# 7

# Standards

## 7.1 AI Standards

AI standardisation activities are receiving attention across various Standard Development Organizations (SDOs) to address the diverse challenges and opportunities AI technologies present. These SDOs include international bodies such as ISO, IEC, IEEE, and regional organisations like ETSI and CEN-CENELEC.

ISO and IEC are collaborating on a joint technical committee (JTC 1) that focuses on standardising AI across different dimensions, such as terminology, risk management, and ethical considerations. This committee has initiated the development of standards that outline best practices for AI implementation, ensuring interoperability, safety, and reliability in AI systems. Their work also emphasises the importance of transparency and accountability, with an aim to facilitate trust in AI technologies among users and stakeholders.

The IEEE has established its Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems, striving to lead standardisation activities that promote ethical considerations and inclusive practices in AI development. Through initiatives like the IEEE 7010 series [63], which focuses on the ethical considerations of autonomous systems, IEEE addresses challenges specific to AI, such as real-time processing, and the safe deployment of AI algorithms in edge environments. These standards emphasise the importance of reliability and resilience in AI applications.

IEEE's efforts focus on creating standards that guide technical aspects and encompass values such as fairness, accountability, and privacy. Their extensive engagement with industry stakeholders, academia, and policymakers aims to address the societal impacts of AI technologies and ensure that standards reflect diverse perspectives.

ETSI is also actively involved in AI standardisation, particularly in relation to telecommunications and the IoT. It is working on frameworks that facilitate the integration of AI into network and service management while

addressing security and privacy challenges. By providing guidelines and standards, ETSI aims to enhance the deployment of AI-driven solutions within its domains, fostering innovation while ensuring compliance with regulatory requirements.

CEN-CENELEC Joint Technical Committee 21 on "Artificial Intelligence" [169] created a dedicated task group (TG) dedicated to inclusiveness with the aim to elaborate recommendations to ensure and improve the inclusiveness of standards for AI and to contribute to their implementation.

Moreover, OECD has developed principles for AI [82] that focus on promoting AI's beneficial use while addressing its potential risks. These principles serve as a foundation for member countries to consider in their policymaking and standardisation efforts. The OECD AI Principles were initially adopted in 2019 and updated in May 2024.

The digital transformation of industrial sectors is highly dynamic, and standardisation plays an essential role in achieving the objectives set for this transformation. In this context, AI standardisation efforts and industry AI efforts are intertwined. Industrial AI applications rely on standardisation to build and sustain trust in industrial AI. Conversely, standardisation relies on industrial AI applications to play an essential role in forming emerging AI standards. Even though the challenges involved differ from those of similar processes in the consumer market, AI standardisation is a lever for the industry's digitalisation journey [71].

AI standardisation activities across SDOs are multifaceted, addressing technical, ethical, and societal dimensions of AI technologies. The SDOs are working collaboratively to create frameworks and guidelines that ensure AI systems are safe, reliable, transparent, and aligned with ethical principles, thereby laying the groundwork for responsible innovation in the AI landscape.

The evolution of the standardisation landscape itself reveals a significant strategic shift. Early efforts were focused on foundational questions, such as defining a common terminology to answer the question, "What is AI?". However, spurred by widespread deployment and regulatory responses to the risks posed by AI, the focus has pivoted dramatically towards operational governance, seeking to answer the question, "How do we build, manage, and verify trustworthy AI and edge AI systems?". This transition is evident in the work of ISO/IEC, which has progressed from foundational standards like the terminology in ISO/IEC 22989:2022 to comprehensive management system standards like ISO/IEC 42001:2023 [180] Similarly, the work of CEN-CENELEC JTC 21is almost entirely dedicated to operationalising

the requirements on health, safety and fundamental rights established by the AI Act [126, 149]. This shift reflects the evolution of the industry itself, extending the activities from technological capability to addressing the accountability and control as well.

In Europe, the relationship between product legislation and European standards is particularly important, a concern reflected in the AIA [116]. The law defines essential requirements for high-risk AI systems and general-purpose AI models which will be subject to further technical specification by ESOs by means of European harmonised standards. The AIA does not merely request standards; it actively shapes their content, scope, and timeline, creating a top-down demand that accelerates their development [9]. This creates a feedback loop where policy defines the high-level objectives, the "what," such as the requirements for managing risk in high-risk systems, and the SDOs define the technical implementation, the "how," such as the specific processes and documentation for a compliant risk management system. This model differs from traditional, bottom-up standardisation and has the specificity of focusing on the development of standards that are linked to legal obligations, making them indispensable for any organisation wishing to operate within the common European market.

As mentioned in this chapter, the standards and standardisation activities address AI technology and applications and are not focusing specific at edge AI. The standardisation of edge AI is still in its early stages and is often intertwined with broader standardisation efforts in AI, the IoT, and telecommunications. The challenges for edge AI include resource constraints, decentralised data governance, and the need for robust and efficient models that can operate with limited connectivity. IEEE has begun to address this space with standards like IEEE 2846-2022 [187] on safety models for automated vehicles, which often rely on edge processing, and IEEE 3652.1-2020 [188] on federated machine learning, a key enabling technology for privacy-preserving edge AI [78]. ETSI's work on securing AI is also highly relevant to the edge, as decentralised systems can present unique security vulnerabilities. As edge AI continues to grow, there will be an increasing need for dedicated standards that address its specific architectural, performance, and security requirements.

While standardisation for general AI is accelerating rapidly, the domain of edge AI presents a more nascent and fragmented picture. Edge AI, which involves deploying AI models and processing data on or near the devices where it is generated, introduces unique challenges related to resource constraints, network latency, security, and distributed management [125].

Standardisation for edge AI is not driven by a single, unified effort but instead is emerging from the convergence of work in telecommunications, industrial automation, and device-level engineering. This overview will systematically dissect the contributions of each major SDO, analyse the domains they cover for both general and edge AI, and provide a synthesised analysis of the synergies, gaps, and future trajectory of this critical field.

As edge AI technology matures and emerges as a critical focus area due to the increasing adoption of decentralised computing models, standardisation activities will address edge AI, focusing on specific factors such as latency, bandwidth limitations, and data privacy.

### 7.1.1 ISO/IEC: Building the Foundational Layer for AI

The joint efforts of ISO and IEC represent an important development for creating broad, horizontal standards for AI. The work is led by the Joint Technical Committee 1, Subcommittee 42 (ISO/IEC JTC 1/SC 42) [150], which was established in 2018 to serve as the central point for AI standardisation across both organisations. SC 42 employs an ecosystem approach, aiming to develop an integrated and interoperable suite of standards that addresses the entire AI lifecycle, from foundational concepts to governance and trustworthiness. This approach is designed to provide a stable, internationally agreed-upon foundation upon which domain-specific and application-level standards can be built.

#### 7.1.1.1 Foundational Concepts and Frameworks

A central activity of the SC 42 portfolio is establishing a common language and conceptual understanding. ISO/IEC 22989:2022, Information technology - Artificial intelligence - Artificial intelligence concepts and terminology, serves this critical function. It provides authoritative definitions for core concepts such as “AI system,” “machine learning,” and “deep learning,” models creating a universal vocabulary that is essential for ensuring consistency and preventing ambiguity across the entire global landscape of AI standards, and technical literature. An AI system, for instance, is defined as an “engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives” [21]. This foundational work ensures that when different standards or organisations discuss AI, they are operating from a shared set of definitions.

ISO/IEC:2022 [21] states that concepts and categories of AI allow for a comparison and classification of different solutions with respect to properties

like trustworthiness, robustness, resilience, reliability, accuracy, safety, security and privacy, while ISO/IEC TR 24028:2020 [43] has as aim to establish trust in AI systems through transparency, explainability, controllability, etc. present the engineering pitfalls and typical associated threats and risks to AI systems, along with possible mitigation techniques and methods; and provide approaches to assess and achieve availability, resiliency, reliability, accuracy, safety, security and privacy of AI systems to ensure responsible use of AI, traceability, transparency and reliability as stated by ISO/IEC 42001:2023 [180].

Building on this terminological base, SC 42 has developed several framework standards that provide a high-level structure for AI development and management. ISO/IEC 23053:2022 [41], "Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)", is a key document that describes the end-to-end pipeline for ML-based systems. It outlines the distinct phases of the ML lifecycle, including data acquisition and preparation, model training, verification and validation, model deployment, and ongoing operation and monitoring. This standard provides a crucial architectural reference for organisations building and deploying ML solutions.

To integrate AI development into established engineering practices, ISO/IEC 5338:2023 [135], "Information technology - Artificial intelligence - AI system life cycle processes", adapts the well-known software lifecycle processes from ISO/IEC/IEEE 12207-2017 for the unique needs of AI systems. It incorporates the AI system lifecycle phases defined in ISO/IEC 22989:2022 from inception and design through to retirement-and integrates the ML pipeline from ISO/IEC 23053:2022. It introduces new processes specific to AI, such as a knowledge acquisition process for rule-based systems and an "AI data engineering process" to handle the complexities of preparing datasets for model training. The standards are aligned with system and software engineering lifecycle standards ISO/IEC/IEEE standards [55–59].

#### 7.1.1.2 Management Systems, Risk, and Trustworthiness

Perhaps the most impactful standard from SC 42 is ISO/IEC 42001:2023, "Information technology - Artificial intelligence - Management system". This is an AI Management System (AIMS) standard modelled after other successful management system standards like ISO 9001:2015 [181] (quality) and ISO/IEC 27001:2022 [182] (information security), ISO/IEC 42001:2023 provides a structured, certifiable framework for organisations to govern their development, provision, or use of AI systems responsibly. It offers

a systematic approach to managing risks and opportunities related to AI, helping to harmonise innovation with governance and providing a clear path for organisations to demonstrate their commitment to responsible AI practices to regulators, customers, and other stakeholders.

Complementing the AIMS is ISO/IEC 23894:2023 [183], "Information Technology – Artificial Intelligence – Guidance on risk management", which provides specific guidance on implementing risk management for AI systems. The standard adapts the generic principles of ISO 31000:2018 [184] for the unique risks posed by AI, such as algorithmic bias, data quality issues, model drift, and adversarial attacks. It provides methodologies for identifying, assessing, and mitigating these risks throughout the AI system lifecycle, offering a practical framework for both technical and operational risk management.

The concept of trustworthiness is a central theme in SC 42's work, addressed horizontally across multiple documents. ISO/IEC TR 24028:2020, "Information technology – Artificial intelligence - Overview of trustworthiness in artificial intelligence", provides a high-level framework for this concept, breaking it down into constituent components such as reliability, availability, resilience, accountability, safety, security, and privacy. It also introduces key properties like ability, integrity, and benevolence as assessable quality components of trustworthiness.

Specific aspects of trustworthiness are explored in greater detail in dedicated technical reports and standards. ISO/IEC TR 24027:2021 [137], "Information technology – Artificial intelligence - Bias in AI systems and AI aided decision making", provides a comprehensive overview of the sources and types of bias, from human cognitive biases to data-driven and algorithmic biases, and offers methods for their mitigation. The forthcoming ISO/IEC TS 6254:2025 [138], "Information technology - Artificial intelligence - Objectives and approaches for explainability and interpretability of machine learning (ML) models and artificial intelligence (AI) systems" addresses the critical areas of explainability and interpretability of AI systems, providing a taxonomy of explanation needs and methods for assessment.

In this context, the definition of guidelines for the application of data governance and data quality in AI systems is crucial. Addressing bias in the data of technological systems is a significant challenge in the digital age, as the decisions made by algorithms can have substantial societal and personal implications, which can be measured according to the ISO/IEC standards [132].

#### 7.1.1.3 Quality and Data for AI Systems

Recognising that AI systems are fundamentally software-based, SC 42 has worked in close collaboration with ISO/IEC JTC 1/SC 7 (Software and systems engineering) to adapt existing software quality models for AI. The forthcoming ISO/IEC 25059:2023 [136], Quality model for AI-based systems, extends the widely used SQuaRE series (ISO/IEC 25000) [44–52]. It proposes modifications to the standard quality characteristics defined in ISO/IEC 25010:2023 to make them more relevant for AI. For example, it adds "User Controllability" and "Transparency" as sub-characteristics of Usability, and "Robustness" as a sub-characteristic of reliability, reflecting the unique quality demands of intelligent systems.

Data is key for AI and edge AI systems, and its quality is paramount. SC 42 has dedicated a significant effort to standardising data quality specifically for analytics and machine learning. The ISO/IEC 5259 series of standards provide a complete foundation for this topic. This multi-part standard is crucial because it differentiates between the quality of general-purpose data, covered by ISO/IEC 25012:2008, and the specific quality requirements of datasets used for training, validation, and testing ML models. While ISO/IEC 25012:2008 addresses characteristics like accuracy and completeness, the ISO/IEC 5259 series introduce additional, ML-specific characteristics such as "balance," "diversity," "relevance," and "representativeness," which are critical for building fair and effective models. ISO/IEC 5259-2:2024 [141] provides explicit data quality measures for these new characteristics, while other parts cover management requirements and a process framework. ISO/IEC 5339:2024 guides AI applications based on a common framework to provide multiple macro-level perspectives. The framework incorporates "make", "use" and "impact" perspectives. It includes AI characteristics and non-functional characteristics such as trustworthiness and risk management. The guidance can be used by standards developers, application developers, and other interested parties to provide answers to the question: "What are the characteristics and considerations of an AI application?". The stakeholders are mapped to various stages of the AI system life cycle, highlighting their roles and responsibilities and making them aware of the processes to follow to enable a coherent stakeholder engagement for the AI application. These stakeholders can have various levels of AI expertise and knowledge. Since AI applications can differ from non-AI software applications due to their continuously evolving nature and aspects of trustworthiness, all stakeholders should be made aware of AI-specific characteristics [134].

A defining characteristic of SC 42's strategy is the development of a deeply interconnected system of standards rather than a collection of isolated documents. This architectural approach ensures coherence and interoperability across the portfolio. For example, the terminology defined in ISO/IEC 22989:2022 is the common language used throughout all other SC 42 standards, including the AIMS in ISO/IEC 42001:2023. The risk management principles from ISO/IEC 23894:2023 are an integral component of the management system defined in ISO/IEC 42001:2023. Likewise, the data quality requirements from the ISO/IEC 5259 series are essential inputs for the ML framework described in ISO/IEC 23053:2022. This deliberate design creates a holistic and non-contradictory suite of standards that organisations can use together to build and govern complex, trustworthy AI systems from the ground up.

Despite the comprehensive nature of this foundational work, a review of the published and active projects within SC 42 reveals a conspicuous absence of standards explicitly scoped for edge AI. The portfolio focuses almost entirely on horizontal concepts-risk, governance, quality, data-that apply to AI systems regardless of their deployment environment. This implies that, from the perspective of ISO and IEC, edge AI is not considered a fundamentally new technological paradigm requiring its unique foundational standards. Instead, it is viewed as a specific deployment context or application domain. An organisation developing an edge AI system would be expected to apply the existing ISO/IEC standards for risk management, data quality, and governance, just as an organisation developing a cloud-based AI system would. This strategic choice to remain horizontal and foundational creates an opportunity and a clear need for other, more specialised SDOs to develop the practical, implementation-focused standards required for the unique challenges of the edge.

### 7.1.2 IEEE: A Focus on Ethics and Practical Implementation

The Institute of Electrical and Electronics Engineers (IEEE) has established a distinctive and influential position in the AI standardisation landscape through a dual-focus strategy. At the same time, the IEEE Standards Association (IEEE SA) has become a global leader in developing frameworks to address the ethical and societal dimensions of AI, translating abstract principles into actionable engineering processes. In this context, IEEE SA's technical committees, are developing efficient, engineering-centric standards

that address specific implementation challenges, with a notable pioneering role in the domain of edge AI [152].

#### 7.1.2.1 The Ethical Dimension: Codifying Principles in the P7000 Series

The IEEE's most visible contribution to responsible AI is the P7000™ series of standards, a comprehensive portfolio dedicated to "Ethically Aligned Design". The P7000 series represents a concerted effort to systematically embed ethical considerations into the AI system design and development lifecycle. The P7000 series is designed to provide engineers and developers with concrete, actionable processes and guidelines, and effectively bridges the gap between high-level ethical principles and day-to-day engineering practice to ensure that values are built into systems by design, not merely assessed as an afterthought.

The flagship standard of this series is IEEE 7000-2021 [189], "IEEE Standard Model Process for Addressing Ethical Concerns During System Design". It provides a systematic process for identifying and analysing potential ethical issues from the outset of a project, integrating value-based considerations into system requirements and design choices. This is complemented by IEEE 7001-2021 [190], "IEEE Standard for Transparency of Autonomous Systems", which specifies what information about an AI system should be accessible and to whom, providing a framework for clear and understandable disclosures.

Other key standards in the series tackle specific ethical challenges. IEEE 7003-2024 [192], "IEEE Standard for Algorithmic Bias Considerations", guides identifying and mitigating unintended bias in algorithms, a critical issue for fairness and equity.

IEEE 7002-2022 [191], "IEEE Standard Data Privacy Process", defines a process for managing data privacy throughout the system lifecycle, aligning with global privacy principles [109–112]. The series extends to a wide range of societal concerns, with standards addressing the governance of child and student data (IEEE P7004-2020 [193], "Standard for Child and Student Data Governance"), fail-safe design for autonomous systems (IEEE 7009-2024 [195], "IEEE Standard for Fail-Safe Design of Autonomous and Semi-Autonomous Systems"), and even the ethics of AI-driven "nudging" (IEEE P7008-2017 [194], "Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems"). To further promote these principles, IEEE SA has also launched certification programs like IEEE CertifAIEd™

to assess the ethics in the creation and implementation of Autonomous Intelligent Systems (AIS).

#### 7.1.2.2 The Practical Dimension: Standardising Edge AI Implementation

While ISO/IEC provides the foundational "what" and "why" of AI governance, IEEE has taken a leading role in defining the practical "how" of edge AI implementation. Recognising the unique engineering challenges of deploying AI on resource-constrained devices, IEEE has initiated several standards projects that provide concrete guidance for developers and system architects [153]. This work fills a critical gap left by the more abstract, horizontal standards from other organisations and is driven by a bottom-up response to immediate engineering needs in the rapidly growing edge AI market.

A landmark project in this area is IEEE P3342-2023 [125], "Standard for Functional Requirements of Toolchain for Artificial Intelligence Model Deployment on Edge Devices". This standard is one of the first of its kind to directly address the end-to-end engineering pipeline required to take a trained AI model and make it run efficiently at the edge. Its scope covers the entire toolchain, specifying functional requirements for crucial steps such as frontend adaptation (converting models from different frameworks), model compression (e.g., quantisation and pruning to reduce size and computational cost), graph optimisation (to streamline model execution), backend adaptation (targeting specific edge hardware), and runtime optimisation. This provides a standardised blueprint for building the software infrastructure needed to operationalise edge AI.

Another key standard is IEEE P2975.3-2023 [154], "Recommended Practice for Software Framework for Industrial Artificial Intelligence (AI) at-the-edge". This project focuses on a key vertical application for edge AI: industrial control systems. It describes a software framework, including key features and software building blocks, for deploying AI at the edge in a manufacturing or industrial context. This is vital for applications like predictive maintenance and process automation, where low latency and high reliability are paramount. By defining functionalities and interfaces, this standard promotes interoperability and simplifies the integration of AI into complex industrial environments [154].

Beyond these specific edge standards, IEEE is also working on related enabling technologies. For example, IEEE P3652.1-2020, "Guide for Architectural Framework and Application of Federated Machine Learning",

addresses a key technique for training AI models across distributed devices without centralising sensitive data. This is inherently an edge-centric paradigm that is crucial for privacy-preserving AI in sectors like healthcare and consumer electronics. These practical, engineering-focused standards demonstrate IEEE's focus to provide the tangible tools and frameworks necessary to build and deploy real-world AI and edge AI systems.

### 7.1.3 ETSI: Standardising AI for the Communications and Edge Ecosystem

The European Telecommunications Standards Institute (ETSI) plays a unique and critical role in the AI standardisation landscape, with a primary focus on enabling AI and edge AI applications [155] through the standardisation of network and communications infrastructure. ETSI's strategy can be understood not as an attempt to standardise AI algorithms or models themselves, but rather to standardise the underlying "plumbing" the network platforms and architectures that allows innovative AI services to be deployed efficiently, securely, and at scale. This network-centric approach is epitomised by its pioneering work in Multi-access Edge Computing (MEC), which has become a foundational technology for the entire edge AI ecosystem.

#### 7.1.3.1 Multi-access Edge Computing (MEC) as the Enabler for Edge AI

ETSI's Industry Specification Group on Multi-access Edge Computing (ISG MEC) was established to create a standardised, open environment that brings cloud-computing capabilities to the edge of the network, typically within the Radio Access Network (RAN) [146]. The MEC architecture is designed to provide an IT service environment characterised by properties that are essential for high-performance edge AI: ultra-low latency, high bandwidth, and real-time access to radio network information that applications can leverage for context-aware operations. By creating this standardised platform, ETSI enables a competitive ecosystem where third-party application developers, including AI service providers, can deploy their services on any compliant operator's network, fostering innovation on top of a stable infrastructure.

The link between MEC and the requirements of edge AI is direct and explicit. ETSI's white paper, "MEC support towards Edge Native Design", details how the MEC platform is purpose-built to address the challenges of running sophisticated AI applications at the edge. Many modern AI models, large language models or high-resolution video analytics models, are too

computationally intensive to run on resource-constrained end-user devices like smartphones or IoT sensors. MEC provides the solution by enabling task offloading, where these intensive computational workloads can be moved to a nearby MEC server within the network, achieving low-latency processing without the long round-trip delay of sending data to a distant cloud data centre [157]. This capability is critical for use cases like real-time augmented reality, interactive gaming, V2X communications, and industrial automation.

ETSI has published a comprehensive set of specifications that define the MEC architecture and its interfaces [156–158]. Key standards include ETSI GS MEC 003, which describes the Framework and Reference Architecture, and ETSI GS MEC 011, which specifies Edge Platform Application Enablement. These standards detail how applications are managed, how they discover and consume edge services, and how they interact with the underlying network. This standardised framework is the key to enabling a multi-vendor, multi-operator edge ecosystem where AI applications can be deployed seamlessly.

#### 7.1.3.2 Securing AI and Fostering Network Evolution

Beyond enabling the platform, ETSI is also addressing the security of the AI systems that will run on it. The ETSI Technical Committee on Securing AI (TC SAI) was formed to tackle the novel security vulnerabilities associated with AI systems, such as prompt injection and data poisoning attacks. In a significant development, TC SAI has produced a technical specification on Baseline Cyber Security Requirements for AI Models and Systems [159]. This is reported to be the first global standard that defines a robust set of minimum-security requirements that apply across the entire AI lifecycle, from secure design and development to secure deployment, maintenance, and end-of-life. This provides a crucial security baseline for all stakeholders in the AI supply chain, from model developers to system operators.

The demanding requirements of edge AI applications are not only served by the network but are also a powerful force driving the evolution of the network itself. The need for ultra-low latency and high throughput required by data-intensive AI models is a significant catalyst for the deployment of 5G networks and the continued development of MEC and future 6G architectures. AI is not merely a passive service running on the network; its performance requirements are actively shaping the design and capabilities of next-generation communication systems. This positions AI as a key business driver for telecommunication operators, who can leverage their MEC

infrastructure to offer premium, low-latency services for a new generation of intelligent applications.

ETSI's work also extends to fostering data interoperability for AI agents [160]. Recognising that the proliferation of autonomous AI applications will create complex data sharing patterns, ETSI has launched a group to develop technical standards for data and semantic interoperability. This work will address fundamental aspects like data representation, access control, and privacy preservation, initially focusing on telecom networks and later expanding to other sectors like industrial applications and eHealth. Through these multifaceted efforts, ETSI is building the critical network and security infrastructure necessary for a robust and trustworthy edge AI ecosystem.

### 7.1.4 ITU-T: Integrating AI into Global Telecommunication Networks

ITU-T approaches AI standardisation from the perspective of a global standards body responsible for the interoperability and operation of worldwide telecommunication networks. Its work is primarily focused on how AI can be integrated into the fabric of these networks to improve their efficiency, enable new services, and manage their increasing complexity. This network-centric viewpoint leads to a focus on "AI for networks" (AI4N) and the development of architectures where intelligence is a native component of the network itself [162, 164].

#### 7.1.4.1 From AI for Networks to AI-Native Architectures

The central body for this work within the ITU-T is Study Group 13 (SG13), which serves as the lead study group on "Future networks and emerging network technologies," with a specific mandate covering the application of AI and machine learning in networks. A foundational document from this group is Recommendation ITU-T Y.3172, Architectural framework for machine learning in future networks including IMT-2020. Approved in 2019, this recommendation was one of the first to provide a standardised architecture for embedding ML functions within the network, defining logical components and interfaces for tasks like data collection, model training, and policy-driven network management.

Building on this foundation, the ITU-T's vision has evolved towards the concept of "AI-native" networks. In July 2024, SG13 established a new Focus Group on AI-Native for Telecommunication Networks (FG-AINN)

[162, 163]. This group's objective is to explore the fundamental architectural changes required to move beyond simply applying AI to existing networks and instead to design networks where AI is deeply embedded in the core architecture from the ground up. The goal is to create networks capable of self-management, self-optimisation, and self-repair, enabling unprecedented levels of automation and intelligence to meet the demands of future applications requiring extreme agility and precision [162]. This work represents a paradigm shift, viewing AI not as an add-on tool but as an intrinsic property of the network itself.

This focus on using AI to manage and optimise the network infrastructure is a key differentiator for the ITU-T. Concepts like "autonomous networks" and "AI-native networks" are primarily concerned with making the network more efficient, resilient, and automated for the benefit of the network operator [161]. Use cases being explored by groups like FG-AINN include using large language models for network anomaly resolution and AI-based modelling for network optimisation. This "AI for the network" perspective is distinct from the "AI on the network" perspective of application developers, positioning the network operator as the primary user of the AI technology being standardised.

#### 7.1.4.2 Standardising Intelligent Edge Computing (IEC)

The ITU-T has formally recognised and standardised the convergence of edge computing and artificial intelligence through its work on "Intelligent Edge Computing" (IEC). This work acknowledges that the network edge is not just a location for distributed processing but a critical point of intelligence within the overall network architecture. Recommendation ITU-T Q.5001 [166] defines IEC and specifies its architecture, signalling requirements, and use cases [165]. The standard explicitly states that IEC solves issues like network bottlenecks by "applying the intelligent data processing functions by providing AI technologies" at the edge. Its focus on supporting mission-critical services underscores the understanding that this localised intelligence is crucial for reliable, high-stakes applications.

This holistic view, which integrates network intelligence with edge deployment, is further developed in other ITU-T recommendations. For example, Recommendation ITU-T Y.4122 [167] specifies the requirements and capability framework for an "edge-computing-enabled gateway" on the IoT. This standard recognises that edge gateways in IoT systems must support not only connectivity but also intelligence, providing computation and data processing near IoT devices.

Furthermore, the ITU-T addresses the application of IEC in specific vertical domains. Recommendation ITU-T X.1384 provides security requirements and guidelines specifically for vehicular edge computing (VEC). It analyses the unique threats associated with deploying AI-driven services for intelligent transport systems at the edge and provides the necessary security requirements to ensure their safe deployment. This work demonstrates a clear understanding that the combination of AI and edge computing requires domain-specific considerations for safety and security.

In addition to its technical work, the ITU-T also considers the broader impacts of AI [60]. Its journal has explored the topic of sustainable AI at the network edge, investigating innovations for energy efficiency through hardware-software co-design, energy-aware decision-making, and sustainable AI applications [168]. This reflects a growing awareness that the widespread deployment of AI, particularly at the edge, must be balanced with environmental considerations. Through these combined efforts, the ITU-T is building a comprehensive framework for integrating intelligence into the core and edge of global telecommunication networks.

### 7.1.5 CEN-CENELEC: Harmonising Standards for the European AI Act

The work of CEN and CENELEC in the field of AI is unique among SDOs as the activities of JTC 21 are driven by a top-down regulatory mandate. The goal is to develop European standards in support of EU legislation as illustrated in Figure 7.1 [143].

The CEN-CENELEC Joint Technical Committee 21 (JTC 21) was established with the specific purpose of developing the technical standards needed to support the European Union's AI Act [126, 169]. This makes JTC 21 a critical instrument of public policy, tasked with translating the legal requirements of the world's first comprehensive AI regulation into practical, implementable technical specifications for industry.

#### 7.1.5.1 A Mandate for Harmonised Standards

The work of CEN-CENELEC JTC 21 is inscribed within a particular regulatory framework at EU level that aims to harmonise essential product requirements across EU Member States. For this purpose, Regulation (EU) No. 1025/2012 empowers the European Commission to request the drawing up of European harmonised Standards ('hENs') by ESOs [127]. These standards shall address essential product requirements and may be applied

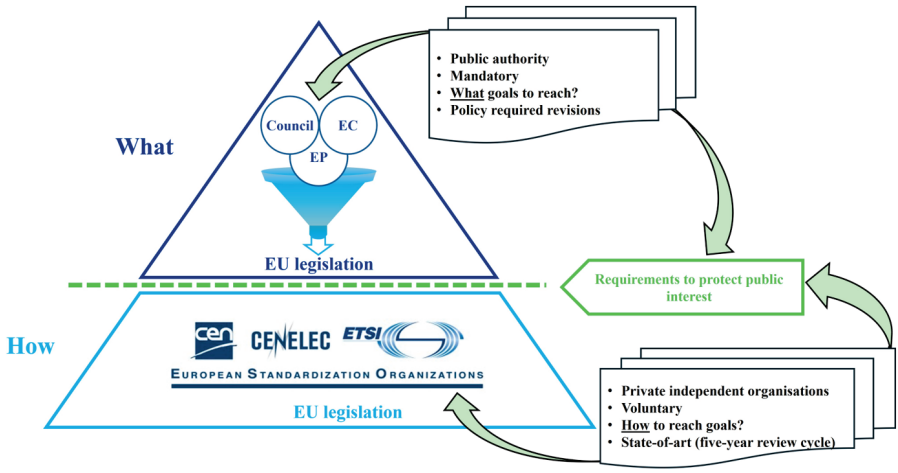


**Figure 7.1** European standards in support of EU legislation [143, 69].

alongside relevant product legislation. This regulatory framework recognises, inter alia, the importance of market-driven processes taking place within ESOs and expert consensus for the implementation of EU product legislation.[1]

The power conferred upon the Commission under the Artificial Intelligence Act ('AIA') to request the development of hENs is an application of this regulatory framework.[2] It is against this regulatory background that the Commission has issued a standardisation request to the CEN-CENELEC in May 2023 for the drafting of European standards and standardisation deliverables covering all the essential requirements applicable to high-risk AI systems, AI providers' quality management systems and conformity assessments for AI systems [128]. While the preparation of these standards is underway within the JTC 21, none of the requested standard has been formally published at the time of writing.[3]

AI providers may choose to comply with these future standards for demonstrating the compliance of their high-risk AI system with the AIA's

[1] See article 10 of Regulation (EU) No. 1025/2012, stating that 'European standards and European standardization deliverables shall be market-driven, take into account the public interest as well as the policy objectives clearly stated in the Commission's request and be based on consensus'.

[2] See article 40 of Regulation (EU) 2024/1689. See also the developments on that Regulation in section 6.2.

[3] Note that the Commission's standardization request is valid until 28 February 2026.

essential requirements. Doing so will create a presumption of conformity with all or parts of these requirements and, in certain cases, adapt the types of conformity assessment procedure that must be followed [115]. Reliance on these standards remains, however, voluntary and does not exempt AI providers from their responsibility to comply with the regulation's provisions.

These standards should provide a clear and predictable pathway for manufacturers to demonstrate compliance, significantly reducing legal uncertainty and streamlining market access. This process elevates the role of standardisation from a source of best practices to an integral component of the legal and regulatory framework. The development process itself reflects this unique status, involving formal steps such as drafting by technical experts, public enquiry, voting by national standards bodies, and finally, assessment by the Commission and citation in the Official Journal of the European Union, which gives them their legal force.

#### 7.1.5.2 Key Standards for AI Act Compliance

The work programme of JTC 21 is directly structured to address the key requirements laid out in the AI Act for high-risk AI systems. The committee is developing a suite of core standards that provide the operational frameworks needed for compliance. These include a standard for AI Risk Management, which will give a definitive approach for EU organisations. This standard builds upon international work like ISO/IEC 23894:2023, being tailored to the European context by integrating the AI Act's risk classification categories (high-risk, limited risk, minimal risk) and providing detailed assessment templates and mitigation strategies aligned with the regulation [147].

Another critical deliverable is a standard for an AI Quality Management System (QMS) [6, 115, 119]. Article 17 of the AI Act mandates that providers of high-risk AI systems implement a QMS. The JTC 21 standard will provide the technical specifications for such a system. It is expected to build upon the international AI Management System standard, ISO/IEC 42001:2023, but will add specific European requirements related to regulatory reporting, post-market monitoring, and conformity assessment procedures as stipulated by the Act.

These foundational management standards are being supplemented by a portfolio of more specific standards that address other key requirements of the AIA. This includes work on data governance and quality, ensuring that datasets used to train high-risk systems are of sufficient quality to prevent bias and errors. Other projects focus on transparency, with standards for logging

to ensure that the operational history of an AI system can be traced and audited; robustness, to ensure systems perform reliably under pressure; and cybersecurity, to protect systems from malicious attacks [115, 119].

#### 7.1.5.3 The Strategy of "Europeanisation"

JTC 21's strategy is to adopt and adapt [119]. The committee actively collaborates with international SDOs, primarily ISO/IEC, through the Vienna Agreement. Its approach is to adopt international standards wherever they are suitable, such as using ISO/IEC 22989:2022 for terminology and ISO/IEC 23053:2022 as the framework for ML systems. This promotes global alignment and prevents unnecessary duplication of effort.

However, where the EU AI Act imposes requirements that go beyond existing international standards-particularly in areas related to fundamental rights, specific high-risk applications, or conformity assessment procedures, JTC 21 is tasked with developing "homegrown" European standards or adapting international ones to fill these gaps. This process of adaptation leads to the "Europeanisation" of global standards. The resulting European standards, such as the forthcoming QMS and risk management standards, will represent a version of the international standards that has been enhanced with additional layers of regulatory rigour. Because the EU is such a significant global market, companies worldwide that wish to sell their AI products in Europe will likely need to adhere to these more stringent, "Europeanized" standards. This has the potential to export European policy and values globally, making the work of JTC 21 a powerful force in shaping the global benchmarks for trustworthy and regulation-compliant AI.

### 7.1.6 Analysis of the AI and Edge AI Standardisation Domains

The global landscape of AI standardisation is a complex tapestry woven by multiple organisations, each with its philosophy, focus, and constituency. While their efforts are largely complementary, understanding their distinct roles is crucial for navigating this environment. A comparative analysis reveals a logical, multi-layered structure, with different SDOs addressing different levels of the AI technology stack, from foundational principles to network infrastructure and practical implementation. The domain of edge AI highlights this multi-layered approach, as its standardisation is not happening in a single committee but at the convergence of several distinct technological streams.

### 7.1.7 Comparative Analysis of SDO Philosophies and Focus Areas

The major SDOs have carved out complementary niches, reflecting their institutional histories and expertise. ISO/IEC, through JTC 1/SC 42, operates at the most foundational and horizontal level. Its purpose is to create a stable, globally applicable, and consensus-driven architectural framework for AI [148].

The system of standards approach focuses on defining the core building blocks, terminology, management systems, risk and quality frameworks, and data principles, that apply to all AI systems, regardless of their application domain or deployment environment.

The IEEE takes a more hands-on, engineering-oriented approach. It operates on a dual track: its P7000 series translates high-level ethical principles into actionable design processes for engineers, while its technical committees develop practical, bottom-up standards that solve immediate implementation challenges [152]. The work in standardising toolchains and frameworks for edge AI demonstrates a focus on the "how-to" of building real-world systems [125].

The telecommunications-focused SDOs, ETSI and ITU-T, view AI through the lens of network architecture and management. Their primary concern is not the internal workings of AI models but how to enable, manage, and secure AI-driven services on communication networks. ETSI's work on Multi-access Edge Computing (MEC) is a prime example of standardising the network infrastructure, the "plumbing", to create an open platform for edge AI applications. The ITU-T, meanwhile, focuses on using AI as a tool to manage the network itself, with its vision of "AI-native" networks that are self-optimising and autonomous [161].

Finally, CEN-CENELEC has a unique and highly focused role. Its work in JTC 21 is entirely top-down and regulation-driven, with the explicit mandate to create harmonised standards that provide a presumption of conformity with the EU AI Act [9].

The focus is on translating legal requirements into technical specifications for risk management, quality, and conformity assessment, making it the key SDO for organisations concerned with regulatory compliance in the European market [119].

Table 7.1 provides a comparative overview of the primary focus areas for each of these SDOs, highlighting their key committees and flagship standards or projects.

**Table 7.1** Comparative overview of the primary focus areas for each of the SDOs.

| Standardisation Domain | ISO/IEC | IEEE | ETSI | ITU-T | CEN-CENELEC |
|---|---|---|---|---|---|
| **Foundational Concepts and Terminology** | **Lead:** JTC 1/SC 42 (ISO/IEC 22989, 23053) | Contributor (P3123) | Adopts/ References | Adopts/ References | **Lead (EU):** JTC 21 (Adopts ISO/IEC 22989) |
| **Risk Management** | **Lead:** JTC 1/SC 42 (ISO/IEC 23894) | Contributor (P3396) | Addresses in security context | Addresses in network context | **Lead (EU):** JTC 21 (European AI Risk Mgt. Std.) |
| **Quality and Trustworthiness** | **Lead:** JTC 1/SC 42 (ISO/IEC 25059, TR 24028) | Contributor (P3396) | Focus on testing (MTS) & security (SAI) | Focus on QoS | **Lead (EU):** JTC 21 (AI Trustworthiness Framework) |
| **AI Management Systems** | **Lead:** JTC 1/SC 42 (ISO/IEC 42001) | Contributor | | | **Lead (EU):** JTC 21 (AI QMS for Reg. Purposes) |
| **Ethics and Societal Concerns** | Contributor (TR 24368, TR 24027 on bias) | **Lead:** P7000 Series (7000, 7001, 7003) | Contributor | Contributor | **Lead (EU):** JTC 21 (Foundational & Societal Aspects WG) |
| **Data Quality and Governance** | **Lead:** JTC 1/SC 42 (ISO/IEC 5259 series) | Contributor (P2801 for medical) | Contributor (ISG for AI agents) | | **Lead (EU):** JTC 21 (Standards on datasets) |
| **Network Integration and Management** | | Contributor (2040-2023) | **Lead:** ZSM, ENI | **Lead:** SG13 (FG-AINN, Y.3172) | |
| **Edge AI Platforms (MEC)** | | | **Lead:** ISG MEC (GS MEC 003, 011) | Contributor (Q.5001) | |
| **Edge AI Implementation and Toolchains** | | **Lead:** C/AISC (P3342), C/SM (P2975.3) | | Contributor (IEC use cases) | |
| **Regulatory Compliance (EU AI Act)** | Provides foundational inputs | | Provides inputs for telecom | | **Lead:** JTC 21 |

### 7.1.8 The State of Edge AI Standardisation

As the analysis and table indicate, edge AI standardisation is an emerging field that is not being driven by a single, dedicated committee but is instead coalescing from the work of multiple SDOs with different perspectives on what "the edge" is. There are three primary viewpoints shaping the landscape.

First is the Network Edge perspective, led by ETSI and the ITU-T. Here, the edge is a location within the telecommunications network infrastructure. The focus is on standardising platforms like MEC and Intelligent Edge Computing (IEC) to provide the low-latency, high-bandwidth environment that enables real-time AI services. *7* This view is concerned with service delivery, network management, and creating an ecosystem for applications.

Second is the device edge perspective, led by the IEEE. Here, the edge refers to the end-user devices themselves, such as industrial controllers, IoT sensors, or autonomous vehicles [125]. The focus is on the practical engineering challenges of deploying AI models on these resource-constrained devices. Standardisation efforts like IEEE P3342-2023 (toolchains) and P2975.3-2023 (industrial frameworks) are designed to provide developers with the specific tools and software architectures they need to make AI work in these environments [125].

Third is the Foundational Principles perspective, led by ISO/IEC. From this viewpoint, the location of deployment, be it cloud or edge, is secondary to the need for universal principles of governance. The standards for risk management (ISO/IEC 23894:2023), quality (ISO/IEC 25059:2023), and data management (ISO/IEC 5259 series) are designed to be applied to any AI system, providing the essential underpinnings for trustworthiness regardless of where the computation occurs.

These three streams are highly synergistic. An organisation building a sophisticated edge AI product for the industrial sector might use ISO/IEC 42001:2023 to establish its AI management system, follow the guidance in IEEE P2975.3-2023 to design its software framework, use tools compliant with IEEE P3342-2023 to deploy its models, and run its application on a network operator's MEC platform that conforms to ETSI standards. However, a significant gap remains, as noted in the initial analysis: there is no single, unified, and comprehensive set of standards that covers the entire edge AI lifecycle holistically. A key challenge for the future will be the harmonisation of terminology and frameworks across these different perspectives to create a more seamless and less fragmented standardisation environment for the burgeoning edge AI industry.

Based on the analysis and the overview of the AI standards discussed, Table 7.2 lists the primary AI standards and standardisation activities in the standard development organisations mentioned in this chapter.

**Table 7.2** Relevant AI standards and standardization activities

| | |
|---|---|
| **ITU-T - International Telecommunication Union - Telecommunication Standardization Sector** | |
| Y.Suppl.63 to ITU-T Y.4000 series | Unlocking the Internet of Things with artificial intelligence: Where we are and where we could be. |
| **CEN-CENELEC - European Committee for Normalization / European Committee for Electrotechnical Standardization** | |
| FG on AI | Focus Group on Artificial Intelligence. It was the first and only contributor on AI topics in CEN and created a set of interesting documents on first ideas on AI (late 2010') later superseded by a CEN/CLC JTC 21 on AI. |
| JTC 21 | Joint Technical Committee 21 "Artificial Intelligence". It identifies and adopts international standards already available or under development from other organizations like ISO/IEC JTC 1 and its subcommittees, such as SC 42 Artificial Intelligence. Furthermore, it focuses on producing standardization deliverables that address European market and societal needs, as well as underpinning EU legislation, policies, principles, and values. |
| **ISO/IEC - International Organization for Standards / International Electrotechnical Commission** | |
| JTC 1/SC 42 | Artificial Intelligence. This overarching JTC focuses on different aspects of AI, produces a set of standards (among which the ISO/IEC 8183: Artificial intelligence - Data life cycle framework) and is composed of a set of WGs. |
| WG 1 | Foundational standards. |
| WG 3 | Trustworthiness. |
| WG 4 | Use cases and applications. |
| WG 5 | Computational approaches and characteristics of artificial intelligence systems. |
| JWG 4 | It administers several Joint WGs with other subcommittees e.g., with IEC TC65/SC65A: Functional safety and AI systems. |
| TR 24027 | Information technology - Artificial Intelligence (AI) – Bias in AI systems and AI-aided decision making. |
| TR 24028:2020 | Information technology - Artificial intelligence - Overview of trustworthiness in artificial intelligence [43]. |
| DTR 24029-1 | Artificial Intelligence (AI) - Assessment of the robustness of neural networks - Part 1: Overview [139]. |
| AWI 24029-2 | Artificial Intelligence (AI) - Assessment of the robustness of neural networks - Part 2: Methodology for the use of formal methods [142]. |

**Table 7.2** *Continued.*

| | |
|---|---|
| WD 5259-1 | Data quality for analytics and ML - Part 1: Overview, terminology, and examples. |
| WD 5259-2 | Data quality for analytics and ML - Part 2: Data quality measures |
| WD 5259-3 | Data quality for analytics and ML - Part 3: Data quality management requirements and guidelines. |
| WD 5259-4 | Data quality for analytics and ML - Part 4: Data quality process framework |
| WD 5338 | Information technology - Artificial intelligence - AI system life cycle processes. |
| AWI TR 24368 | Information technology - Artificial intelligence - Overview of ethical and societal concerns. |
| AWI TR 24372 | Information technology - Artificial intelligence (AI) - Overview of computational approaches for AI systems. |
| 25012:2008 | Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Data quality model. |
| WD TS 4213 | Information technology - Artificial Intelligence - Assessment of machine learning classification performance [140]. |
| 23894:2023 | Information Technology – Artificial Intelligence – Guidance on Risk Management. |
| WD 42001 | Information Technology - Artificial intelligence - Management system. |
| AWI 25059 | Software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Quality model for AI-based systems. |
| **ETSI - European Telecommunications Standards Institute** | |
| OCG AI | Co-ordination Group on Artificial Intelligence. It acts as a coordination group for the standardisation activities related to AI handled in the technical bodies and committees and ISGs of ETSI. |
| ISG ENI | Industry Specification Group Experiential Network Intelligence. It focuses on leveraging AI methods to increase the dynamicity, adaptability and reaction of telecommunication networks and its acting entities, and on the following MARS-related topics: develop standards for a Cognitive Network Management system, incorporating one or more closed control loops; provide a telemetry processing framework that uses context and situation awareness to learn and reason about which data should be collected using what types of processing mechanisms to support information collection and measurement about network performance, network resources and services. |
| **IEEE SA- Institute of Electrical and Electronics Engineers Standard Association** | |
| A-IS | Autonomous and Intelligent Systems. It ensures that every stakeholder involved in the design and development of autonomous and intelligent systems is educated, trained, and empowered to prioritize ethical considerations so that these technologies are advanced for the benefit of humanity. |

**Table 7.2** *Continued.*

| | |
|---|---|
| ECPAIS | Ethics Certification Program for Autonomous and Intelligent Systems. It focuses on certification and marking processes that advance transparency, accountability, and reduction in algorithmic bias in (A-IS). |
| P3333.1.3 | Standard for the Deep Learning-Based Assessment of Visual Experience Based on Human Factors. |
| P3652.1-2020 | Guide for Architectural Framework and Application of Federated Machine Learning. |
| P2805.3 | Cloud-Edge Collaboration Protocols for Machine Learning. It specifies the collaboration protocols of enabling ML on the edge computing node with support from industrial clouds and provides implementation reference for ML on lower powered, cheaper, embedded devices. |
| P2961 | Guide for an Architectural Framework and Application for Collaborative Edge Computing. It defines a ML framework that allows a computing task to be decomposed and distributed across edge and cloud nodes, the architectural framework and application guidelines for collaborative edge computing, and provides a blueprint for data usage, ML, and computing collaboration in edge computing environments. |

## 7.2 Spatial Web Standards

The IEEE 2874-2025 "Standard for Spatial Web Protocol, Architecture and Governance" defines the foundational specifications for a reference model of the Spatial Web, a system designed to integrate physical and virtual environments into a globally accessible, interoperable, and governable framework [59]. This standard addresses the convergence of distributed edge technologies, including extended reality (XR), artificial intelligence (AI), autonomous systems, robotics, and the Internet of Things (IoT) to create a cohesive cyber-physical ecosystem [59]. It serves as a foundational standard that defines compliance for subsequent Implementation Specifications and domain-specific architectures.

As a sociotechnical standard, the IEEE 2874-2025 Spatial Web Standard establishes foundational requirements that are implemented through separate Implementation Specifications to address the following key requirements:

- **Semantic Interoperability:** Establish a shared ontological framework for representing and exchanging meaning between human and AI agents within the Spatial Web.
- **System Explainability:** Enable the modelling and representation of intelligent agent activities and decision-making to enhance transparency and accountability.

- **Cross-Domain Interoperability:** Facilitate universal data and model interoperability in the continuum compute to enable collaboration across organizational, network, and jurisdictional boundaries.
- **Regulatory Compliance:** Ensure adherence to diverse local, regional, national, and international regulations, cultural norms, and ethical standards through built-in governance mechanisms.
- **Identity and Access Management:** Implement decentralized authentication and credentialing systems with privacy and security safeguards to enable fine-grained control over system activities and resources.
- **Multi-Scale Cognitive Computing:** Support distributed, multi-agent AI systems operating across various scales of the Spatial Web ecosystem.
- **Polycentric Governance:** Enable flexible, context-specific governance models that can adapt to diverse domains and use cases within the Spatial Web.
- **Hyperspace Representation:** Provide a framework for representing and navigating multi-dimensional spaces, including physical, virtual, and abstract domains.
- **Real-time Interaction:** Support low-latency, high-fidelity interactions between users, AI agents, and digital twins across the Spatial Web.

The IEEE 2874-2025 standard framework encompasses core components including the Hyperspace Modelling Language (HSML), the Hyperspace Transaction Protocol (HSTP), the Universal Domain Graph (UDG) and a governance framework designed to address ethical, legal, and social considerations in AI deployment and autonomous technologies at the edge. These components are formalized through separate Implementation Specifications that define compliance requirements.

### 7.2.1 HSML

The Hyperspace Modelling Language (HSML) is a human- and machine-readable semantic modelling language and ontology that provides a shared vocabulary for Domains, Entities, Agents, Activities, Credentials, Channels, and Hyperspaces within the Spatial Web. HSML leverages W3C standards (RDF, OWL, SHACL, and others) to express and validate formal statements and updates, enforcing structure and constraints across heterogeneous implementations. It supports multiple spatial or relational structures including topological, metric, cellular, and vector spaces via well-defined hyperspace

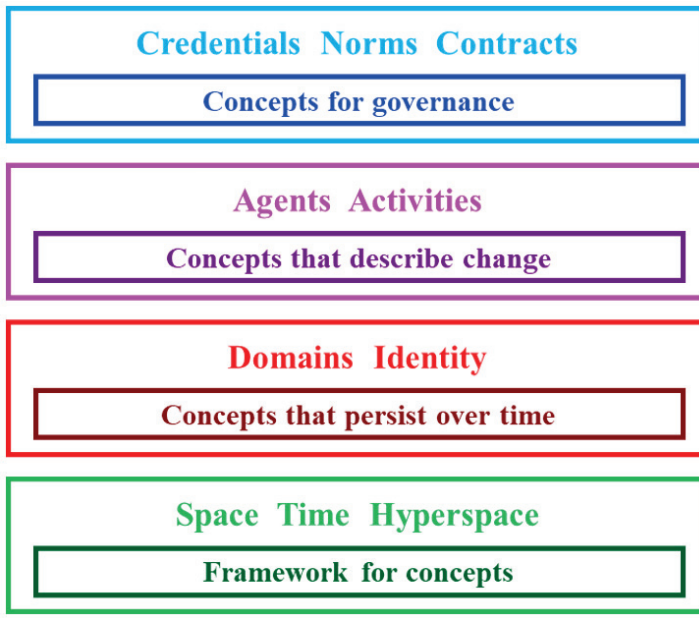


**Figure 7.2** HSML knowledge model

constructs such as points, paths, subspaces, tensor products, and structure-preserving morphisms. HSML requires the use of Spatial Web Identifiers (SWIDs) conformant with W3C DID Core for decentralized identity and discoverability. Figure 7.2 illustrates the HSML knowledge model [79].

### 7.2.2 UDG

The Universal Domain Graph (UDG) refers to the interconnected network of graphs from all domains within both the physical and digital worlds, along with their relationships within the Spatial Web ecosystem. A domain is defined as an entity with a persistent Spatial Web Identifier (SWID) endowed with specific rights and credentials over time. A Domain Authority is an entity credentialed to define the norms and terms governing actors, actions, and credentials within that domain's scope. The UDG comprises nodes representing entities and edges representing the semantic relationships between these entities. The UDG serves as distributed discovery and state management infrastructure, functioning as a critical component for enabling cross-domain semantic interoperability across the global Spatial Web [79].

### 7.2.3 HSTP

The Hyperspace Transaction Protocol (HSTP) is an application-layer protocol that enables nodes across the edge-to-cloud continuum to communicate, execute functions, and share HSML-encoded data. HSTP is designed as a generic, generalizable protocol to standardize communication between heterogeneous systems, essential for building a coherent, decentralized, secure, and privacy-respecting Spatial Web. HSTP supports multiple protocol bindings to facilitate communication and data transfer between diverse edge and cloud systems in various deployment contexts. By providing a standard semantic layer above these protocol bindings, HSTP enables compliant systems to communicate effectively regardless of underlying transport mechanisms. HSTP sends messages as HSTP Operations, which are transmitted over transport protocols. These requests and responses are encoded using profile encoding formats (JSON, JSON-LD, OData, GraphQL) as specified in the HSML Implementation Specification [79].

### 7.2.4 Governance

The governance framework addresses the critical need for machine-readable and machine-executable representation of rules, regulations, and policies within Spatial Web domains. Traditional regulatory approaches have been designed solely for human interpretation, with limited consideration for automated compliance by AI systems and autonomous technologies. The Spatial Web governance framework bridges this gap by enabling both human and machine interpretation of the same regulatory structures, ensuring consistent adherence to rules across human and AI actors.

To enable effective governance of rules and policies, the Spatial Web is organized in a hierarchical, nested architecture where policies and rules are inherited from higher jurisdictional levels and cascaded down to edge systems, following established precedence relationships between different governance levels. Domain Authorities define the norms and terms for creating contracts within their jurisdictional scope, establishing governance for actors, actions, and credentials. This hierarchical structure, combined with the Spatial Web's support for heterarchical and nested domain relationships, enables polycentric governance models that can adapt to diverse regulatory contexts while maintaining coherence across overlapping authorities.

This governance structure enables real-time policy updates from regulatory authorities, allowing edge-deployed systems and autonomous agents

to adapt dynamically to changing conditions such as environmental factors, security threats, or operational requirements. The framework provides specifications and tools for industry stakeholders and regulatory bodies to create, govern, and manage domain-specific implementations while ensuring compliance with broader jurisdictional requirements [79].

## 7.3 AI and Edge AI Standardisation Future Outlook

The international and European standardisation landscape for Artificial Intelligence is a dynamic and rapidly evolving domain, shaped by the dual forces of profound technological advancement and pressing regulatory demand. The collective work of ISO, IEC, IEEE, ITU-T, ETSI, and CEN-CENELEC has resulted in a multi-layered and largely complementary framework that provides the foundational principles, practical tools, and infrastructure specifications needed to guide the development of trustworthy AI. The landscape has matured from defining concepts to building operational frameworks for governance, risk, and quality, a shift driven by the widespread deployment of AI and the legal imperatives of frameworks like the EU AI Act.

Our analysis reveals that the SDOs have successfully carved out distinct yet synergistic niches. ISO/IEC provides the universal, horizontal foundation for AI governance. IEEE focuses on translating ethical principles into engineering practice and solving specific implementation challenges, particularly at the device edge. ETSI and ITU-T are building the network-centric infrastructure required for high-performance AI and edge AI services. Finally, CEN-CENELEC serves the critical function of translating European regulations into harmonised technical standards, creating a clear path to compliance.

While significant progress has been made, the standardisation journey is far from over, and several challenges and future directions are apparent. The most critical challenge, especially for the nascent field of edge AI, is harmonisation. With different SDOs approaching the "edge" from network, device, and foundational perspectives, there is a risk of creating a fragmented landscape with conflicting terminology and overlapping frameworks. Continued and deepened collaboration between these bodies will be essential to ensure the development of a coherent and interoperable set of global standards.

The relentless pace of technological innovation presents another challenge. The rise of Generative AI and Large Language Models (LLMs) introduces new and complex issues related to quality, safety, transparency,

and evaluation that existing standards may not fully address.1 SDOs will need to be agile in developing new standards and guidance to tackle the unique risks and opportunities presented by these powerful technologies. This will require new metrics and measures, new testing methodologies, and even new quality characteristics beyond those currently defined.

As organisations adopt these standards, there will be a growing need for clear pathways to demonstrate compliance and maturity. The development of AI engineering maturity models, like the Capability Maturity Model Integration (CMMI) in software engineering, could provide a valuable tool for organisations to improve their AI governance and development processes progressively. Furthermore, certification against standards like ISO/IEC 42001:2023 and programs like IEEE CertifAIEd$^{TM}$ will become increasingly important mechanisms for organisations to build trust and demonstrate their commitment to responsible AI to regulators, business partners, and the public.10

In conclusion, the development of a robust, comprehensive, and harmonised body of international standards is indispensable for fostering a global AI ecosystem that is not only innovative and economically vibrant but also safe, reliable, and aligned with fundamental human values. The work of the SDOs analysed in this report forms the essential bedrock for achieving this future, providing the common language and shared principles necessary to navigate the complexities of the artificial intelligence era.