4

Edge AI Non-Functional Requirements

4.1 Definition

The field of edge AI is relatively new and there is no established standardised definition solely for edge AI system non-functional requirements (NFRs) provided by ISO or IEEE standards. This work intends to use the concepts associated with NFRs for edge AI systems using broader concepts of systems based on the existing hardware, software, AI components and data engineering. These concepts guide specifying non-functional requirements that can be adapted to edge AI environments' unique characteristics and constraints.

While no standard exclusively defines edge AI non-functional requirements, ISO and IEEE standards such as ISO/IEC/IEEE 29148:2018 [55], IEEE 2874-2025 [186], and ISO/IEC 25010:2023 [45] provide robust frameworks for understanding and specifying these requirements. Non-functional requirements are essential for ensuring that a system performs correctly and meets broader quality and operational demands, aligning with stakeholder expectations and regulatory constraints.

The ISO/IEC/IEEE 29148:2018 [55] standard defines non-functional requirements as quality requirements that include several of the ilities' in requirements, for example, reliability, usability, security, compatibility, reusability, scalability, maintainability, flexibility, safety, and portability. The kinds of quality requirements (e.g., "ilities") should be identified prior to initiating the requirements activities. This should be tailored to the system(s) being developed. As appropriate, measures for meeting the quality requirements should also be included. Additional guidance on software quality requirements can be found in the ISO/IEC SQuaRE standards, particularly ISO/IEC 25030:2019 [53], as well as in ISO/IEC 25010:2023 [45] and IEEE 2874-2025 [186]. A summary of the product quality model characteristics presented in ISO/IEC 25010:2023 is shown in Table 4.2, which includes characteristics such as functional suitability, performance efficiency, compatibility, interaction capability, as well as reliability, security, maintainability, flexibility, and safety with several specific sub-characteristics.

In the design of edge AI systems, NFRs, or quality requirements are the primary architectural drivers that dictate the system's design and feasibility. The convergence of AI's probabilistic nature with the severe constraints of edge computing creates a new and complex landscape of quality attributes that must be proper engineered.

Many traditional NFRs are intensified in the edge AI context, becoming more critical and challenging to satisfy. Performance, often measured in terms of latency and throughput, is paramount for the real-time applications that edge AI enables. Energy efficiency is a critical constraint for battery-powered or thermally limited devices, directly impacting their operational lifespan and viability. Reliability and availability are essential, as edge AI systems must often function autonomously and dependably, even with intermittent network connectivity. Security and privacy take on new dimensions; physically accessible edge devices are exposed to novel threats, including direct attacks on the edge AI models (e.g., data poisoning, adversarial evasion), while the local processing of data introduces new challenges in preventing information leakage.

Edge AI introduces a new class of emergent quality attributes that are central to a system's trustworthiness and social acceptance. Model accuracy, including measurements like precision and recall, is a quality that must be specified and measured. Robustness, the model's ability to maintain performance in the presence of noisy or adversarial inputs, is critical for real-world deployment. Explainability (XAI), the capacity to provide human-understandable reasons for a model's decision, is an increasingly vital requirement for user trust, debugging, and regulatory compliance. Fairness and the mitigation of bias are crucial ethical and legal requirements, ensuring that the edge AI models do not make systematically discriminatory decisions. Adaptability and retrainability refer to the system's capacity to evolve in response to changing data distributions (concept drift) over time, often through on-device or federated learning techniques.

The edge AI NFR landscape is a multi-layered construct as quality attributes apply to different parts of the edge AI system and a detailed approach requires decomposing NFRs and specifying them for distinct scopes: the data (e.g., quality, completeness, lack of bias), the edge AI model (e.g., accuracy, robustness, fairness), the hardware and software platform (e.g., performance, energy efficiency), and the overall system-in-operation (e.g., reliability, security, privacy). This multi-scope view is essential for effective requirements management and trade-off analysis. Edge AI system

NFRs refer to the criteria describing how a system operates rather than specific behaviours or functions. These requirements define an edge AI system's quality attributes and characteristics, performance benchmarks, and constraints, encompassing functional suitability, performance efficiency, compatibility, interaction capability, reliability, security, maintainability, flexibility, and safety [55].

Capturing non-functional requirements is critical to ensuring edge AI systems meet necessary quality and performance standards. Non-functional requirements in this context focus on "how" an edge AI system performs its functions, providing detailed specifications for quality attributes.

4.2 Methodology for Defining NFRs

The process of engineering edge AI systems is an exercise in making reasoned trade-offs between numerous conflicting NFRs and constraints. To manage the complexity, qualitative goals must be translated into quantitative, verifiable requirements. For example, an imprecise goal like "the system should be energy efficient" must be specified as "under operational load A, the system's average power consumption shall not exceed 100 mW". In the same manner, an ethical goal like "the edge AI model should be fair" must be quantified as "the edge AI model's false positive rate for demographic group A shall not differ from that of group B by more than a specified percentage on benchmark dataset Z".

This quantification enables structured trade-off analysis, which is an important design activity in edge AI. However, it is not possible to simultaneously maximise all desirable qualities, such as achieving the highest accuracy with the lowest latency and the minimum power consumption and therefore, the engineering goal is not maximisation but optimisation to find the best possible compromise that satisfies the most critical requirement within the given constraints.

Several key trade-off axes dominate edge AI system design. The most common trade-off is between model accuracy and system performance (latency and throughput), where more complex and accurate models are inherently slower and more resource-intensive. This is managed through techniques like model compression and hardware acceleration. Another critical axis is performance versus energy consumption, which is addressed through hardware-software co-design and power management techniques.

Table 4.1 Trade-off analyses in edge AI system design

Trade-off	**Conflicting NFRs**	**Design considerations**	**Management techniques**
Model Complexity	Accuracy vs. Latency, Memory Footprint, Energy consumption	Target hardware's compute/memory capacity. Real-time performance requirements. Power budget.	Model Pruning, Quantization, Knowledge Distillation, Neural Architecture Search (NAS), HW-SW Co-design.
Computational Efficiency	Performance (Latency/ Throughput) vs. Energy Consumption	Thermal design power (TDP) of the device. Battery life requirements. Required responsiveness of the application.	HW Acceleration (GPU, NPU, FPGA), Hardware-Software Co-design, Dynamic Voltage and Frequency Scaling (DVFS), Efficient algorithm-to-hardware mapping.
Data Management	Privacy vs. Model Accuracy/Adaptability	Regulatory requirements (e.g., GDPR). Need for model personalisation and continuous improvement. Network bandwidth availability.	Federated Learning, Differential Privacy, On-device training, Data minimisation and anonymisation techniques.
System Security	Security vs. Performance, Cost	Threat model, including physical access and model-specific attacks. Resource cost of cryptographic operations and security monitoring.	Trusted execution environments (TEEs), Lightweight cryptography, HW Security Modules (HSMs), Adversarial training, Model obfuscation.

Another example of a trade-off is that enhancing an edge AI model's robustness against adversarial attacks may require a more complex architecture, negatively impacting efficiency in federated learning. Table 4.1 provides a set of examples for trade-off analyses in edge AI system design.

To navigate this multi-dimensional design space, engineers can employ formal methods for trade-off analysis. Creating Pareto frontiers, which are a set of optimal solutions that strike a balance between revenue maximisation and cost minimisation in the design and scheduling, allows for the visualisation of optimal solutions for multi-objective problems, showing the set

Table 4.2 ISO/IEC 25010:2023 [45] overview, including characteristics and sub-characteristics

Software product quality				
Functional suitability	**Performance efficiency**	**Compatibility**	**Interaction capability**	
Functional completeness. Functional correctness. Functional appropriateness.	Time behaviour. Resource utilization. Capacity.	Co-existence. Interoperability.	Appropriateness recognizability. Learnability. Operability. User error protection. User engagement. Inclusivity. User assistance. Self-descriptive.	
Reliability	**Security**	**Maintainability**	**Flexibility**	**Safety**
Faultlessness. Availability. Fault tolerance. Recoverability.	Confidentiality. Integrity. Non-repudiation. Accountability. Authenticity. Resistance.	Modularity. Reusability. Analysability. Modifiable. Testability.	Adaptability. Scalability. Instability. Replaceability.	Operational constraint. Risk identification. Fail safe. Hazard warning. Safe integration.

of designs that offer the best possible accuracy for a given latency budget. Quantitative frameworks can also be used to structure the decision-making process by weighting different NFRs according to priorities, ensuring that trade-offs are made consciously and defensibly. This continuous process of co-design and co-optimisation across the entire system stack, data, edge AI model, software, and hardware, is the essence of engineering edge AI.

The NFRs can be mapped to the ISO/IEC 25010:2023 attributes or characteristics and sub-characteristics for edge AI systems and data quality requirements in ISO/IEC 25012:2008 [46].

A summary of the product quality model characteristics presented in ISO/IEC 25010:2023 is shown in Table 4.2.

Each NFR has a KPI identified and a measure to provide a verifiable and quantifiable (qualitative/quantitative) assessment. The methodology proposed is based on the measures described in ISO/IEC 25023:2016 [51] and ISO/IEC 25021:2012 [49] (parts of the ISO/IEC 25000:2014 and series of standards [171, 172] SQuaRE series - System and software quality requirements and evaluation) as reference.

The role of ISO/IEC 25000 in measuring and assessing AI product quality is widely recognised and has received increasing interest, as the standards propose measurement methods like those developed in scientific literature and projects, aligning with the ISO 25000 conforming measurement method [133]. The work in [133] analysed this similarity and concluded that most measurement methods used for AI can be easily mapped into the ISO 25000 format.

The ISO/IEC 25012:2008 standard can be used in edge AI systems to extend the product quality model defined in ISO/IEC 25010:2023 with the data properties. The standard covers data held in a structured format, and it specifies a general data quality model. The target is data processed or stored by the system which can be considered persistent data. Conformance of data to a data design specification is outside the scope of the standard. Data quality is the degree to which data properties satisfy explicit and implicit needs when used in a specified context. The quality is intended to be application-dependent. It does not consider universal data quality that can be applied for any purpose.

Data quality characteristics are defined as the attributes that affect quality. ISO/IEC 25012:2008 defines data quality through two main categories: inherent data quality and system-dependent data quality. These categories encompass fifteen data quality characteristics, five for inherent data quality (accuracy, completeness, consistency, credibility, currentness) and ten for system-dependent data quality (accessibility, compliance, confidentiality, efficiency, precision, traceability, understandability, availability, portability, recoverability).

The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems [78] highlighted in 2016 the importance of integrating socio-technical standards early in development to ensure that autonomous and intelligent systems align with human values, intentions, and understanding, thereby reducing the risk of unwanted behaviours. These standards are informed by IEEE's Ethically-Aligned Design P7000 Series of standards that address human rights, well-being, accountability, and transparency for AI and autonomous intelligent systems.

In response to this initiative, the Spatial Web Foundation [79] and the IEEE P2874 Spatial Web, Architecture, and Governance Working Group [80] have developed the IEEE P2874 standards, including the Spatial Web Protocol, Architecture, and Governance specifications. These specifications, approved and ratified by IEEE in May 2025, define the system requirements for the interoperability and governance of cyber-physical systems, encompassing autonomous devices, applications, spatial content, and operations. Networked communication systems designed to meet these specifications enable the standardised representation of statements, relationships, interactions in the physical and digital sociotechnical systems, making them suitable for computational modelling, simulation, and automation.

The design and development of edge AI systems need to embed AI trustworthiness concepts. These encompass several aspects addressed by system engineering dependability that include several system quality properties (e.g., security, safety, availability, connectability, resilience, reliability, maintainability, and privacy) covered by ISO/IEC TS 5723:2022 in addition to ISO/IEC 25010:2023 and ISO/IEC 25012:2008.

The further development of edge AI systems includes ethical edge AI considerations (e.g., fairness, responsibility, accountability, governance) and specific (e.g., explainability, interpretability) that are intrinsic to the data-centric and black-box nature of ML/DL edge AI.

An extensive list of quality attributes or characteristics that can be used as NFRs for edge AI systems is given below.

- **Functional suitability** represents the degree to which a product or system provides functions that meet stated and implied needs when used under specified conditions. This characteristic is formed by sub-characteristics functional completeness, functional correctness, functional appropriateness.
- **Performance efficiency** reflects the performance relative to the resources used under stated conditions. This characteristic is formed by sub-characteristics of time behaviour, resource utilisation, and capacity.
- **Compatibility** is the degree to which a product, system or component can exchange information with other products, systems, or components and/or perform its required functions while sharing the same hardware or software environment. This characteristic is composed of sub-characteristics of co-existence and interoperability.
- **Interaction capability** is the degree to which a product or system can be interacted with by specified users to exchange information in the user interface to complete specific tasks in a variety of contexts of use. This characteristic is composed of the following sub-characteristics appropriateness recognizability, learnability, operability, user error protection, user engagement, user assistance, self-descriptiveness.

- **Reliability** is the degree to which a system, product or component performs specified functions under specified conditions for a specified period of time. This characteristic comprises sub-characteristics of faultlessness, availability, fault tolerance, and recoverability. Reliability is the system ability of an item to perform as required, without failure, for a given time interval, under given conditions. The time interval duration can be expressed in units appropriate to the item concerned (e.g. calendar time, operating cycles, distance run, etc.) and the units should always be clearly stated. The conditions include aspects that affect reliability, such as mode of operation, stress levels, environmental conditions, and maintenance (IEC 60050-192:2015 [185]).
- **Security** is the degree to which a product or system protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorisation. The authorisation comprises sub-characteristics confidentiality, integrity, non-repudiation, accountability, authenticity and resistance. Security represents the degree of resistance to intentional, unauthorised act(s) designed to cause harm or damage to an edge A *system* (ISO/IEC 23643:2020 [173]).
- **Maintainability** represents the degree of effectiveness and efficiency with which a product or system can be modified to improve it, correct it, or adapt it to changes in the environment and requirements. This characteristic comprises sub-characteristics modularity, reusability, analysability, modifiability, and testability.
- **Flexibility** is the degree to which a product can be adapted to changes in its requirements, contexts of use or system environment. This characteristic is composed of sub-characteristics adaptability, scalability, installability, and replaceability.
- **Safety** represents the degree to which a product under defined conditions to avoid a state in which human life, health, property, or the environment is endangered. This characteristic is composed of sub-characteristics operational constraint, risk identification, fail safe, hazard warning and safe integration. Safety is the property of an edge AI *system* such that it does not, under defined conditions, lead to a state in which human life, health, property, or the environment is endangered (ISO/IEC/IEEE 12207:2017 [56]).
- **Accountability** relates to an allocated responsibility, which can be based on regulation or agreement or through assignment as part of delegation.

Accountability is a property that ensures that an entity's actions can be traced uniquely to the entity (ISO 7498-2:1989 [174]). In the context of edge AI, accountability is the obligation of the producer of the edge AI system to account for its system or services and disclose the results transparently if needed. The responsibility for the edge AI's action/inaction/malfunction is attributed to an actor that is part of a business agreement, the owner, designer/developer, manufacturer, operator of an edge AI technology or application.

- **Governance** refers to the framework of norms, laws, and regulations that guide the development, deployment, and use of artificial intelligence within a specific domain. It encompasses the principles and standards that ensure AI systems operate ethically, transparently, and responsibly, aligning with societal values and legal requirements. It seeks to establish accountability and protect rights while preventing harm and mitigating risks associated with their application.
- **Accuracy** is a measure of the closeness of results of observations, computations, or estimates to the true values or the values accepted as being true (ISO 17572-1:2022, 3.1 [175]).
- **Authenticity** is a property that an entity is what it claims to be (ISO/IEC 27000:2018, 3.6 [176]).
- **Availability** is the property of being accessible and usable on demand by an authorised entity (ISO/IEC 27000:2018, 3.7).
- **Spatiability** refers to the capability of representing information as locations and relationships within a hyperspace to structure and interpret data. The spatial representation allows intelligent computing systems to perform tasks and make decisions based on spatio-temporal context (IEEE 2874-2025).
- **Controllability** is the property of an AI *system* that allows a human or another external agent to intervene in the edge AI system's functioning (ISO/IEC 22989:2022, 3.5.6 [21]).
- **Integrity** is a property whereby data have not been altered in an unauthorised manner since they were created, transmitted, or stored (ISO/IEC 29167-19:2019, 3.3 [177]). Integrity can be a system property of *accuracy* and completeness (ISO/IEC 27000:2018, 3.36).
- **Privacy** is the freedom from intrusion into the private life or affairs of an individual (ISO/IEC 2382:2015, 2.22).

- **Resilience** is the *capability* of an edge AI *system* to maintain its functions and structure in the face of internal and external change and to degrade gracefully when this is necessary.
- **Robustness** is the ability of an edge AI *system* to maintain its level of performance under a variety of circumstances (ISO/IEC 22989:2022). Robustness is the ability of edge AI systems to maintain their performance when faced with various challenges, such as perturbations, unexpected changes or adversarial and malicious inputs. This quality attribute or characteristic of edge AI systems encompasses two key aspects: algorithm robustness, which evaluates the learning algorithm's resilience to variations in the training dataset, and model robustness, which assesses how well a trained model withstands alterations and perturbations in input data.
- **Transparency** is the property of an edge AI system or process to imply openness and *accountability* (ISO/IEC 27036-3:2023 [178]). Transparency relates to the capability of an edge AI system to, always, be able to provide a satisfactory explanation for its decisions, auditable either by an in-house or an independent human authority assessment. In the case of failure causing harm, it should be possible to ascertain why.
- **Usability** represents the extent to which an edge AI *system,* product, or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context (ISO 9241-11:2018 [179]).
- **Fairness** represents the extent to ensure mechanisms embedded in guidelines and initiatives related to ethics, bias mitigation, and responsible edge AI technology development. Edge AI fairness is discussed in terms like bias mitigation to ensure that edge AI algorithms and datasets do not produce or perpetuate bias, equitability to ensure edge AI systems treat all users fairly, transparency to provide clarity on how edge AI systems make decisions and accountability to ensure that edge AI systems are held responsible for their outcomes. Fairness in edge AI can be context-dependent and subject to varying interpretations based on cultural, social, and legal factors.
- **Explainability** is the ability to explain the decision-making process in terms that are understandable to the end user. An explainable model provides a clear and intuitive explanation of the decisions made, enabling users to understand why the model has produced a particular result;

it focuses on why an algorithm has made a specific decision and how that decision can be justified. It requires a straightforward and intuitive presentation of information using an ontology familiar to the user. It is particularly valuable and beneficial in the case of deep neural networks, where the models are difficult to interpret due to the convoluted structure and complex internal interactions. Explainability is a consideration of the deployed AI model.

- **Interpretability** is the ability to understand the decision-making process of an edge AI model. An interpretable edge AI model provides clear information about the relationship between inputs and outputs. An interpretable algorithm can be explained clearly and understandably by a person. Interpretability is essential to ensure that users will trust AI models. Interpretability is mostly associated with model training, evaluation, and quality assurance.

Using the information provided in [45] non-functional requirements for edge AI systems are specifying how well the functionality should present itself and behave, aligning to the other quality characteristics outlined in ISO/IEC 25010:2023 System and software quality models, ISO/IEC 25012:2008 Data quality model and specific AI quality attributes or characteristics. Non-functional requirements are related to some, or all the functionality and typically functional requirements are associated with appropriate non-functional requirements, either individually or in groups.

The non-functional requirements for edge AI systems can have a two-layer representation following the ISO/IEC 25010:2023 model with a "high-level" non-functional requirement assigned to the quality characteristics or attributes and a "low-level" non-functional requirement assigned to the quality sub-characteristics or attributes.

Table 4.3 provides a set of examples for the comparison between the traditional NFRs and the AI-centric ones.

4.3 Edge AI Non-Functional Requirements, Key KPIs and Measures.

The following section provides examples (structured in tables) of edge AI non-functional requirements, KPIs, and measures that researchers and practitioners can use as references for their projects. The examples cover various areas of application.

Table 4.3 Comparison of traditional and AI-centric NFRs

NFR Category	Traditional System Context	Edge AI System Context and Key Measures
Performance	Response time, throughput, resource utilisation.	**Latency:** Inference time (ms). **Throughput:** Inferences per second (IPS). **Energy:** Joules per inference.
Reliability	Mean Time Between Failures (MTBF), availability (uptime percentage).	Includes traditional metrics plus model stability and graceful degradation under data drift or noisy inputs.
Security	Network security (firewalls, IDS), access control, data encryption.	Includes traditional aspects plus model-specific vulnerabilities. Metrics include resilience to model inversion, membership inference, data poisoning, and adversarial evasion attacks. Physical device security is critical.
Privacy	Data protection compliance (e.g., GDPR), anonymisation of stored data.	Enhanced by on-device processing. Challenges include preventing data leakage during federated learning or model updates. Compliance with data minimisation principles.
Explainability	New type of NFR. System logic is documented in specifications.	A critical emergent NFR. Measured by techniques like LIME/SHAP scores, rule extraction fidelity, or qualitative user studies on explanation clarity.
Fairness	New type of NFR. Assumed to be handled by business logic.	A critical ethical and legal NFR. Measured by statistical parity, equal opportunity, or equalised odds across demographic groups on benchmark datasets.
Robustness	Fault tolerance, graceful degradation to HW/SW faults.	Model's resilience to perturbations in input data. Measured by accuracy drop on corrupted or adversarial datasets (e.g., Projected Gradient Descent-PGD attacks).
Adaptability	System's ability to be modified for new requirements (maintainability, extensibility).	Model's ability to adapt to concept/data drift over time. Measured by performance retention after on-device retraining or federated learning cycles.

4.3.1 Performance Efficiency

Table 4.4 Performance efficiency (Time-behaviour)

NFR aspect	**NFR description**
Name	Characteristics: **Performance efficiency** Sub-Characteristics: **Time-behaviour**
Definition	System frame rate.
Description	Frame rate.
What is measured	How many predictions the system can perform per unit of time.
KPI	System throughput.
Methods of collection/ measurement and verification/validation	Measurement of inference time on a realistic use-case configuration (e.g., same data format, same system configuration) in various task-related conditions (e.g., night, light for the external camera).
Target Value	Given number of sample per seconds (e.g., frame/s, token/s, sample/s).

Table 4.5 Performance efficiency (Resource utilization)

NFR aspect	**NFR description**
Name	Characteristics: **Performance efficiency** Sub-Characteristics: **Resource utilization**
Definition	System power consumption.
Description	Power consumption.
What is measured	How much the edge AI system consume power while used on raw sensor data.
KPI	Power consumption.
Methods of collection/ measurement and verification/validation	Inference in real-use conditions. Power measurement on various scenes and conditions.
Target Value	A given/max value of power consumption [mW] (e.g., 50 mW).

Table 4.6 Performance efficiency (Resource utilization)

NFR aspect	**NFR description**
Name	Characteristics: **Performance efficiency** Sub-Characteristics: **Resource utilization**
Definition	System memory consumption
Description	Memory consumption
What is measured	How much memory is required by the edge AI system, and the related AI model.
KPI	Memory
Methods of collection/ measurement and verification/validation	Static requirements for storing model parameters and monitoring dynamic memory needs for execution.
Target Value	A given/max value of memory use [MB] (e.g., $<$ 2MB).

Table 4.7 Performance efficiency (Capacity)

NFR aspect	**NFR description**
Name	Characteristic: **Performance efficiency** Sub-characteristics: **Capacity**
Definition	Degree to which the maximum limits of a product or system parameter meet requirements.
Description	The system capacity of handling many requests, data or events.
What is measured	Maximum volume of events or data that can be processed by the system/edge system.
KPI	Highest number of requests (data units, event units, messages units) that the system can handle without significant failure (failure to answer, wrong response, delayed response).
Methods of collection/ measurement and verification/validation	Counting the volume of requests in units. Stress test with typical data in operational conditions.
Target Value	Number of user requests processing at the same time (depends on the system) (e.g., processing 1000 user requests simultaneously).

4.3.2 Compatibility

Table 4.8 Compatibility (Co-existence)

NFR aspect	**NFR description**
Name	Characteristic: **Compatibility** Sub-characteristics: **Co-existence**
Definition	Co-existence of SSMA and existing equipment methods. Co- existence of developed methods with other existing methods consume the same HW and data source → degree to which a product can perform its required functions efficiently while sharing a common environment and resources with other products, without detrimental impact on any other product.
Description	Co- existence of developed methods with other existing methods consume the same HW and data source. • Understanding of computational resources • Finding out limitations and opportunities
What is measured	RAM on the computational resource, connection latency on other existing methods, usage of CPU.
KPI	Utilization of resources.
Methods of collection/ measurement and verification/validation	Tracking of existing computational resources via existing dashboard. Verification: deployment on test environment. Validation: Comparison of resources w/o running and w/running inference/ training.
Target Value	The average utilization increases less than a given percentage [%] of the available resources depending on inference or training (e.g., average utilization increases less than 50% of the available resources).

Table 4.9 Compatibility (Interoperability)

NFR aspect	NFR description
Domain example	Digital industry domain.
Name	Characteristic: **Compatibility** Sub-characteristics: **Interoperability**
Definition	Interoperability of the SSMA - method(s). What are the constrains where all systems competing for, internally and externally.
Description	Degree to which two or more decision making systems, products or components can exchange information/knowledge and use the information/knowledge that has been exchanged.
What is measured	Number of downstream systems that leverage the results of these models. • Response time for inference on downstream system. • Generalization of the model results. flexibility of the deployment environment (e.g., different frameworks – Keras, TensorFlow, etc.).
KPI	Number of use cases which the model results can be used for. Number of different deployment environment which the model can be host in.
Methods of collection/ measurement and verification/ validation	Develop testing framework to measure inference response time on downstream tasks and test different deployment env. that mimics the actual production line. Count use cases per model. Verification: deployment on test environment.
Target Value	Response time value.

4.3.3 Interaction Capability

Table 4.10 Interaction capability (Learnability)

NFR aspect	NFR description
Name	Characteristics: **Interaction capability** Sub-Characteristics: **Learnability**
Definition	Ensure learnability by ensuring a user-friendly interface and intuitive control for user.
Description	Provision of self-explanatory user interface with intuitive controls, and status of temperature and time-capability of warm water delivery.
What is measured	User satisfaction rating.
KPI	Usability score on a defined scale (e.g., ranging from 1 to 10).
Methods of collection/ measurement and verification/ validation	Let various persons tyre the interface, observe time spend to perform some common functions. Measure task success rate and time on task. Usability test with a defined number of different people related to the company, measuring task success rate and time on task. Record the values.
Target Value	A predefined minimum score according to the given scale. (E.g., target value to be at least 8 on a scale from 1 to 10).

Table 4.11 Interaction capability (User error protection)

NFR aspect	**NFR description**
Name	Characteristics: **Interaction capability** Sub-Characteristics: **User error protection**
Definition	Degree to which a system protects users against making errors.
Description	The end-user should not be required to provide a manual input to obtain a prediction result, which eliminates the possibility of user errors.
What is measured	Number of manual inputs required by the end user.
KPI	End-user manual inputs.
Methods of collection/ measurement and verification/ validation	Analysis of system architecture. Testing by end-users.
Target Value	The number maximum acceptable manual inputs required (e.g., 0 (none)).

Table 4.12 Interaction capability (User engagement)

NFR aspect	**NFR description**
Name	Characteristic: **Interaction capability** Sub-characteristics: **User engagement**
Definition	Degree to which a user interface presents functions and information in an inviting and motivating manner encouraging continued interaction.
Description	The use of the device or system should de motivating for human users to keep them engaged with the system.
What is measured	Average session duration, user retention rate, interaction frequency.
KPI	Duration of a session in minutes, return rate of identified users, number of interactions per minute.
Methods of collection/ measurement and verification/ validation	Automatic collection in the log file of the system. Analysis of the log files and measure of the above-mentioned KPIs.
Target Value	Session duration greater than a given time [min], retention greater than a given rate [%], and number of interactions per minute (e.g., session time $>$ 20 minutes, retention $>$ 30%, 3-5 interactions per minute).

Table 4.13 Interaction capability (Inclusivity)

NFR aspect	**NFR description**
Name	Characteristic: **Interaction capability** Sub-characteristics: **Inclusivity**
Definition	Degree to which a product or system can be used by people of various backgrounds (such as people of various ages, abilities, cultures, ethnicities, languages, genders, economic situations, etc.).
Description	The system should avoid barriers for people with various backgrounds
What is measured	The extent to which the system is usable from a large portion of the population.
KPI	Number of supported languages in the interface, visibility/contrast of user interface, possibility of use with disabilities
Methods of collection/ measurement and verification/ validation	Analysis of the user interface, user satisfaction survey on usability for specific populations. Analysis of the system and counting the elements or conduction of a user study with a given number of users from a specific background.
Target Value	Number of supported languages their satisfaction score target value. (E.g., supported languages $>$ 8, satisfaction score $>$ 8 out of 10).

Table 4.14 Interaction capability (User assistance)

NFR aspect	**NFR description**
Name	Characteristic: **Interaction capability** Sub-characteristics: **User assistance**
Definition	Degree to which a product can be used by people with the widest range of characteristics and capabilities to achieve specified goals in a specified context of use.
Description	System should be accessible with different means to cover differences in abilities from the users.
What is measured	Capacity of accomplishing the desired goal in presence of disabilities.
KPI	Number of input/output methods proposed for interacting with the system (voice, typing, sound etc.).
Methods of collection/ measurement and verification/ validation	Analysis of the system in terms of number of interaction possibilities. Test run with various input/output methods.
Target Value	Number of available interacting (input/output methods) alternatives. (E.g., the system should offer at least 2 alternatives for interacting).

Table 4.15 Interaction capability (Self-descriptive)

NFR aspect	**NFR description**
Name	Characteristic: **Interaction Capability** Sub-characteristics: **Self-descriptive**
Definition	Degree to which a product presents appropriate information, where needed by the user, to make its capabilities and use immediately obvious to the user without excessive interactions with a product or other resources (such as user documentation, help desks or other users).
Description	The system should contain enough information to be used without referring to documentation.
What is measured	Ease of interaction and clarity of what is happening and how to interact.
KPI	User satisfaction with the interaction with the system.
Methods of collection/ measurement and verification/ validation	Running tests with selected users and evaluate satisfaction with an adequate feedback form. User satisfaction survey with a defined minimum of users.
Target Value	A predefined minimum satisfaction level score according to the given scale (e.g., satisfaction level of 8 on a scale from 1 to 10).

4.3.4 Reliability

Table 4.16 Reliability (Availability)

NFR aspect	**NFR description**
Name	Characteristics: **Reliability** Sub-Characteristics: **Availability**
Definition	Degree to which a system, product or component is operational and accessible when required for use.
Description	High reliability is key for eventual use in productive environment: Ideally, each measurement in the production line should correspond to a prediction.
What is measured	Number of measurements in the production line, number of predictions done.
KPI	Ratio of predicted lots to measured lots.
Methods of collection/ measurement and verification/ validation	Semi-automated comparison of equipment tracking data and prediction output. Data analysis.
Target Value	The minimum ration of predicted lots to measured lots given in percentages [%]. (E.g., ≥ 75 %).

Table 4.17 Reliability (Availability)

NFR aspect	NFR description
Name	Characteristics: **Reliability** Sub-Characteristics: **Availability**
Definition	Degree to which a system, product or component is operational and accessible when required for use in a specified period.
Description	Energy management system availability and mean downtime.
What is measured	The occurrence of system downtime for a specified period of time.
KPI	Qualitative [%].
Methods of collection/ measurement and verification/ validation	Demonstrator evaluation. Validation of availability/downtime parameters.
Target Value	System availability versus downtime given in percentages [%] (e.g., availability $\geq$ 90 %).

Table 4.18 Reliability (Fault tolerance)

NFR aspect	NFR description
Name	Characteristic: **Reliability** Sub-characteristics: **Fault tolerance**
Definition	Degree to which a system, product or component operates as intended despite the presence of hardware or software faults.
Description	The system should continue to provide the expected output when a software or hardware fault arises.
What is measured	Correspondence between provided output and expected output in presence of known faults.
KPI	The difference between output and expected output.
Methods of collection/ measurement and verification/ validation	Depends on the output type (unit, quantity). Injection of faults and stress test, or system log to analyse the behaviour in occurrence of a natural fault.
Target Value	The difference (in percentage [%]) of real output versus expected output in presence of a specific hardware or software fault (e.g., less than 10 % difference with expected output in presence of a specific HW or SW fault).

Table 4.19 Reliability (Recoverability)

NFR aspect	NFR description
Name	Characteristic: **Reliability** Sub-characteristics: **Recoverability**
Definition	Degree to which, in the event of an interruption or a failure, a product or system can recover the data directly affected and re-establish the desired state of the system.
Description	Ability of the system to return to a functioning state after a failure happened and has been detected and corrected.
What is measured	Failover mechanism to ensure data is not lost or corrupted and maintenance of the expected service
KPI	Integrity of the data after failure, continuity of data processing despite network failure
Methods of collection/ measurement and verification/ validation	Simulation of failure or actual failure in controlled environment. Simulated or intentional failure injection.
Target Value	The maximum amount of data loss [MB], when continue functioning (e.g., amount of lost data is less than 1 MB, ability to continue function even if as much as 1 MB of data is lost).

4.3.5 Security

Table 4.20 Security (Confidentiality)

NFR aspect	NFR description
Name	Characteristic: **Security** Sub-characteristics: **Confidentiality**
Definition	Degree to which a product or system ensures that data are accessible only to those authorized to have access.
Description	Systems should implement mechanisms to prevent access to confidential data by unwanted entities (hackers/other users).
What is measured	Number of successful attacks in which confidential data is accessed
KPI	Attack success rate = number of successful attacks over total number of attacks in a fixed period of time.
Methods of collection/ measurement and verification/ validation	Log files on system attacks or simulated attacks. Measure on the log files and/or after simulation.
Target Value	Maximum attack success rate [%] for a defined period of time (e.g., attack success rate < 0.001 %).

Table 4.21 Security (Confidentiality)

NFR aspect	NFR description
Name	Characteristic: **Security** Sub-characteristics: **Confidentiality**
Definition	Degree to which a product or system ensures that data are accessible only to those authorized to have access.
Description	Systems should implement mechanisms to prevent access to confidential data by unwanted entities (hackers/other users).
What is measured	Attacker's capability to reconstruct confidential data.
KPI	Percentage of data samples or features per sample reconstructed by the attacker, quality of the reconstructed data/features.
Methods of collection/ measurement and verification/ validation	Log files on system attacks or simulated attacks. Measure on the log files and/or after simulation.
Target Value	Maximum percentage of data/features reconstructed, minimum reconstruction error for given attacker's capabilities.

Table 4.22 Security (Integrity)

NFR aspect	NFR description
Name	Characteristics: **Security** Sub-Characteristics: **Integrity**
Definition	Degree to which a system protects data so other systems and sub-systems can access and use the data.
Description	Data synchronization and transfer mechanisms must guarantee the integrity in terms of protecting exchanged data from being corrupted, and handle cases when a device has not had internet access for a period of time.
What is measured	Number of faults in a series of messages. Number of packets without encryption.
KPI	Number of failed requests in Apache Kafka Broker.
Methods of collection/ measurement and verification/ validation	Live demonstration.
Target Value	Maximum number of failed decrypted messages (e.g., failed decrypted messages < 2 per connection).

4.3.6 Maintainability

Table 4.23 Maintainability (Modularity)

NFR aspect	**NFR description**
Name	Characteristics: **Maintainability** Sub-Characteristics: **Modularity**
Definition	Management Framework capable of serving AI models and updating them as needed, as well as scaling up types of supported sensory input.
Description	To develop an efficient, scalable, and maintainable edge AI framework adaptable to various forms of sensory feedback.
What is measured	Downtime required for maintenance and updates.
KPI	Time required for maintenance and updates.
Methods of collection/ measurement and verification/ validation	Measurement of time during live deployment.
Target Value	Maximum downtime [min] required for maintenance and updates (e.g., under 30 minutes of downtime).

Table 4.24 Maintainability (Reusability)

NFR aspect	**NFR description**
Name	Characteristics: **Maintainability** Sub-Characteristics: **Reusability**
Definition	Degree to which an asset can be used in more than one system, or in building other assets.
Description	The architecture should not only support the current, but also future use-cases. Therefore, the main architectural building blocks (scripts, hardware, training methodology, . . .) should be reusable.
What is measured	How many building blocks can be reused for future use-cases.
KPI	Ratio of re-used building blocks to total building blocks.
Methods of collection/ measurement and verification/ validation	Analysis of system architecture. Data analysis.
Target Value	The minimum number of re-used building blocks versus total building blocks given in percentages [%] (e.g., $\geq$ 60 %).

Table 4.25 Maintainability (Reusability)

NFR aspect	NFR description
Name	Characteristics: **Maintainability** Sub-Characteristics: **Reusability**
Definition	Degree to which the intelligent gateway can be used in more than one energy management system, or in building other systems.
Description	How efficient the gateways functional blocks can be used to other energy management system regarding reusability assets.
What is measured	The efficiency of the functional block used in different energy management applications.
KPI	Qualitative [%].
Methods of collection/ measurement and verification/ validation	Demonstrator evaluation. Validation of reusability.
Target Value	The degree (in percentage [%]) of reusing the intelligent gateway in other energy management systems or in building other management systems. (e.g., at least 80 % reusability).

Table 4.26 Maintainability (Analysability)

NFR aspect	NFR description
Name	Characteristic: **Maintainability** Sub-characteristics: **Analysability**
Definition	Degree of effectiveness and efficiency with which it is possible to assess the impact on a product or system of an intended change to one or more of its parts, to diagnose a product for deficiencies or causes of failures, or to identify parts to be modified.
Description	The extent to which a system can be understood when planning an extension of searching for causes of failures.
What is measured	Readability and understandability of code, documentation of hardware, documentation of pipeline and modules.
KPI	Complexity of the units, unit size, number of classes, structures.
Methods of collection/ measurement and verification/ validation	Analysis of the software code, analysis of the hardware documentation. Analysis of the code and hardware.
Target Value	Maximum number of classes and pipeline modules (e.g., less than 100 classes, pipeline with less than 12 modules, presence/ absence of non-documented elements (magic numbers etc).

Table 4.27 Maintainability (Testability)

NFR aspect	**NFR description**
Name	Characteristic: **Maintainability** Sub-characteristics: **Testability**
Definition	Degree of effectiveness and efficiency with which test criteria can be established for a system, product or component and tests can be performed to determine whether those criteria have been met.
Description	A system must foresee the possibility to conduct tests of individual modules and functionalities
What is measured	Difficulty to run specific test on the system
KPI	Number of tests that can be run on the system, possibility to test individual modules, availability of test data
Methods of collection/ measurement and verification/ validation	Analysis of the code/hardware. Verification of test procedure for each module
Target Value	The minimum number of tests that can be run on each module. (e.g., each module has one or more test with specific data).

4.3.7 Flexibility

Table 4.28 Flexibility (Adaptability)

NFR aspect	**NFR description**
Name	Characteristics: **Flexibility** Sub-Characteristics: **Adaptability**
Definition	Degree to which a system or product can effectively/efficiently be adapted for different or evolving HW/SW or other operational/usage environments.
Description	Adaptability to the evolving AI-based algorithms running on the HW/SW architecture.
What is measured	Types of AI-based algorithms running on the platform.
KPI	Qualitative [Times].
Methods of collection/ measurement and verification/ validation	Demonstrator evaluation. Validation of the types of AI-based algorithms running on the intelligent gateway.
Target Value	The increased number of AI-based algorithms that can be run on the platform in the end of the project compared to the start of the project (e.g., types of AI-based algorithms increased with 3 times from the start to the end of the project).

Table 4.29 Flexibility (Installability)

NFR aspect	NFR description
Name	Characteristic: **Flexibility** Sub-characteristics: **Installability**
Definition	Degree of effectiveness and efficiency with which a product or system can be successfully installed and/or uninstalled in a specified environment.
Description	Developed system consisting of software and hardware should be easily deployed and installed in new unknown environments
What is measured	Test on possibility to install the edge device – HW/SW system
KPI	Number of successful installability test as percentage over all tests
Methods of collection/ measurement and verification/ validation	Following procedures in installation/deployment document. Tests of installation in various environments.
Target Value	Number of successful installation tests as percentage [%] versus all tests. (e.g., > 95 % of successful installations).

Table 4.30 Flexibility (Replaceability)

NFR aspect	NFR description
Name	Characteristic: **Flexibility** Sub-characteristics: **Replaceability**
Definition	Degree to which a product can replace another specified software product for the same purpose in the same environment.
Description	Testing the capability of one software component to be replaced by another software component within a single system. The system, in regard to the replaced component, should produce the same results that it produced before the replacement.
What is measured	Capacity of the system to produce the expected behaviour when a component has been replaced by another one
KPI	Successful run of the system providing the expected output on a series of tests after replacement
Methods of collection/ measurement and verification/ validation	Replacement of one module and conduction of full system tests. Tests of system after replacement in a number of test cases.
Target Value	Rate of successful runs (in percentage [%]) after replacing a SW component within a single system (e.g., > 95 % of successful runs after module replacement).