collection Domain/E2E service Analytics Domain/E2E service Control **Needed Services/service Enhancements** **AI training data management services** Feature extraction and storage Data labelling and grouping **Deployed AI Model performance evaluation service** Root cause analysis for detected performance degradation from a supported list of causes (e.g. model drift, data bias, context change, etc.) **AI model management and orchestration services** E2E/Domain or Cross-Domain model aggregation (federation) Model selection services and Fall-back mechanisms Model updates and model parameter transfer
CI/CD for ZSM framework functional components	1. Capability to make ZSM framework functional components as managed entities that can be deployed independently. 2. Capability to change and upgrade functional components of ZSM framework without impacting other functional components and ZSM services. 3. Capability for automated lifecycle management of ZSM framework functional components. 4. Interoperation between DevOps and operator CI/CD systems. 5. Functional components of ZSM framework should be reusable and interchangeable.	Domain/E2E service Data collection Domain/E2E service Analytics Domain/E2E service Orchestration Domain/E2E service Control
Zero-touch self-optimizing network	1. Support the use of automated decision loops, with different characteristics and scope, as a means to perform network and service management. 2. Provide an interface for the purpose of bringing decision criteria to the decision loops, i.e. triggers, policies. 3. Hinder an overarching loop from infringing on a more local loop's responsibility. Exceptions from this rule should be possible based on operator preferences. 4. Enable the collection of all relevant and available data, and the corresponding context information, needed by a specific decision loop. 5. Evaluate the network resources needed to enable the collection of data for each decision loop. 6. Enable monitoring of the effects of automation functions to build trust in every stage of increased automation towards a fully automated solution. 7. Enable the network owner to disable any automation function in case of malfunction.	Data services Domain/E2E service Data collection Domain/E2E service Analytics Domain/E2E service Control

ETSI GS ZSM 001 [1] Scenario	ZSM Requirements - ZSM framework should (support the capability to/for):	ZSM Services
Self-learning based on reinforcement learning	1. Provide access to operational and historical data to authorized consumers. 2. Allow the creation and execution of ML sand-box environments where self-learning algorithms can get access and use data. 3. Provide means to store self-learning software's knowledge in a persistent manner.	Data services Domain/E2E service Data collection Domain/E2E service Intelligence Domain/E2E service Analytics Domain/E2E service Control
Optimization of supervised/unsupervised learning used in management services for closed loop	1. Support the capability of collecting and storing data obtained in both training phase and operation phase such as performance, log, alarm, topology, trouble information. 2. Support the capability of exposing the stored data set obtained in training/operation phase to ML used in management services to enhance the accuracy of ML based on these data. **Needed Requirements** 3. Prepare the data as input to training/inference according to the requirements of the AI/ML model 4. Support Inter AI/ML interfaces that facilitate AI/ML specific information exchange (e.g. model parameter, model policy updates, AI/ML performance measurements, etc.).	Data services Domain/E2E service Data collection Domain/E2E service Intelligence Domain/E2E service Analytics Domain/E2E service Orchestration Domain/E2E service Control **Needed Services/service Enhancements** **AI training data management services** Feature extraction and storage Data labelling and grouping **Deployed AI Model performance evaluation service** Root cause analysis for detected performance degradation from a supported list of causes (e.g. model drift, data bias, context change, etc.) **AI model management and orchestration services** E2E/Domain or Cross-Domain model aggregation (federation) Model selection services and Fall-back mechanisms Model updates and model parameter transfer **E2E service Orchestration** Orchestration and control based on AI inference outputs e.g. (AI recommendations to policy mapping)

Annex D (informative): Bibliography

- ETSI GS ZSM 007: "Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM".
- Ji, Zhanglong, Zachary C. Lipton, and Charles Elkan: "Differential privacy and machine learning: a survey and review". arXiv preprint arXiv:1412.7584 (2014).

Annex E (informative): Change History

Date	Version	Information about changes
02-2021	0.0.1	Approval of work item skeleton
02-2021	0.0.2	Inclusion of informative annexes on i) Terminology, ii) Analysis of ZSM001 and iii) Analysis of ZSM002
11-2021	0.0.3	Incorporated contributions: -ZSM(21)000179_ ZSM012 - Analysis of ETSI ZSM GS 001
12-2021	0.0.4	Incorporated contributions: - ZSM(21)000234r3_ZSM012___Further_Analysis_of_ETSI_ZSM_GS_001 - ZSM(21)000396_ZSM012_Terminology_for_Trustworthy_Machine_Learning - ZSM(21)000387_ZSM012_Section_5_2_Enabling_Area_Execution - ZSM(21)000391_ZSM012_Section_5_6_Enabling_Area_Governance
01-2022	0.0.5	Incorporated contributions: -ZSM(21)000390r1_ZSM012_Section_5_5_Enabling_Area_Action -ZSM(21)000430r1_ZSM012_Annex_A3_AI_ML_model_validation_and_model_monitoring -ZSM(21)000429r1_ZSM012_Annex_A2_Decentralized_ML_for_Network_and_Service_Aut -ZSM(21)000388r2_ZSM012_Section_5_3_Enabling_Area_Data -ZSM(21)000389r2_ZSM012_Section_5_4_Enabling_Area_Inter_AI -ZSM(21)000395r2_ZSM012_Annex_A1_Trustworthy_ML_for_Network_and_Service_autom -ZSM(21)000437r1_ZSM012_Annex_A4_Anomaly_Management_using_AI_ML_based_closed
04-2022	0.0.6	Incorporated contributions: - ZSM(22)000045r2_ZSM012_Sec_5_6_3_1_ML_Data_Trust_Management_Service - ZSM(22)000046r2_ZSM012_Sec_5_6_3_2_ML_Data_Trust_Evaluation_Service - ZSM(22)000048r2_ZSM012_Sec_5_6_3_4_ML_Model_Trust_Evaluation_Service - ZSM(22)000049r2_ZSM012_Sec_5_7_1_ML_Events_Notification_Service - ZSM(22)000050r2_ZSM012_Sec_5_7_2_ML_Log_Collection_Service - ZSM(22)000066r5_ZSM012_Annex_A_1_3_ZSM_scenario_details - ZSM(22)000090_ZSM012_Sec_5_7_4_ML_Data_Processing_Service - ZSM(22)000091r1_ZSM012_Sec_5_7_5_ML_Training_Reporting_Service - ZSM(22)000092_ZSM012_Sec_5_3_3_1_ML_model_validation_service - ZSM(22)000094r1_ZSM012_Sec_5_4_3_5_4_3_1_FL_configuration_service - ZSM(22)000129_ZSM012_Sec_5_7_3_ML_Feasibility_Check_Service
05-2022	0.0.7	Incorporated contributions: - ZSM(22)000047r4_ZSM012_Sec_5_6_3_3_ML_Model_Trust_Management_Service - ZSM(22)000153_ZSM012_5_6_3_1_5_6_3_3_Additional_examples - ZSM(22)000167_ZSM012_change_section_numbering - ZSM(22)000170_ZSM012_adding_examples_to_Sec_5_7_4 - ZSM(22)000073r1 ZSM012_Annex_A5_ML_Model_modular_cooperation - ZSM(22)000169r1_ZSM012_Sec_5_2_3_2_Sandbox_Configuration_Service - ZSM(22)000171r1_ZSM012_Security_related_description
06-2022	0.0.8	Updated ToC Incorporated contributions: - ZSM(22)000204_ZSM012_sec_5_6_1_Security_description_update - ZSM(22)000205_ZSM012_Sec_5_6_3_3_update_for_model_cooperation - ZSM(22)000172r2_ZSM012_Sec_5_6_3_5_ML_Fallback_management_service - ZSM(22)000115r4_ZSM012_Changing_section_5_4_Inter_AI
07-2022	0.0.9	Incorporated contributions: - ZSM(22)000206r2_ZSM012_Sec_5_7_6_ML_model_cooperation_management_service - ZSM(22)000231_ZSM012_Sec_5_7_3_update_Feasibility_service_capability - ZSM(22)000232_ZSM012_5_7_1_update_Event_Notification_Service_capability - ZSM(22)000251_ZSM012_Resolving_Editors_note_Sec_3_1 - ZSM(22)000256_ZSM012_Resolving_Editors_note_Chapter_5 - ZSM(22)000258_ZSM012_Resolving_Editors_note_Annex_A - ZSM(22)000259_ZSM012_Resolving_Editors_note_Annex_B - ZSM(22)000260_ZSM012_Resolving_Editors_note_Annex_C - ZSM(22)000261_ZSM012_Resolving_Editors_note_Annex_D
08-2022	0.1.0	Incorporated contributions: - ZSM(22)000267_ZSM012_Resolving_Editors_note_Sec_4 - ZSM(22)000268_ZSM012_Resolving_Editors_note_Annex_D_3_1_D_3_2 - ZSM(22)000272r1_ZSM012_Resolving_Editors_note_Introduction - ZSM(22)000273r1_ZSM012_Resolving_Editors_note_Sec_1_Scope - ZSM(22)000309r1_ZSM012_update_5_6_1 - ZSM(22)000233_ZSM012_Sec_5_1_Overview - ZSM(22)000257_ZSM012_Resolving_Editors_note_Sec_5_6_3_1
10-2022	0.1.1	Incorporated contributions: - ZSM(22)000358r1_ZSM012_Changing_Transfer_to_Share_in_section_4_4_2 - ZSM(22)000334r4_ZSM12_Adding_Annex_A_6_FL_Scenario
11-2022	0.1.2	Editorial changes Incorporating contributions: - ZSM(22)000373 - ZSM012 review comments

History

Document history		
V1.1.1	December 2022	Publication