ETSI GS ENI 002 V3.1.1 (2020-12)

Experiential Networked Intelligence (ENI); ENI requirements

Disclaimer

The present document has been produced and approved by the Experiential Networked Intelligence (ENI) 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
RGS/ENI-0015

Keywords
artificial intelligence, management, network, requirements

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Experiential Networked Intelligence (ENI).

Modal verbs terminology

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

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

1 Scope

The present document captures the requirements of how intelligence is applied to the network and applications in different scenarios to improve experience of service provision and network operation. Also, how intelligence enables dynamic autonomous behaviour and adaptive policy driven operation in a changing context. The ENI requirements are based on the ENI use case document and identified requirements from other SDOs. These requirements will form the base for the architecture design work.

The present document includes:

- Requirements derived from API descriptions
- Requirements derived from System Architecture
- Requirements derived from new use cases

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.

Not applicable.

2.2 Informative references

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

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

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

[i.1] ETSI GR ENI 001: "Experiential Networked Intelligence (ENI); ENI use cases".

[i.2] ETSI TS 102 165-1 (V5.2.3): "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.3] ETSI GR ENI 004: "Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI".

[i.4] ETSI GS NFV-MAN 001 (V1.1.1): "Network Functions Virtualisation (NFV); Management and Orchestration".

[i.5] Service Operations Specification MEF 55: "Lifecycle Service Orchestration (LSO): Reference Architecture and Framework".

[i.6] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.7] ETSI GR ENI 003: "Experiential Networked Intelligence (ENI); Context-Aware Policy Management Gap Analysis".

[i.8] ETSI TS 101 158: "Telecommunications security; Lawful Interception (LI); Requirements for network functions".

[i.9] ETSI GS ENI 005: "Experiential Networked Intelligence (ENI); System Architecture".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR ENI 004 [i.3] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

AI	Artificial Intelligence
API	Application Programming Interface
BP	Back Propagation
CAP	Context Aware related Policy
CAPEX	CAPital EXpenditure
DC	Data Collection

NOTE: Used in the context of servers.

DCA	Data Collection and Analysis
DSL	Domain-Specific Language
EMS	Element Management System
ENI	Experiential Networked Intelligence
GDPR	General Data Protection Regulation
GPM	General Policy Management
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
LI	Lawful Interception
LSO RA	Lifecycle Service Orchestration - Reference Architecture
LSO	Lifecycle Service Orchestration
MANO	MANagement and Orchestration
MEC	Multi-access Edge Computing
MEF	Metro Ethernet Forum
MOP	Mode Of Operations
NFV	Network Functions Virtualisation
NPD	Network Planning & Deployment
OPEX	OPerational EXpenditure
OR	Operational Requirements
PR	Performance Requirements
RA	Reference Architecture

RR	Resilience and Reliability
SDN	Software Defined Networking
SLA	Service Level Agreement
SOM	Service Orchestration and Management
SP	Security and Privacy
SP.2A	Security and Privacy 2A
SP.2B	Security and Privacy 2B
SVM	Support Vector Machine
TCO	Total Cost of Ownership
TVRA	Threat, Vulnerability and Risk Analysis
VNF	Virtualised Network Function
WAN	Wide-Area Network

4 Introduction

4.1 Categorization of the requirements

The present document structure addresses the requirements in the following areas:

1) Service and network requirements:
   - General requirements
   - Service orchestration and management
   - Network planning and deployment
   - Network optimization
   - Resilience and reliability
   - Security and privacy
2) Functional requirements:
   - Data collection and analysis
   - Policy management
   - Data learning
   - Interworking with other systems
   - Mode of operations
   - Model training and iterative optimization
   - API requirements
3) Non-functional requirements:
   - Performance requirements
   - Operational requirements
   - Regulatory requirements

5 Service and network requirements

5.1 Overview

The requirements in this clause are addressed from service and network point of view and are derived directly from the related use cases.

5.2 General requirements

This clause captures the requirements that are general and independent from other requirements categorized in other specific clauses.

[GR.1] The ENI framework shall use history data, context, and decisions taken to learn, process and provide responses to events, whether generated from devices or from management systems.

[GR.2] The ENI framework shall use context information as part of the computations that result in recommendations, advisement, predictions, and decisions that are used to assist other network systems, e.g. orchestration and management systems.

NOTE: As an example, MANO (from ETSI GS NFV-MAN 001 [i.4]) or the LSO RA (from MEF [i.5]) are different types of orchestration and management systems.

[GR.3] The ENI architecture shall be flexible enough to support extensibility.

5.3 Service orchestration and management

This clause captures requirements related to the ENI framework service provisioning, e.g. how to compile the service intent and orchestrate the service atoms and work flows, as well as automatic service on boarding.

[SOM.1] The ENI framework shall invoke policies based on models that describe and/or define traffic behaviour, such as SLAs (e.g. past or current telemetry).

[SOM.2] The ENI framework shall support the closed loop control model when different orchestration and management systems are used.

NOTE 1: As an example, MANO (from ETSI GS NFV-MAN 001 [i.4]) and LSO RA (from MEF [i.5]) are different types of orchestration and management systems.

[SOM.3] The ENI framework should not directly manage, control or orchestrate physical or virtual entities, either at the infrastructure level or service level.

NOTE 2: ENI framework may interact with the Orchestration system, EMS or OSS/BSS to influence the state of the resources or services.

5.4 Network planning and deployment

This clause captures requirements related to network planning and deployment, e.g. how to allocate network resources to VNFs, or automatic VNF on boarding.

NOTE 1: The network resources that can be managed are not limited to the requirements addressed in this clause.

[NPD.1] The ENI framework shall recommend allocation or retrieval of network resources, e.g. virtual machines, bandwidth, IPv4 addresses and IPv6 prefixes to end users or service flows, in an intelligent way to improve the efficiency of resource utilization. This ENI framework function may be implemented in a centralized and/or distributed manner, according to what is defined in ETSI GR ENI 004 [i.3] and according to ETSI GS ENI 005 [i.9].

[NPD.2] The ENI framework shall assist the network equipment to use the resource pools that are used for resource allocation (e.g. virtual machines, bandwidth, IP addresses), in an intelligent way in order to improve the efficiency of resource utilization.

[NPD.3] The ENI framework should dynamically and intelligently compute and recommend the required network resources, including both IPv4 and IPv6 resources as well as other resources.

[NPD.4] The ENI framework shall compute the network resources required to dynamically and intelligently deploy a given network service efficiently.

[NPD.5] IT resources to enable network services shall be managed within the ENI framework.

NOTE 2: Similar capabilities within the data centre are outside the network scope of this phase of ENI.

[NPD.6] The ENI framework shall be capable of understanding the context that a set of devices is operating within.

[NPD.7] The ENI framework shall be capable of performing the proper planning and deployment of resources to ensure that applicable deployed policies are not violated.

[NPD.8] The ENI System shall identify different types of rollouts for different types of resources that lead to the upgrade of virtualised software-based resources.

[NPD.9] The ENI System shall, in an efficient and dynamic manner, combine network slices, slice/service prioritization and resource allocation concepts, e.g. in order to resolve resource allocation conflicts between competing network slices deployed on top of a shared infrastructure.

5.5 Network optimization

This clause captures requirements related to network optimization, e.g. how to adjust the network configurations to improve its efficiency and performance, as well as the user experience of the service.

[NO.1] The ENI framework shall collect and process the necessary data according to specific algorithms in order to achieve network optimization.

NOTE: Data collection and processing algorithms for systems will be specified in the functional architecture.

[NO.2] The ENI framework shall meet or exceed all performance requirements when improving the target performance.

[NO.3] The ENI framework shall support central optimization, local optimization and distributed joint optimization, according to what is defined in ETSI GR ENI 004 [i.3].

[NO.4] The ENI framework shall support an adaptive optimization process where changes in the environment are reflected in the results of the optimization.

[NO.5] The ENI framework shall use prioritization and other scheduling and traffic shaping techniques to prevent SLA violations related with priority services.

[NO.6] The ENI framework shall use AI (e.g. Machine Learning) to identify traffic type and support traffic handling and QoS assurance for specific type of traffic.

[NO.7] The ENI framework shall support traffic type identification in different granularity levels, including application types, action types (e.g. sending pictures, voice calls, etc.).

[NO.8] The ENI framework shall support dynamic policy adjustment for a specific flow based on traffic identification results.

5.6 Resilience and reliability

This clause captures requirements related to resilience and reliability of the network, including fault diagnosis and prediction, high availability and back up, conflict detection, and rolling back to previous policies and status.

[RR.1] The ENI framework shall intelligently recommend allocation or retrieval of IP addresses without causing route oscillation.

[RR.2] The ENI framework shall intelligently recommend allocation or retrieval of IP addresses without causing any interruption in the offered services.

[RR.3] The ENI framework shall support root cause analysis to diagnose existent faults and potential faults caused by new cases, according to what is defined in ETSI GS ENI 005 [i.9].

[RR.4] The ENI framework shall support the use of one or more AI algorithms to perform network service fault prediction.

[RR.5] The ENI framework shall learn and predict the pattern of resource requirements of services.

[RR.6] When optimization of energy consumption is required, which implies a switch of servers, the ENI framework shall trigger the reallocation of services to appropriate resources in another server.

[RR.7] The ENI framework shall wake up an appropriate number of servers in time to meet the growing resource needs required by services, after learning and predicting the pattern of resource requirement of those services.

[RR.8] The ENI framework shall provide the operators with the ability to define services that are critical or prioritized.

[RR.9] The ENI framework shall allow the on-going services in a server to be moved from this server to another without interruption, e.g. during reallocation for energy saving purposes.

[RR.10] The ENI framework shall not interrupt the on-going services on the target servers, e.g. when reallocation of services from other servers takes place for energy saving purposes.

[RR.11] Energy saving need not be the only criterion for moving a service.

[RR.12] The ENI system shall calculate and propose proper backup actions to the operators in order to prevent or to mitigate a service degradation or disruption when a planned operation occurs.

[RR.13] The ENI framework shall support the use of one or more intelligent methods to perform network anomaly (fault, error and unusual behaviour) prediction and prevention.

[RR.14] The ENI framework shall be aware of the impact of adjustment on services and guarantee seamless adjustment of network slice and high valued services.

5.7 Security and privacy

This clause captures requirements related to security and privacy issues (e.g. it is recommended that data collection shall be captured in a secure way and not add more security risks). In addition, it is recommended that the collected data shall be accessible by authorized accounts, and that the privacy of both subscribers and operators are protected.

The requirements indicated in the present document have been derived from application of the ETSI TVRA method defined in ETSI TS 102 165-1 [i.2], the details of the analysis leading to the requirements have been examined with respect to the use cases defined in ETSI GR ENI 001 [i.1] and with respect to the terminology defined in ETSI GR ENI 004 [i.3].

[SP.1] The ENI framework shall use AI (e.g. Machine Learning) to detect abnormal traffic patterns that can lead to service disruptions or security threats as well as to carry out the identification of abnormally operating devices.

[SP.2] The ENI framework shall provide means to detect a corrupted device.

[SP.2A] The ENI framework shall provide means to identify a corrupted device.

[SP.2B] The ENI framework shall provide means to isolate and remove a corrupted device from the system.

[SP.3] The ENI framework should provide means to indicate to authorized parties the occurrence of potential and confirmed security threats by using appropriate mechanisms, (e.g. via dedicated interfaces).

[SP.4] The ENI framework shall provide means to invoke policies to isolate threats.

[SP.5] The ENI framework shall be designed in such a way that it complies to the provisions of the GDPR [i.6], when processing of data (traffic or signalling).

[SP.6] The ENI framework shall allow entities that are involved in services that are subject to LI processing to be designed in such a manner that they comply with the general provisions of LI as defined in ETSI TS 101 158 [i.8].

[SP.7] Processing for security functions should always be enabled.

[SP.8] The addition of any processing in the ENI framework to comply with provisions arising from LI compliance shall not be visible to an external observer.

NOTE: The consequence of the above is that an external observer should not assert that an LI operation is taking place by observation of the processing load of the ENI framework.

6 Functional requirements

6.1 Overview

The requirements in this clause are addressed from the architecture point of view.

6.2 Data collection and analysis

This clause captures requirements related to how data is collected and analysed by the ENI framework.

[DCA.1] The ENI framework shall gather network status data (e.g. related to connection or routing protocols in use) as well as network operational, administrative, and state information (e.g. network configuration).

[DCA.2] The ENI framework shall store the data either as raw data or aggregated data for further analysis, according to what is defined in ETSI GR ENI 004 [i.3].

[DCA.3] The ENI framework shall provide data analysis functionalities, which make use of collected data in order to produce intermediate information that will support further analysis.

NOTE 1: Examples of information related to this requirement include network context information (such as time of the day, device/link state, and location of users).

[DCA.4] The ENI framework shall collect and analyse the necessary data in order to determine traffic patterns.

NOTE 2: This requirement can be governed by national and international regulations on Data Protection and Privacy.

[DCA.5] The ENI framework shall collect information from the infrastructure.

[DCA.6] The ENI framework shall collect and store the history data to be used for e.g. further analysis, learning process, etc.

[DCA.7] The ENI framework shall collect and store required run-time data in order to e.g. determine the policy.

[DCA.8] The ENI framework shall provide data collection methods for network KPI status data (e.g. packet loss rate, latency, throughput) in different granularities (e.g. physical interface, logical interface, flow).

[DCA.9] The ENI framework may perform analysis on the combination of data, collected from various relevant infrastructure elements, to generate an overall view of network status.

[DCA.10] The ENI framework shall be capable of requesting or retrieving certain kind of data from the assisted system.

[DCA.11] The ENI framework shall be capable of extracting configuration information from the collected data to generate policies intelligently (e.g. avoiding adjust DC servers that are unavailable or inaccessible).

[DCA.12] The ENI framework shall automatically assign labels to new samples.

6.3 Policy management

6.3.1 General policy management requirements

This clause captures requirements related to how policies are managed by the ENI framework.

The ENI system enforces policies. Policies should be used to constrain the operation of the assisted system. The actions may be either a set of commands or recommendations, depending on the role that the ENI system is playing. The ENI system may use any combination of imperative, declarative and intent policies to form the actions, see ETSI GR ENI 004 [i.3].

[GPM.1] The ENI framework should be constrained by predefined policies when a decision is being made.

NOTE: If a policy states that the requirement of higher priority users is to be satisfied first, the ENI framework will first output the decision to allocate sufficient resources to fulfil the requirement of those higher priority users. Consequently, it is possible that the requirements of the lower priority users are not satisfied. However, if another policy states that all users are able to be served when resources are sufficient and available, the ENI framework attempt to allocate resources to serve lower priority users after sufficient resources have been allocated for higher priority users.

[GPM.2] The ENI framework shall use policies that are triggered by one or more events.

[GPM.3] When an event indicates that a policy violation is detected, the ENI framework shall perform appropriate actions.

[GPM.4] The ENI framework shall be capable of performing policy conflict resolution in order to guarantee the integrity of Infrastructure and/or Services.

[GPM.5] The ENI system shall use policies intelligently according to enterprise needs, such as cost priority, quality priority, cost-effective priority, or the needs demanded by enterprise communications applications as a result of the customization of communication service level assurance.

[GPM.6] The ENI system shall use WAN policies intelligently when identifying and managing diverse WAN traffic.

[GPM.7] The ENI system shall detect changing conditions in the network and adapt WAN traffic routing through intelligent WAN policies.

[GPM.8] The ENI system shall use policies to modify the assisted system, such as make environmental adjustments of the DC servers.

6.3.2 Context aware related policy requirements

This clause captures policy related functional requirements defined in ETSI GR ENI 003 [i.7].

[CAP.1] A single information model shall be used to represent the structure and semantics of policies. Multiple information models shall not be used.

[CAP.2] Multiple data models may be derived from the (single) information model.

[CAP.3] The Policy information model shall be integrated into the system's information model. This facilitates relating policies to Services, Resources, Functional Blocks, and other managed entities of the system.

[CAP.4] The information model shall be used in constructing APIs and DSLs.

[CAP.5] Different types of Policies shall be supported in the same system.

[CAP.6] Policy within a domain shall act as a mechanism to define and manage the behaviour of entities contained within that domain. This includes entities in a sub-domain contained in a higher-level domain.

[CAP.7] Policy defined in peer domains may act as a mechanism to negotiate mutually acceptable behaviour between the domains.

[CAP.8] Context shall be used to select active policies (and deactivate policies that are no longer appropriate). This enables the ENI system to adjust its goals and behaviours accordingly to changes in context.

[CAP.9] The ENI system, based on contextual changes, may construct new policies to address problems found and/or improve system behaviour by using operator intervention if no suitable policies currently exist.

NOTE: According to what is defined in ETSI GR ENI 004 [i.3], a policy may be cloned and modified by an applicable functional block, such as policy engine (as opposed to the policy itself being self-modified). The changes allowed by this process will be limited according to parameters defined in the ENI architecture. Self-modifying policies are still in the early research stage; in this stage of ENI, self-modifying policies are not specified.

[CAP.10] Policy shall be augmented by metadata and shall be used to describe and prescribe functionality.

[CAP.11] Policy shall be realized by using centralized and/or distributed architectures, according to what is defined in ETSI GR ENI 004 [i.3].

[CAP.12] The (single) information model, and each data model, should use a set of software design patterns to provide extensibility and consistency.

[CAP.13] The derivation of a data model should be done by defining formal transformations from the (single) information model to each different data model. This facilitates the development of associated software tooling.

[CAP.14] Different actors may be represented by different roles, and shall be mapped to different levels in the Policy Continuum.

[CAP.15] Different actors have different concepts and terminologies for their policies. Therefore, the notion of a Policy Continuum, where each continuum corresponds to a given set of actors, should be realized.

[CAP.16] Formal mathematical transformations between each level of the Policy Continuum and its actors shall be defined, which facilitates the development of APIs and DSLs.

[CAP.17] Actors operate in a context. Context may change throughout the lifecycle of the system. Therefore, the context of an actor may be used to map the activities of the actor to a particular level in the Policy Continuum.

[CAP.18] The ENI system may use historical data about contextual changes along with other collected data to perform analysis and generate policies.

6.4 Data learning

This clause captures requirements related to data learning in ENI framework.

[DL.1] The ENI framework shall provide basic data learning functionalities, such as classification, regression, and clustering.

NOTE: The ENI framework may contain common algorithms to support these functionalities, such as SVM for classification, BP for regression and K-Means for clustering.

[DL.2] The ENI framework shall provide feature analysis functionalities, which can rank all features of the data in the order of their importance and provide suggestions to operators for their further feature weighting.

[DL.3] The ENI framework shall provide big data mining and analysis functionalities, which can find the hidden patterns, correlations and knowledge and reveal the relationship between correlation rules and events through mining and analysing large amounts of data.

6.5 Interworking with other systems

This clause captures requirements related to how the ENI framework interworks with other systems.

[IWOS.1] The ENI framework shall interwork with other systems, e.g. NFV, MEC, SDN, MEF LSO, and others that may show up in a 5G-Network context, by reusing existing functions and interfaces as much as possible.

[IWOS.2] The failure of ENI framework shall not interrupt the services provided by other systems.

6.6 Mode of operations

This clause captures requirements on the mode of operations of the ENI framework.

[MOP.1] The ENI system shall support a recommendation mode and may support a management mode of operation or a mixed mode where different mode is used for different sets of decisions.

[MOP.2] Regulatory policies and operator goals inputs should be used by ENI to control the ENI modes of operation.

[MOP.3] The ENI system shall discover the assisted system capabilities in supporting the desired mode and associated Reference Points, consider the regulatory policies and operator goals input and make decisions on its mode of operation, according to the current and future situations of the assisted system, underlying network and their contexts.

[MOP.4] The ENI system, when decides to operate on a mode that is different from the previous mode, shall switch the mode of operation, if that resulting mode is supported by the ENI and the assisted system.

[MOP.5] The ENI system, when decides to operate on a mode that is different from the previous mode, shall interact with the assisted system, e.g. to inform its decision on the change of mode of operations.

[MOP. 6] The ENI System shall support and adapt to external inputs for each mode of operation:

- [MOP.6A] The ENI System shall support and adapt to changes in the context and/or situation of the Assisted System.
- [MOP.6B] The ENI System shall support external input of regulatory policies and operator goals.

[MOP.7] The ENI System shall use the above two factors in [MOP.6] to select its mode of operation.

[MOP.8] The ENI System shall ask permission from the Operator or Designated Entity, to change modes of operation. This shall be done using an agreed Reference Point.

[MOP.9] The Assisted System, or its Designated Entity, shall ask the ENI System to change modes of operation. This shall be done using an agreed Reference Point.

[MOP.10] The ENI System shall confirm through the agreed Reference Point to the Operator or Designated Entity of the Assisted System when it has successfully switched modes of operation.

[MOP.11] The ENI System may suggest that a particular mode of operation is used when a class of decision is reached that is not specified by the Assisted System.

[MOP.12] The Assisted System and/or its Designated Entity need not accept the recommendations offered by ENI when in recommendation mode. This includes those decisions that apply to recommendations when the Assisted System is in a mixed mode of operation.

[MOP.13] The Assisted System and/or its Designated Entity need not accept the recommendations offered by ENI when in management mode. This includes those decisions that apply to commands when the Assisted System is in a mixed mode of operation.

[MOP.14] Decisions and commands in management mode are subject to the approval of the Assisted System (or its Designated Entity).

NOTE: If the Assisted System has chosen management mode, it (or its Designated Entity) still has the ability to reject commands sent to it by the ENI System.

[MOP.15] If the Assisted System (or its Designated Entity) rejects a command set to it by the ENI System when it is in management mode, it shall send a notification to the ENI System.

6.7 Model training and iterative optimization

[MTIO.1] The ENI framework shall be able to support the selected algorithms according to the types of problems, e.g. classification, regression, etc., and support the initialization of model parameters and structure based on data features and task objectives.

[MTIO.2] The ENI framework shall support the ability to adjust a model's hyperparameters or choose a new model.

[MTIO.3] The ENI framework shall re-train the model using various learning techniques and algorithms through continuously extending the existing model's knowledge according to input data.

NOTE: Learning techniques may include Online Learning and Offline Learning techniques: including, Incremental Learning, Transfer Learning with their associated algorithms, etc.

[MTIO.4] The ENI framework may solve related problems based on knowledge gained while solving one or more previous problems.

6.8 Mode of deployments

[MOD.1] The ENI system shall support centralized deployment and distributed deployment.

[MOD.2] Information exchange shall be supported between distributed ENI systems located in the same network domain.

[MOD.3] Information exchange shall be supported between distributed ENI systems located in different network domains.

[MOD.4] Information exchange shall be supported between distributed ENI systems and one or more centralized ENI systems.

6.9 API requirements

[API.1] The ENI system shall support API based programming mode.

NOTE 1: If [API.1] is used then the following corollaries follow:

[API.1a] The ENI system shall provide a set of common APIs in driver level to support AI development across a range of data parallel accelerators.

[API.1b] The ENI system shall provide a set of APIs to support AI development across different AI frameworks.

[API.1c] The ENI system shall reuse the APIs provided by an existing external system as external ENI APIs, if these APIs can meet the requirement of interworking between ENI system and the external system.

[API.2] The ENI system should support direct programming mode if the API based programming mode cannot meet the required needs.

NOTE 2: [API.1] & [API.2] can be used in combination.

NOTE 3: API based programming mode is the way that programmers produce code to achieve particular function by calling existing APIs. Direct programming mode is the way that the programmers use programming language to produce code to achieve particular function without calling existing APIs.

[API.3] The ENI system shall be able to communicate with external systems by a single set of ENI APIs directly or via an optional API Broker.

7 Non-functional requirements

7.1 Overview

The requirements in this clause are addressed from non-functional point of view.

7.2 Performance requirements

This clause captures requirements related to system performance, e.g. latency, accuracy, efficiency.

[PR.1] The ENI framework shall be capable of analysing real-time data collected from a large number of devices, common in IoT environments, in order to ensure a proper performance according to SLA contracts.

7.3 Operational requirements

This clause captures operational requirements.

[OR.1] When using the ENI framework to provide intelligent network operation and management, it shall be possible to minimize the Total Cost of Ownership (TCO), including OPEX (Operating Expenses) and CAPEX (Capital Expenses) of the network infrastructure. Existing network infrastructure shall be reused as much as possible to build or interwork with the ENI framework.

[OR.2] The ENI framework shall help to improve the energy efficiency of the whole network, where the information is available.

[OR.3] The ENI framework shall provide, by using a functional block architecture, the support for multiple applications as used in different use cases.

7.4 Regulatory requirements

This clause captures regulatory requirements.

[RegR.1] The privacy of the users shall be properly protected during the collection, storage and analysis of the data.

NOTE: In Europe, the GDPR applies.

[RegR.2] It shall be possible to analyse the network data without exposing its users.

[RegR.1] The provider of an ENI framework shall comply with the provisions of the Lawful Interception regulations.

[RegR.2] The provider of an ENI framework shall comply with the provisions of the data protection regulations.

[RegR.3] The provider of an ENI framework shall comply with the provisions of the information security regulations.

Annex A (informative): Change History

Date	Version	Information about changes
2017-05	v0.0.1	Initial early draft with skeleton
2017-06	v0.0.2	Combine ENI(17)000012r1
2017-07	v0.0.3	Combine ENI(17)000028r1
2017-08	v0.0.4	Combine ENI(17)000039r1, ENI(17)000044r1
2017-09	v0.0.5	Combine ENI(17)000079r1, ENI(17)000080r1
2017-10	v0.0.6	Combine ENI(17)003_029r1, ENI(17)003_031r1, ENI(17)003_032r1, ENI(17)003_035r1
2017-10	v0.0.7	Combine ENI(17)000086r1
2017-11	v0.0.8	Adding requirements from clause 4.12 of ETSI GR ENI 003
2017-11	v0.0.9	Change GR to GS, revise requirements in clause 6 & 7
2017-12	v0.1.0	Combine ENI(17)004_007r1, ENI(17)004_020r1, ENI(17)004_021r1
2018-02	v0.1.1	Combine ENI(18)000042r1, ENI(18)000043r1
2018-03	v0.1.2	Combine ENI(18)005_019, ENI(18)005_020r1, ENI(18)005_022r3
2018-04	v1.1.1	Publication
2018-05	v2.0.0	Combine ENI(18)000105r1, ENI(18)000106r1
2018-06	v2.0.1	Combine ENI(18)006_024r2, ENI(18)006_027, ENI(18)006_026r4
2018-11	v2.0.2	Combine ENI(18)000186r1
2019-02	v2.0.3	Combine ENI(19)000021r1
2019-03	v2.0.4	Combine ENI(19)000046r1
2019-05	v2.0.5	Combine ENI(19)000121, ENI(19)000125r1
2019-07	V2.0.6	Combine ENI(19)000100r1 and changes agreed during ENI#10
2019-09	V2.1.1	Publication
2019-09	V3.0.1	Combine ENI(19)011_026r1 and new scope agreed during ENI#11
2019-12	V3.0.2	Combine ENI(19)012_028
2020-03	V3.0.3	Combine ENI(20)000041
2020-03	V3.0.4	Combine ENI(20)013_032r1
2020-04	V3.0.5	Combine ENI(20)000_008r1
2020-06	V3.0.6	Combine ENI(20)014_037r1

History

Document history		
V1.1.1	April 2018	Publication
V2.1.1	September 2019	Publication
V3.1.1	December 2020	Publication