



Artificial Intelligence in Manufacturing leading to Sustainability and Industry5.0

Project Acronym:

AIMS5.0

Grant agreement no: 101112089

Deliverable no. and title	**D3.3 – Final architecture concepts and realisation and recommendations for future standardisation**	
Work package	WP3	Cyber architecture for AI supported sustainable production
Task	T3.4	Standardization-based feedback and guidelines for architecture and integration platform
Subtasks involved	ST3.4.1 Identifying suitable standardization activities ST3.4.2 Analysis of architectures based on the relevant use cases ST3.4.3 Development of report	
Lead contractor	Infineon Technologies AG Thomas Gutt:thomas.gutt@infineon.com	
Deliverable responsible	AIT – Austrian Institute of Technology GmbH Christoph Schmittner, mailto: christoph.schmittner@ait.ac.at Erwin Schoitsch, mailto: erwin.schoitsch@ait.ac.at Abdelkader Shaaban, mailto: abdelkader.shaaban@ait.ac.at	
Version number	V2.1	
Date	13/05/2026	
Status	Final	
Dissemination level	Public	

Copyright: AIMS5.0 Project Consortium, 2026

Authors

Participant no.	Part. short name	Author name	Chapter(s)
48	LTU	Jerker Delsing	3, 4 and 5
14	AIT	Christoph Schmittner	4
14	AIT	Erwin Schoitsch	1, 3, 4, and 5
14	AIT	Abdelkader Shaaban	1 and 2
33	AITIA	Peter Olaszi	4
34	BME	Frankó Attila Ernő	4

Document History

Version	Date	Author name	Reason
V0.1	15.12.2025	Abdelkader Shaaban	Initial Template
V1.1	09.04.2026	Abdelkader Shaaban	Consolidated version
V1.2	13.04.2026	Peter Olaszi	Updates some citation
V1.3	13.04.2026	Abdelkader Shaaban	Review version
V1.4	19.04.2026	Germar Schneider	Review version
V1.5	19.04.2026	Markus Tauber	Review version
V1.6	27.04.2026	Yasin Ghafourian	Executive summary and Section 2
V1.7	27.04.2026	Peter Olaszi	Add related references
V1.8	30.04.2026	Abdelkader Shaaban	Consolidated and updated version considering all updates
V1.9	06.05.2026	Abdelkader Shaaban	Changes and updates included
V1.9	06.05.2026	Erwin Schoitsch	Standards-related information updates
V2.0	08.05.2026	Abdelkader Shaaban	Semi-final Version
V2.1	13.05.2026	Abdelkader Shaaban	Final Version

Publishable Executive Summary

Deliverable D3.3 reports on the standardisation, regulatory analysis, and architectural analysis activities conducted within Work Package 3 (WP3) of the AIMS5.0 project. The deliverable presents the outcomes of three interconnected workstreams.

The first workstream provides a comprehensive analysis of the European regulatory landscape governing AI and connected products, focusing on the Cyber Resilience Act (CRA) and the EU AI Act. It examines their scope, risk-based requirements, conformity obligations, and the areas of overlap in product safety, cybersecurity, risk management, and post-market monitoring. It further maps the harmonised standards landscape developed by CEN/CENELEC JTC 21 and the CRA standardisation programme, identifying the impact on AI, IoT, robotics, and industrial automation systems.

The second workstream identifies and maps relevant standardisation activities at European and international levels, including ISO/IEC JTC1 SC42, ETSI, IEC TC65, and the Eclipse Arrowhead framework, and reviews ongoing standards development relevant to AI, IoT, and industrial automation, including human-collaborative aspects.

The third workstream delivers an architecture analysis of the WP3 Eclipse Arrowhead-based microservice framework against the use case requirements expressed across AIMS5.0's use cases. Eclipse Arrowhead is an open-source framework for enabling interoperability and secure service-oriented communication in IoT and industrial automation systems. Nine architectural capability dimensions are evaluated, and concrete guidelines and standardisation recommendations are formulated to address identified compliance and interoperability gaps, with direct linkages to active standards bodies and processes. The deliverable concludes with a high-level synthesis that offers an outlook on WP3 evaluation results and cross-references to regulatory and standardisation frameworks.

Across these workstreams, the deliverable documents the synergies between WP3 and the project's parallel work on AI governance and architectural automation. The WP7 self-assessment chatbot for navigating the regulatory and standards landscape is mapped in Chapter 2 (Ádám Kővári, 2025) (Belal Abu Naim, 2024), and the application of ThreatGet to UC11 in support of CRA conformity (Chapter 4), together translate the regulatory analysis of this deliverable into actionable engineering and compliance support, in line with the principles for engineering secure, trustworthy, and ethically sound AI-based systems articulated by (Yasin Ghafourian, 2024) . The architectural automation work of (Hegedűs, Tóth, Bancsics, & Varga, 2025) complement WP3's model-based engineering activities. These outcomes complement the standardisation activities reported in full in D8.3 (WP8), which includes a thorough assessment and analysis of all Use Cases with respect to relevant standards, knowledge of partners and involvement of partners in standardisation, and D7.3 (WP7, Acceptance, trust and ethics for industrial AI) on standardisation with respect to ethical and human aspects

Table of Contents

1. Introduction 7
1.1 Objective and Scope of the Document 7
1.2 Structure of the Deliverable Report 7
2. Regulatory and Standardisation Content 9
2.1 Overview of the Cyber Resilience Act (CRA) 9
2.1.1 Conditions for Market Placement 9
2.1.2 Essential Cybersecurity Requirements Relating to Product Properties 9
2.1.3 Vulnerability Handling Requirements 10
2.2 Overview of the AI Act and Relevant Requirements 11
2.2.1 Scope of the Application 11
2.2.2 Risk-Based Structure of the AI Act 11
2.2.2.1 … Prohibited AI Systems (Unacceptable Risk) 12
2.2.2.2 .. High-Risk AI Systems 12
2.2.2.3 .. Limited-Risk AI Systems 12
2.2.2.4 .. Minimal-Risk AI Systems 13
2.3 Overlaps and Interactions between CRA and AI Act 13
2.3.1 Overlap in Product Safety and Cybersecurity 13
2.3.2 Overlap in Conformity Assessment and CE Marking 14
2.3.3 Overlap in Risk Management 14
2.3.4 Overlap in Post-Market Monitoring and Incident Handling 15
2.3.5 Interaction in Safety Components and Regulated Products 15
2.3.6 Distinction Despite Overlap 15
2.4 From Regulation to Tool Support: AIMS5.0 Approaches for the AI Act and CRA 15
2.4.1 ThreatGet for CRA-Oriented Threat Modelling and Risk Assessment 16
2.4.2 Self-Assessment Chatbot for Regulatory and Governance Mapping 16
2.5 Harmonised Standards Landscape for the CRA and the AI Act 17
2.5.1 AI Act: Requested Harmonised Standards and Standardisation Deliverables 17
2.5.2 CRA: Current Work Programme and Standardisation Structure 18
2.5.3 Impact of Harmonised Standards on CRA and AI Act Implementation for AI, IoT, Robotics, and Industrial Automation Systems 19
2.5.4 Emerging Harmonised Standards as a Forward-Looking Compass for AIMS5.0 19
3. Identification of Relevant Standardisation Activities 20
3.1 Engagement with European and International Standardisation Bodies 20
3.1.1 European Harmonised Standards, Directives and Regulations 20
3.1.2 ISO/IEC JTC1 SC42 Standards 20
3.1.3 ETSI Secure AI Standards 21
3.1.4 Standards Related to ARROWHEAD DSL 21
3.2 Mapping of Relevant Standards and Standardisation Activities 21
3.2.1 ISO/IEC JTC1 SC42 Artificial Intelligence Standards Mapping 21
3.2.2 Analyse and Align Architectural Outcomes with Standardisation Landscape 23
3.3 Review Ongoing Standards Development Relevant to AI, IoT, and Industrial Automation, Including Human Collaborative Aspects 25
3.4 Next Steps and Continuation Plan 27
4. Architecture Analysis Based on Use Cases 28
4.1 Architecture Fulfilment of UC Requirements 28

4.1.1 Overview of Use Case Architectural Requirement Categories 28
4.1.2 Fulfilment by Architectural Capability Dimension 29
4.1.3 Fulfilment Summary 32
4.2 Architectural Analysis for Standardisation in the Use Cases 33
4.2.1 UC02 – AI Enhanced Value Chain: Protocol Interoperability and Semantic Standards 34
4.2.2 UC05 – Multi-Layer AI in Machine Tool Domain: OPC UA Integration and Industrial Security 34
4.2.3 UC08 – AI Supporting Human and Manufacturing Cycles: Real-Time Networking and Human–AI Safety Standards 35
4.2.4 UC09 – Energy-Aware Scheduling in Wafer Fabrication: Energy Standards and Use Case Methodology 36
4.2.5 Cross-Cutting Standardisation Analysis Summary 37
4.3 Architectural Analysis for Standardisation involved in UC11 38
4.3.1 System Architecture and Key Components 38
4.3.2 Key Standardisation Activities and Technical Work 39
5. High-Level Evaluation and Synthesis 41
5.1 Outlook of WP3 Architecture Evaluation Results 41
5.1.1 Semantic Interoperability and Automation and Scalability of Information Integration 41
5.1.2 Automation of the Engineering Processes 41
5.1.3 Orchestration along the Edge 2 Cloud Compute Continuum 42
5.2 Cross-Reference with Regulatory and Standardisation Frameworks 42
5.2.1 Regulatory Compliance Mapping 43
5.2.2 Guidelines for Future Architectural Improvements 45
5.2.3 Standardisation Recommendations 48
6. Conclusions 52
7. References 53
8. Appendices 56
8.1 Appendix A – Abbreviations 56
8.2 Appendix B: Current list of ISO/IEC SC42 AI standards 57

List of figures

Figure 1 AI Act Harmonised Standards Mapping..... 18
Figure 2 Conceptual engineering process for CPS automation systems, from early design to deployment, highlighting areas where AI and formal tools support engineering automation . 42

List of tables

Table 1 Additional Standardisation Landscape..... 24
Table 2 Use case Requirement Categories..... 29
Table 3 Architectural fulfilment across the requirement dimensions 33
Table 4 Standards-relevant architectural findings across the four analysed use cases 37

1. Introduction

1.1 Objective and Scope of the Document

Deliverable D3.3 aims to consolidate the project's regulatory, standardisation, and architectural analyses, and to translate these findings into actionable guidelines and standardisation recommendations based on the WP3 architecture.

This document has three objectives. First, it clarifies the European regulatory obligations for the AIMS5.0 system architecture, focusing on the Cyber Resilience Act and the EU AI Act. Second, it maps the relevant European and international standardisation landscape and identifies specific engagement points where AIMS5.0 WP3 results can contribute to ongoing standardisation processes. Third, it assesses how well the WP3 microservice architecture, based on the Eclipse Arrowhead framework, meets the architectural requirements of the AIMS5.0 use cases and identifies any compliance and interoperability gaps.

This deliverable focuses on WP3 architectural outcomes and their relationship to the regulatory and standardisation landscape and focuses on a selected number of use cases. It does not replace D8.3, the final standardisation report of WP8, but provides technical input based on architecture to support and complement the project's standardisation efforts. Detailed standardisation engagement activities, partner contributions, and the full mapping of standards to use cases are included in D8.3. The deliverable additionally documents the points of synergy between WP3 and WP7 (Acceptance, trust and ethics for industrial AI), in particular, the use of the WP7 self-assessment chatbot (Ádám Kővári, 2025) (see Section 2.4) for navigating the regulatory and standards landscape mapped in this report, the ethical and human-aspects-related impacts, and the application of ThreatGet (see Section 4.3.2) for risk-driven CRA alignment. It discusses a selected set of use cases in detail, whereas D8.3 (final standardisation deliverable) includes a thorough assessment and analysis of all Use Cases with respect to relevant standards, knowledge of partners and involvement of partners in standardisation, and D7.3 (WP7) discusses standardisation with respect to ethical and human aspects

1.2 Structure of the Deliverable Report

The deliverable is structured as follows.

Chapter 2 presents the regulatory and standardisation content, covering the Cyber Resilience Act (CRA) (European Commission (EC) - CRA Act, 2024) and the EU AI Act (European Commission (EC) - AI Act, 2024), their scope, essential requirements, risk-based structures, areas of overlap and interaction, and the harmonised standards landscape under development by CEN/CENELEC and ETSI.

Chapter 3 identifies standardisation activities, provides an overview of engagement with European and international standardisation bodies, maps relevant standards and standardisation activities, reviews ongoing standards development relevant to AI, IoT, and industrial automation, and outlines a continuation plan for future standardisation activities.

Chapter 4 delivers the architecture analysis based on use cases, assessing the extent to which the WP3 Eclipse Arrowhead-based architecture fulfils use-case architectural requirements across nine capability dimensions, and provides architectural analysis for standardisation across selected use cases, including UC02, UC05, UC08, UC09, and UC11. All Use Cases are discussed in D8.3 (final standardisation deliverable) based on a thorough assessment and analysis of all

Use Cases with respect to relevant standards, knowledge of partners and involvement of partners in standardisation

Chapter 5 provides a high-level evaluation and synthesis, presenting the outlook of WP3 architecture evaluation results in the areas of semantic interoperability, engineering process automation, and edge-to-cloud orchestration, and cross-referencing these results with the regulatory and standardisation frameworks through compliance mapping, architectural improvement guidelines, and standardisation recommendations.

Chapter 6 presents the conclusions of the deliverable. References and appendices, including an abbreviations table and an annex on ISO/IEC SC42 AI standards, follow thereafter.

Appendix A (Section 8.1) provides a list of the abbreviations used throughout this deliverable. Appendix B (Section 8.2) presents a comprehensive overview of the standards and projects under ISO/IEC JTC 1/SC 42, including AI-related standards as well as Big Data standards.

2. Regulatory and Standardisation Content

2.1 Overview of the Cyber Resilience Act (CRA)

The European Cyber Resilience Act (CRA) introduces binding cybersecurity obligations for products with digital elements placed on the European Union market. It establishes a harmonised regulatory framework to ensure that software and hardware products, including their remote data processing functionalities, comply with essential cybersecurity requirements throughout their entire lifecycle.

The Regulation applies to any product with digital elements, meaning software or hardware products whose remote data processing solutions are designed and developed by, or under the responsibility of, the manufacturer, and whose absence would prevent the product from performing one of its intended functions.

2.1.1 Conditions for Market Placement

The market context for the CRA is significant. The European cybersecurity market was valued at approximately €67 billion in 2025 and is projected to reach €172 billion by 2033, growing at a compound annual growth rate of 12.4% (CBI, 2026). This growth is driven by the rising frequency and severity of cyberattacks - ENISA reported (ENISA, 2024)11,079 cyber incidents across the EU between July 2023 and June 2024 alone, alongside accelerating digital transformation and the proliferation of connected products (CBI, 2026). The CRA directly responds to this landscape by addressing a recognised market failure: the inadequate level of cybersecurity embedded in products with digital elements and the insufficient provision of security updates throughout product lifecycles (ComplianceHub, 2025). It is estimated that non-critical products, those subject to the least stringent conformity requirements, account for approximately 90% of all products with digital elements currently on the EU market, indicating the scale of the regulatory transition ahead (Hogan Lovells, 2024). With main obligations applying from 11 December 2027, and reporting obligations taking effect from September 2026, manufacturers, importers, and distributors across the EU supply chain are under increasing pressure to begin compliance preparations now (Pillsbury, 2025).

Under the CRA, a product with digital elements may only be placed or made available on the Union market if two fundamental conditions are fulfilled:

1) The product itself complies with the essential cybersecurity requirements relating to its properties (Part I of Annex I), provided that it is properly installed, maintained, and used in accordance with its intended purpose or under reasonably foreseeable conditions, and that necessary security updates have been applied.
2) The manufacturer’s internal processes comply with the essential vulnerability-handling requirements (Part II of Annex I).

Compliance, therefore, extends beyond the technical features of the product to include the governance, development, and maintenance processes established by the manufacturer.

2.1.2 Essential Cybersecurity Requirements Relating to Product Properties

The essential cybersecurity requirements set out in the CRA can be directly linked to practical implementation experience generated within AIMS5.0. For example, in Use Case 11 (UC11 - AI-supported Industrial IoT for Indoor Food Production), a comprehensive cybersecurity framework

was established using ThreatGet, a systematic threat modelling and risk assessment tool, explicitly aligned with the CRA's essential requirements. The UC11 system deploys a vertically organised architecture of interconnected components across field, edge, and cloud layers. The ThreatGet-based threat analysis covered the full interconnected architecture, documenting the operational environment, including field-layer components, sensors, and actuators, as well as the remote monitoring and control environment, including network devices, servers, and data stores. Security controls were defined for critical components such as sensor ECUs, and the threat database was used to identify potential cyber risks across the full system lifecycle.

So the main vision of the CRA is more focused on the products with digital elements, which must be designed, developed, and produced to ensure an appropriate level of cybersecurity proportionate to the identified risks.

On the basis of a cybersecurity risk assessment, products with digital elements are quired to:

a) Be placed on the market without known exploitable vulnerabilities.
b) Be delivered with secure-by-default configurations, including the ability to restore the product to its original secure state.
c) Provide mechanisms to address vulnerabilities through timely security updates, including automatic updates enabled by default where appropriate, accompanied by clear user notification and opt-out options.
d) Implement safeguards against unauthorised access through appropriate authentication, identity, and access control mechanisms, and enable detection or reporting of unauthorised access.
e) Protect the confidentiality of data processed, stored, or transmitted by applying state-of-the-art encryption and other technical measures.
f) Ensure the integrity of data, commands, programs, and configurations against unauthorised modification, and detect or report data corruption.
g) Limit data processing to what is necessary and proportionate to the intended purpose of the product (data minimisation).
h) Preserve the availability of essential functions, including resilience against denial-of-service attacks and the ability to maintain operation following an incident.
i) Avoid negatively impacting the availability of services provided by other devices or networks.
j) Minimise attack surfaces, including through secure design of external interfaces.
k) Mitigate the potential impact of incidents through appropriate technical protection mechanisms.
l) Provide relevant security information through logging and monitoring of significant internal activities, subject to user control.
m) Enable users to securely and permanently remove data and settings, and where data are transferred, ensure secure transfer mechanisms.

These requirements ensure that cybersecurity is embedded at product level, from design through operational use.

2.1.3 Vulnerability Handling Requirements

Manufacturers are subject to structured and ongoing vulnerability management obligations. They must:

a) Identify and document vulnerabilities and components included in the product, including through the preparation of a software bill of materials (SBOM) in a commonly used, machine-readable format.

b) Address and remediate vulnerabilities without undue delay, including through the provision of security updates that are, where technically feasible, separated from functional updates.
c) Conduct regular and effective testing and security reviews of the product.
d) Once a vulnerability has been fixed, disclose relevant information to users in a transparent and accessible manner, including severity, impact, and remediation guidance, unless a justified delay is necessary to avoid additional security risks.
e) Establish and enforce a coordinated vulnerability disclosure policy.
f) Facilitate the reporting of vulnerabilities by providing clear communication channels for external parties.
g) Implement secure mechanisms for distributing updates to ensure timely mitigation of vulnerabilities, including automatic update mechanisms where appropriate.
h) Ensure that security updates addressing identified risks are provided without delay and, unless otherwise agreed in specific business contexts, free of charge, accompanied by clear advisory information for users.

These requirements ensure that cybersecurity is maintained beyond market placement through continuous monitoring, disclosure, remediation, and update mechanisms.

2.2 Overview of the AI Act and Relevant Requirements

The European Artificial Intelligence Act (AI Act) establishes the first comprehensive and horizontal legal framework governing artificial intelligence systems within the European Union. It introduces harmonised rules for the development, placing on the market, putting into service, and use of AI systems in the Union.
The Act applies to providers placing AI systems on the EU market, deployers using AI systems within the Union, as well as importers and distributors. Its objective is to ensure that AI systems placed on the Union market are safe, respect fundamental rights, and operate in a trustworthy manner.

2.2.1 Scope of the Application

The AI Act regulates AI systems defined as machine-based systems designed to operate with varying levels of autonomy and capable of generating outputs, such as predictions, content, recommendations, or decisions, that influence physical or virtual environments.

The Regulation applies to:
a) Providers placing AI systems on the market or putting them into service in the Union,
b) Deployers of AI systems located within the Union,
c) Importers and distributors making AI systems available on the Union market,
d) Providers and deployers of general-purpose AI models under specific conditions.

2.2.2 Risk-Based Structure of the AI Act

The AI Act follows a structured risk-based regulatory model. Obligations depend on the level of risk an AI system poses to health, safety, and fundamental rights.

2.2.2.1 Prohibited AI Systems (Unacceptable Risk)

Certain AI practices are prohibited where they are considered to present unacceptable risks. These include AI systems that:

- Manipulate behaviour in a manner likely to cause harm,
- Exploit vulnerabilities of natural person or specific groups,
- Implement social scoring by public authorities,
- Use certain forms of real-time remote biometric identification in publicly accessible spaces (subject to limited exceptions).

These systems may not be placed on the market or put into service in the Union.

2.2.2.2 High-Risk AI Systems

An AI system is classified as high-risk under the Regulation where one of the following conditions applies: first, where the AI system itself constitutes a regulated product category; second, where the AI system functions as a safety component of a regulated product; or third, where the AI system falls within one of the specifically listed high-risk use cases defined by the Regulation.

High-risk AI systems may be placed on the Union market, put into service, or operated only if they comply with the applicable mandatory requirements established by the Regulation. These requirements are intended to ensure that high-risk AI systems made available within the Union, or whose outputs are used within the Union, do not create unacceptable risks to significant public interests recognised and protected under Union law.

High-risk AI systems must comply with comprehensive requirements including:

- A risk management system,
- Data governance and data quality measures,
- Technical documentation,
- Record-keeping and logging capabilities,
- Transparency and provision of information to users,
- Human oversight,
- Accuracy, robustness, and cybersecurity requirements.

Conformity assessment procedures must be completed before high-risk AI systems are placed on the market.

2.2.2.3 Limited-Risk AI Systems

Limited-risk AI systems are those subjects primarily to specific transparency obligations rather than the extensive compliance framework applicable to high-risk systems. In particular, providers must ensure that AI systems intended to interact directly with natural persons clearly inform individuals that they are engaging with an AI system, unless this is already evident from the circumstances. Providers of AI systems generating synthetic audio, image, video, or text content must ensure that such outputs are identifiable as artificially generated or manipulated in a machine-readable and detectable manner, taking into account technical feasibility and state-of-the-art standards. Furthermore, deployers of emotion recognition or biometric categorisation systems are required to inform affected individuals of the system's operation and comply with applicable data protection legislation. Deployers generating or manipulating deepfake content must disclose that such content has been artificially generated or altered,

particularly where it informs the public on matters of public interest, unless specific legal exceptions apply. These obligations ensure transparency towards natural persons while avoiding the more stringent conformity and risk management requirements reserved for high-risk AI systems.

A practical example of a limited-risk AI system developed within the AIMS5.0 project itself is the self-assessment chatbot produced under WP7 (Ádám Kővári, 2025). The chatbot interacts directly with natural persons, AI developers, integrators, and compliance practitioners, and generates textual outputs consisting of retrieved governance instruments and accompanying explanations. Under the risk-based structure of the AI Act, this places the chatbot within the limited-risk category, triggering the transparency obligations of Article 50: users are clearly informed that they are interacting with an AI system, retrieval-based outputs are explicitly distinguished from authoritative legal interpretation, and the system is positioned as decision support rather than as an autonomous compliance authority. The chatbot does not undertake conformity decisions, nor does it operate as a safety component of a regulated product, which would otherwise shift it into the high-risk regime. A detailed description of the chatbot, its Retrieval-Augmented Generation (RAG) architecture, and its role in supporting CRA and AI Act compliance is provided in Section 2.4, with the full validation results reported in D7.3.

2.2.2.4 Minimal-Risk AI Systems

A general-purpose AI model is classified as a general-purpose AI model with systemic risk where it demonstrates high-impact capabilities, as evaluated using appropriate technical tools, methodologies, benchmarks, and indicators, or where the Commission determines, either on its own initiative or following a qualified alert from the scientific panel, that the model possesses capabilities or impacts equivalent to those defined for high-impact models in accordance with the criteria set out in Annex XIII. A model is presumed to have high-impact capabilities where the cumulative computational resources used for its training exceed the threshold specified in the Regulation. Providers of such models are required to notify the Commission without delay, and in any event within two weeks of meeting the relevant threshold or becoming aware that it will be met. The Commission may designate a general-purpose AI model as presenting systemic risk where the applicable criteria are satisfied and may publish and maintain an updated list of such models. Providers may submit substantiated arguments contesting the classification, and reassessment may be requested under the conditions defined in the Regulation. The Commission is empowered to amend thresholds, benchmarks, and criteria through delegated acts to ensure that the classification framework reflects evolving technological developments and the state of the art.

2.3 Overlaps and Interactions between CRA and AI Act

The Cyber Resilience Act (CRA) and the EU Artificial Intelligence Act (AI Act) intersect when AI systems are embedded in or form part of digital products placed on the Union market. The CRA regulates cybersecurity and vulnerability management of digital products, while the AI Act addresses safety, fundamental rights, governance, and risk management of AI systems. Their scopes overlap when AI is either a product itself or a safety component of a regulated product.

2.3.1 Overlap in Product Safety and Cybersecurity

High-risk AI systems must comply with requirements relating to risk management, robustness, accuracy, and cybersecurity (AI Act, Arts. 8-15). In particular, Article 15 of the AI Act requires high-risk AI systems to achieve appropriate levels of accuracy, robustness, and cybersecurity. At the same time, the CRA requires products with digital elements to meet essential

cybersecurity requirements for secure design, vulnerability management, and lifecycle security management (CRA, Annex I, Parts I and II).

Where an AI system is integrated into a product with digital elements, for example, as a safety component, the product must satisfy both:

- the cybersecurity-by-design and vulnerability management requirements under the CRA (CRA, Annex I), and
- the risk management, data governance, robustness, and human oversight requirements under the AI Act (AI Act, Arts. 9 - 15).

Thus, cybersecurity obligations may derive simultaneously from Article 15 AI Act and Annex I CRA, though the legal rationale differs:

- The AI Act frames cybersecurity in relation to safety and fundamental rights risks.
- The CRA frames cybersecurity in relation to product security and resilience against exploitation.

2.3.2 Overlap in Conformity Assessment and CE Marking

Both Regulations rely on conformity assessment procedures prior to market placement.

Under the AI Act, high-risk AI systems must undergo conformity assessment procedures before being placed on the market or put into service (AI Act, Arts. 16 - 29).

Similarly, under the CRA, products with digital elements must undergo conformity assessment to verify compliance with essential cybersecurity requirements before CE marking and market placement (CRA, Arts. 24 - 32; Annex I).

Where AI systems qualify as high-risk and are embedded in products covered by the CRA, conformity assessments must address both frameworks. In practice, this may require integrated technical documentation covering:

- AI risk management (AI Act, Art. 9),
- cybersecurity design and vulnerability handling (CRA, Annex I),
- logging and monitoring mechanisms (AI Act, Art. 12; CRA, Annex I Part I),
- post-market monitoring and corrective actions under both regimes.

2.3.3 Overlap in Risk Management

The AI Act requires providers of high-risk AI systems to establish a continuous risk management system covering the entire lifecycle (AI Act, Art. 9).

The CRA similarly imposes lifecycle obligations, including vulnerability identification, remediation, coordinated vulnerability disclosure, and secure update mechanisms (CRA, Annex I Part II).

Both Regulations therefore impose lifecycle governance obligations, but with different focal points:

- AI Act → systemic risk to safety and fundamental rights.
- CRA → technical cybersecurity vulnerabilities and exploitability.

Where AI systems are embedded in digital products, both risk management systems must operate coherently.

2.3.4 Overlap in Post-Market Monitoring and Incident Handling

The AI Act requires post-market monitoring systems and reporting of serious incidents for high-risk AI systems (AI Act, Arts. 72 - 73).

The CRA imposes obligations concerning vulnerability handling, security updates, and incident reporting impacting the security of the product (CRA, Arts. 14 - 16; Annex I Part II).

In cases where an incident affects both AI decision logic and product cybersecurity (e.g., adversarial manipulation of AI behaviour through a cyber vulnerability), obligations under both instruments may be triggered.

2.3.5 Interaction in Safety Components and Regulated Products

An AI system is classified as high-risk where it constitutes a safety component of a product covered by Union harmonisation legislation (AI Act, Art. 6).

If that product is also a product with digital elements under the CRA, the manufacturer must simultaneously ensure compliance with:

- AI system high-risk obligations (AI Act, Chapter III), and
- cybersecurity requirements applicable to the product (CRA, Annex I).

Thus, the AI Act governs *what the AI must ensure*, while the CRA governs *how the digital product must be secured against exploitation*.

2.3.6 Distinction Despite Overlap

Despite areas of interaction, the two Regulations pursue distinct regulatory objectives:

- The AI Act focuses on mitigating risks to health, safety, and fundamental rights arising from AI system behaviour.
- The CRA focuses on reducing cybersecurity vulnerabilities in digital products and ensuring resilience against cyber threats.

The AI Act regulates the *functional and societal impact* of AI systems, while the CRA regulates the *technical security integrity* of products with digital elements.

Where AI systems are embedded in digital products, compliance must therefore be cumulative rather than alternative.

2.4 From Regulation to Tool Support: AIMS5.0 Approaches for the AI Act and CRA

The regulatory landscape outlined in the preceding sections, focusing on the CRA, the AI Act, their points of overlap, and the associated harmonised standards, is technically demanding to navigate in practice. Within AIMS5.0, two tools provide practical support in this context: **ThreatGet**, developed by AIT, and the **self-assessment chatbot**, developed by RSA. Together, they help translate regulatory requirements into engineering and compliance practice, reflecting the broader rationale articulated by (Yasin Ghafourian, 2024) for engineering secure, trustworthy, and ethically sound AI-based computer systems.

2.4.1 ThreatGet for CRA-Oriented Threat Modelling and Risk Assessment

ThreatGet is a model-based threat modelling and risk assessment tool, and a self-assessment chatbot for governance-instrument identification. It provides an engineering-oriented alignment with the CRA by translating its cybersecurity objectives into a structured threat modelling and risk assessment workflow. The tool supports the analysis of whether a system architecture and its components are exposed to threats that may undermine CRA-relevant goals such as secure-by-design implementation, attack surface minimisation, protection against unauthorised access, vulnerability identification, and lifecycle-oriented risk handling. In this way, ThreatGet can be used to systematically derive, and document security-relevant architectural findings, threat scenarios, and mitigation needs that directly support the interpretation and operationalisation of CRA obligations in concrete technical systems. Within AIMS5.0, this makes ThreatGet particularly valuable as a bridge between regulatory requirements and system-level cybersecurity engineering, as successfully demonstrated in the activities of UC11: AI-supported Industrial IoT for Indoor Food Production. It supports the investigation of potential threats and helps assess compliance with the CRA, thereby contributing to the European objective of ensuring secure products with digital elements (Abdelkader Magdy Shaaban, 2025).

2.4.2 Self-Assessment Chatbot for Regulatory and Governance Mapping

The AIMS5.0 self-assessment chatbot, developed in WP7, is a Retrieval-Augmented Generation (RAG) tool deployed on cloud infrastructure that helps developers, integrators, and compliance practitioners identify the regulatory, standardisation, and ethical instruments applicable to a given AI use case. The conceptual basis for such a tool was established by (Belal Abu Naim, 2024), who proposed a self-assessment methodology to encourage the uptake of AI in digital workspaces against a fragmented and rapidly evolving landscape of standards and guidelines; the supporting RAG architecture for the chatbot was subsequently introduced by (Ádám Kővári, 2025). Given a natural-language description of an AI application, the chatbot retrieves and surfaces relevant governance documents from a curated knowledge base that intentionally mirrors the landscape mapped in the preceding sections of this chapter, the EU AI Act, the CRA, the GDPR, the CEN/CENELEC harmonised AI standards, the ISO/IEC JTC 1 SC42 portfolio, and sector-specific instruments such as the Machinery Regulation, the UNECE automotive framework, and the Medical Device Regulation. The chatbot has been validated by comparing its outputs against independent assessments performed by legal experts on five representative AIMS5.0 use cases (UC2, UC11, UC12, UC13, UC14), selected to span the project's qualitative use case clusters. Across these cases, the chatbot reliably retrieved the cross-cutting regulatory and ethical instruments present in its corpus, broadly aligning with expert assessments. Remaining mismatches stem from predictable boundaries of the approach: knowledge-base coverage gaps (notably for paywalled standards), granularity and naming differences, and use case descriptions that under-specify contextually relevant factors. The full validation methodology, results across all use cases, and discussion of limitations are reported in D7.3, Section 5. The chatbot is therefore best positioned as a practical first-pass tool for compliance orientation and governance mapping, complementing, rather than replacing, expert legal review.

2.5 Harmonised Standards Landscape for the CRA and the AI Act

The standardisation works relevant to the CRA and the AI Act should be understood as the technical layer that operationalises regulatory requirements into implementable specifications, testable criteria, and conformity-supporting methods. For the AI Act, the Commission standardisation request explicitly states that the requested harmonised standards and European standardisation deliverables must provide technical specifications for the essential requirements of high-risk AI systems under Articles 9 to 15, and for the requirements under Articles 17 and 43, while remaining aligned with the New Legislative Framework and complementing other Union harmonisation legislation (Commission, European, 2025) . For the CRA, the current CEN-CENELEC-ETSI work programme shows how this is being translated into a structured portfolio of horizontal, product-class, and industrial/OT-specific standards (CEN, CENELEC and ETSI Work Programme , 2025).

2.5.1 AI Act: Requested Harmonised Standards and Standardisation Deliverables

For the AI Act, the Commission Implementing Decision of 23 June 2025 requests CEN and CENELEC to draft a structured set of harmonised standards and, where necessary, European standardisation deliverables covering ten technical areas (Commission, 2025):

- risk management systems for AI systems;
- governance and quality of datasets used to build AI systems;
- record keeping through logging capabilities by AI systems;
- transparency and information provisions for users of AI systems;
- human oversight of AI systems accuracy;
- accuracy specifications for AI systems
- robustness specifications for AI systems;
- cybersecurity specifications for AI systems;
- quality management systems for providers of AI systems, including post-market monitoring processes; and
- conformity assessment for AI systems.

These standards should emphasise that they must not be treated as isolated documents; rather, they are to form a coherent system of harmonised standards and standardisation deliverables for high-risk AI systems (Commission, European, 2025).

Figure 1, based on (Smith, 2026), provides an interactive mapping of the intended coverage of harmonised standards, illustrating how each standardisation project relates to specific AI Act articles and indicating the current stage of development for each standard.

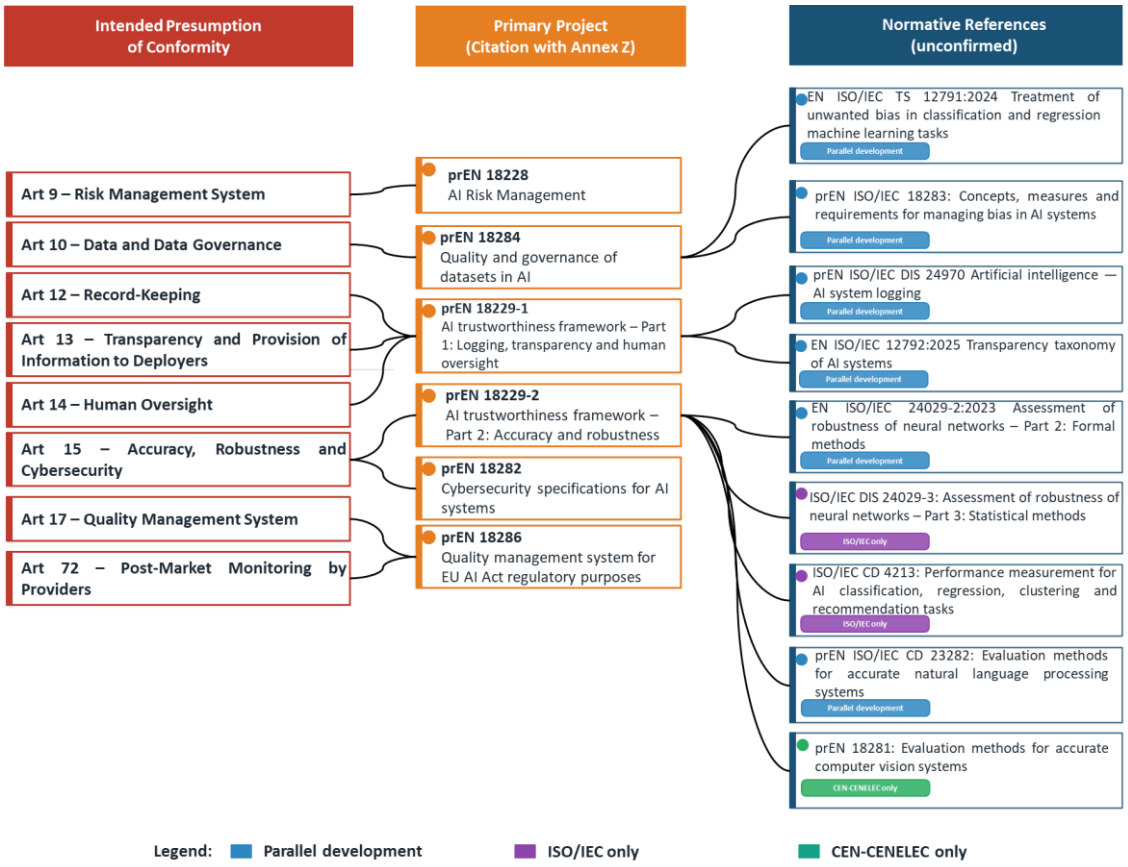

Figure 1 AI Act Harmonised Standards Mapping

The ongoing European standardisation activities supporting the AI Act are being coordinated through **CEN-CENELEC JTC 21**, which is structured into five active working groups covering complementary areas of AI standardisation. These include **WG1** on strategic and cross-cutting coordination, **WG2** on operational aspects, **WG3** on engineering aspects, **WG4** on foundational and societal aspects, and **WG5** on cybersecurity for AI systems. Together, these working groups provide the organisational framework for developing the draft standards and related deliverables intended to support the implementation of AI Act requirements (CEN CENELEC, 2026).

2.5.2 CRA: Current Work Programme and Standardisation Structure

According to the M/606 work programme (CEN, CENELEC and ETSI Work Programme , 2025).The planned standardisation activities supporting the CRA comprise a structured pipeline of standards. At the highest level, the programme identifies three horizontal work items: Principles for Cyber Resilience, Generic Security Requirements, and Vulnerability Handling for products with digital elements. These activities are intended to support the CRA's cybersecurity requirements and lifecycle-related obligations (Commission, 2025).

Beyond these horizontal items, the CRA work programme identifies a large number of product-class and functional standards. These include standards for identity management systems and privileged access management; embedded and standalone browsers; password managers; malware search/removal/quarantine software; VPN products; network management systems; SIEM systems; boot managers; public key infrastructure and digital certificate issuance software; physical and virtual network interfaces; operating systems; routers, modems, and switches; microprocessors and microcontrollers with security-related functionalities; ASICs and FPGAs with security-related functionalities; smart home virtual assistants; smart home security

products; internet-connected toys; personal wearable products; hypervisors and container runtime systems; firewalls and intrusion detection/prevention systems; hardware devices with security boxes; smart meter gateways; and smartcards or similar devices including secure elements (Commission, 2025)

This is especially relevant for AI, IoT, and industrial automation because the CRA work programme also includes industrial and OT-oriented security profiles based on IEC 62443. The M/606 work programme explicitly lists preliminary work items for IEC 62443-5-XX based security profiles for VPNs, network management systems, SIEM systems, physical and virtual network interfaces, routers/modems/switches, and firewalls/IDS/IPS. In addition, the programme includes broad vertical supporting OT deliverables based on EN IEC 62443-4-1, EN IEC 62443-4-2, and EN IEC 62443-3-3, which directly connect CRA implementation with industrial automation and control system security practices (Commission, 2025).

2.5.3 Impact of Harmonised Standards on CRA and AI Act Implementation for AI, IoT, Robotics, and Industrial Automation Systems

The harmonisation of standards with the CRA and the AI Act is essential because it translates regulatory obligations into concrete technical specifications, assessment methods, and implementation practices that can be applied consistently across products and sectors. This is especially important for AI, IoT, robotics, and industrial automation systems, where compliance depends not only on legal interpretation but also on how systems are designed, integrated, tested, secured, and maintained in practice. In this context, harmonised standards can support the reduction of cyberattacks, the secure design of interfaces and communication paths, the implementation of lifecycle vulnerability handling, and, where AI is involved, the operationalisation of requirements related to risk management, transparency, human oversight, robustness, and cybersecurity. As a result, these standards provide a bridge between regulation and system architecture, enabling manufacturers and developers to design compliant and trustworthy solutions. The next step is therefore the continuation of the collaboration with CEN/CENELEC in order to further refine and validate the list of standards relevant to CRA and AI Act requirements, with particular attention to their applicability to AI, IoT, robotics, and industrial automation use cases.

2.5.4 Emerging Harmonised Standards as a Forward-Looking Compass for AIMS5.0

The harmonised standards and standardisation deliverables discussed above are still under development and therefore do not yet constitute a stable set of published reference standards for direct compliance use. Nevertheless, they are highly relevant to AIMS5.0 because they indicate the technical directions along which future European compliance expectations are being shaped. In this sense, the project can already use these ongoing standardisation activities as a forward-looking orientation framework when analysing architecture, trustworthiness, cybersecurity, AI governance, and system integration across its use cases and related toolchain development in AIMS5.0. This is reflected, for example, in D7.3 through the proposed AI assurance framework based on the ALTAI assessment requirements (Commission, European, 2020), in the use of ThreatGet to support analysis against the CRA essential cybersecurity requirements in Annex I (European Commission (EC) - CRA Act, 2024), and in the chatbot's role in identifying whether and which AI Act, CRA (European Commission (EC) - AI Act, 2024), standardisation, and ethical instruments are relevant for specific AI use cases. This is particularly valuable for identifying where current AIMS5.0 technical activities are already consistent with emerging requirements and where further refinement may be needed, while also allowing the evolving harmonised standards landscape to provide a clearer pathway for aligning future research and innovation activities with forthcoming EU regulatory expectations.

3. Identification of Relevant Standardisation Activities

For details on relevant standards and their impact on Use Cases, respectively, the engagement of partners in standardisation (both, using as well as actively contributing), see Deliverable D8.3, section on standardisation. D8.3 includes the result of a thorough assessment and analysis of all Use Cases with respect to relevant standards, knowledge of partners and involvement of partners in standardisation, by a specific questionnaire. A broader survey of AI and Big Data standardisation activities under ISO/IEC JTC 1/SC 42 is provided in Appendix B – Section 8.2.

3.1 Engagement with European and International Standardisation Bodies

3.1.1 European Harmonised Standards, Directives and Regulations

European Directives and Regulations have legal impact and have to applied by EU members by integrating them into their national legal framework. The same is valid for the non-EU countries of the EEA (European Economic Area) Norway, Iceland, Lichtenstein.
The EC sends out a "Standardization Request" to the European SDOs (Standardization Organizations) and assigns CEN/CENELEC or ETSI to take over the task. For the AIU-Act, CEN/CLC JTC21 was created, the CRA harmonized standards are either CEN/CLC JWG13, ETSI Cyber EUSR and a few other CEN or CLC WGs (see "Quick Guide CRA Work Program" (CEN-CENELEC, 2025)).

The engagement with CEN/CENELC is either via the National Standardisation Committees of the partner countries, which also mirror the related ISO, IEC or ISO/IEC JTC1 committees, or ETSI membership (by company or organisation, most relevant international industrial organisations and RTOs are members, e.g. AIT from Austria as RTO).

As an example for AI and the related subtopics, e.g. Cybersecurity, CEN/CLC JTC21 is structured as follows:

- **WG 1 Strategic Advisory Group (SAG)**: Focuses on overarching strategies and cross-sectoral challenges.
- **WG 2 Operational Aspects**: Addresses practical implementation issues.
- **WG 3 Engineering Aspects**: Concentrates on technical design and development.
- **WG 4 Foundational and Societal Aspects**: Examines ethical and societal impacts of AI.
- **WG 5 Cybersecurity for AI Systems**: Ensures secure AI deployment.

An overview of the ongoing standardisation activities in CEN/CENELEC JTC21 and the related articles of the AI-Act that are addressed by each of the preEN-Standards, plus the references to related ISO/IEC Standards, is provided in section 2.5.1, Figure 1.

Engagement of AIMS5.0 partners takes place in a few cases via the WGs of JTC21 (e.g., WG 5, Cybersecurity, and WG 4), but in most cases via the National Mirror Committees (NCs), which send delegates to the JTC21 groups and represent the NC decisions. Section 2.4 reflects the engagement and the utilisation of this work.

3.1.2 ISO/IEC JTC1 SC42 Standards

An overview of the main ISO/IEC Standards from ISO/IEC JTC1 SC42, AI, (published or evolving) is provided in Section 3.2. Please note that there are already 41 AI standards published and 450

under development (three months ago, there were only 47 under development, just to indicate how fast this area is evolving):

A structured mapping is provided in Section 3.2.

3.1.3 ETSI Secure AI Standards

ETSI, a European SDO, works on AI standards as well. ETSI SAI (Securing AI) has developed several AI standards, some examples are:

- ETSI TR 104 128 V1.1.1 (2025-05) - Securing Artificial Intelligence (SAI); Guide to Cyber Security for AI Models and Systems
- ETSI TS 104 224 V1.1.1 (2025-03) - Securing Artificial Intelligence (SAI); Explicability and transparency of AI processing
- ETSI TR 104 032 V1.1.1 (2024-02) - Securing Artificial Intelligence (SAI); Traceability of AI Models
- ETSI TR 104 048 V1.1.1 (2025-01) - Securing Artificial Intelligence (SAI); Data Supply Chain Security.

ETSI Standards are developed close to industrial needs and applicability, since ETSI is financed by its member companies, mainly large or key enterprises in their field, with some academic institutions for support (e.g. AIT). Therefore, they are important for an industry-driven ChipsJU project like AIMS5.0. They are not addressing the AI-Act directly.

3.1.4 Standards Related to ARROWHEAD DSL

Related to the Arrowhead DSL (Domain Specific Language), it is now scheduled for a presentation with OMG (omg.org). The presentation was at the OMG technology meeting in Reston, VA, USA March 24. The presentation was highly welcomed by the key people behind SysML v2. Encouragements for further engagement in the SysML v2 was expressed from Sanford Friedenthal, a key brain behind the SysML technologies.

The presentation addresses the early work on Arrowhead DSL and library by Oystein Haugen, Géza Kulcsár and Jerker Delsing, which has been part of the SysML v2 examples distributed with the SysML v2 drafts and first release. An updated DSL and Arrowhead core and support system library that now primarily reflects Eclipse Arrowhead v5.2. The presentation will become available at the AIMS5.0 web and the OMG web.

3.2 Mapping of Relevant Standards and Standardisation Activities

3.2.1 ISO/IEC JTC1 SC42 Artificial Intelligence Standards Mapping

A full list of ISO/IEC JTC1 SC42 AI standards as valid at submission of this document is provided in the Annex (April 20, 2026).

> **Note 1:** A TR has no requirements, it is rather an informal recommendation and study of an issue; a TS includes already normative requirements like a full standard.
>
> **Note 2:** Standards under development ITALIC.

The main AI-Standardisation Organisation is ISO/IEC JTC1 SC42. A structured list, mapped to important subtopics, is provided here:

Ethical concerns, Governance, Human-machine teaming (use cases): Relevant for WP7 and overlapping topics with WP3 and Use Cases

- **ISO/IEC TR 24368:2022 Information technology** — Artificial Intelligence (AI) — Overview of ethical and societal concerns
- ***ISO/IEC CD TS 22443 Information technology** — Artificial intelligence— Guidance on addressing societal concerns and ethical considerations* *(under development)*
- **ISO/IEC TR 24030:2024 Information technology** — Artificial Intelligence — Use cases (Update of version 2021)
- **ISO/IEC 38507:2022 Information technology** — Governance of IT — Governance implications of the use of artificial intelligence by organizations
- **ISO/IEC TS 6254:2025 Information technology** — Artificial intelligence — Objectives and approaches for explainability of ML models and AI systems
- ***ISO/IEC DIS 42105 - Information technology** — AI— Guidance for human oversight of AI system* *(under development).*

Human-machine teaming, Use cases (under development): Relevant in future for advanced collaborative automation

- ***ISO/IEC AWI TR 24030 Information technology** — Artificial intelligence (AI) — Use cases*
- ***ISO/IEC AW CD 42109 Information technology** — Artificial intelligence —Use cases of human-machine teaming*
- ***ISO/IEC PWI 25880 "Information technology** — Artificial intelligence — Requirements and Guidance for organizational implementation of human-machine teaming concept*

Controllability and bias:

- **ISO/IEC TS 8200:2024 Information technology** — Artificial intelligence — Controllability of automated artificial intelligence systems
- **ISO/IEC TS 12791:2024 Information technology** — Artificial intelligence — Treatment of unwanted bias in classification and regression machine learning tasks
- **ISO/IEC TR 24027:2021 Information technology** — Artificial Intelligence (AI) — Bias in AI systems and AI aided decision making

Trustworthiness and Robustness:

- **ISO/IEC TR 24028:2020 Information technology** — Artificial Intelligence — Overview of trustworthiness in artificial intelligence
- **ISO/IEC TR 24029-1:2021 Artificial Intelligence** — Assessment of the robustness of neural networks — Part 1: Overview
- **ISO/IEC 24029-2: 2023 Artificial Intelligence** — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods
- ***ISO/IEC DIS 24029-3 Artificial intelligence (AI)** — Assessment of the robustness of neural networks — Part 3: Methodology for the use of statistical methods* *(under development)*

Risk management: Key topic for all industrial and mobility automation UCs to check

- **ISO/IEC 23894:2023 Information technology** — Artificial Intelligence — Guidance on Risk Management

- **ISO/IEC 42005:2025 Information technology** — Artificial intelligence — AI system impact assessment
- ***ISO/IEC CD 42007 Information technology** — Artificial intelligence — High-level framework and guidance for the development of conformity assessment schemes for AI systems* *(under development)*
- ***ISO/IEC AWI 25870 Artificial intelligence** — Reporting framework for AI incidents* *(under development)*

Functional Safety and AI: Key topic for all industrial and mobility automation UCs to check

- **ISO/IEC TR 5469:2024 Artificial intelligence** — Functional safety and AI systems
- As follow-up and replacement (under development):
  - ***ISO/IEC AWI TS 22440-1** - Artificial intelligence — Functional safety and AI systems — Part 1: Requirements*
  - ***ISO/IEC AWI TS 22440-2** - Artificial intelligence — Functional safety and AI systems — Part 2: Guidance*
  - ***ISO/IEC AWI TS 22440-3** - Artificial intelligence — Functional safety and AI systems — Part 3: Examples of application*

Other Issues/domains: Use Case dependent, general AIMS5.0 goals (sustainability, resilience, human enforcement)

- **ISO/IEC TR 20226:2025 Information technology** — Artificial intelligence — Environmental sustainability aspects of AI systems
- ***ISO/IEC CD TR 18988: Artificial intelligence** — Application of AI technologies in health informatics* *(under development)*
  ***ISO/IEC AWI 22989-2 - Artificial intelligence** — Concepts and terminology - Part 2: Healthcare* *(under development)*

A Use-Case related assessment and analysis of standards is presented in D8.3, based on a specific questionnaire on involvement, knowledge, use and participation in standardisation. Human-related aspects are handled in WP7, D7.3.

3.2.2 Analyse and Align Architectural Outcomes with Standardisation Landscape

To extend the standardisation landscape presented in the section 3.1. This section summarises the standards used by Eclipse Arrowhead. The summary is not complete but is relevant to the reference implementation of the Eclipse Arrowhead architecture. The following are a set of standards used and interpolated within the reference implementation.

- X.509 (ITU-T X.509) Forms the foundation of Arrowhead's identity and trust model. All secure-mode communication relies on X.509 certificates for authentication and authorization, with Arrowhead defining specific certificate profiles.
- TLS / DTLS (RFC 8446 / RFC 9147, IETF) Provide the transport-layer security mechanisms for Arrowhead communication. TLS is used for TCP-based secure communication, while DTLS supports secure communication over UDP in constrained environments.
- OPC UA (IEC 62541 series, IEC) A primary industrial interoperability standard integrated with Arrowhead. OPC UA enables communication with legacy and industrial automation systems and is a key protocol in Arrowhead-based industrial deployments.
- MQTT and CoAP (OASIS MQTT v5.0; IETF RFC 7252) Represent the main lightweight service communication protocols supported in Arrowhead for IoT and distributed systems interoperability. Arrowhead supports protocol translation and orchestration across these.

- SysML (OMG SysML 1.6) and ISO/IEC/IEEE 42010 Provide the architectural and systems engineering foundation for Arrowhead. SysML profiles support modelling of Arrowhead-based systems-of-systems, while ISO/IEC/IEEE 42010 frames architectural description principles.

Below Table 1 provides even more details with relevant references.

Table 1 Additional Standardisation Landscape

Standard	Acronym	Version	SDO	Use in Eclipse Arrowhead	Citations
Domain Names - Implementation and Specification	RFC 1035	1987	IETF	Used as certificate naming convention in Arrowhead release documentation.	(Foundation, 2021), (Mockapetris, P., 1987)
Date and time — Representations for information interchange	ISO 8601	ISO 8601-1:2019	ISO	Used as timestamp format convention in Arrowhead release documentation.	(Foundation, 2021), (ISO, 2019)
Public-key and attribute certificate frameworks	X.509	ITU-T X.509 (10/2019)	ITU-T / ISO/IEC	Used for certificate-based authentication and identity in Arrowhead secure mode and X.509 profiles.	(Arrowhead, 2022), (x509-profiles, 2021), (ITU-T, 2019)
Transport Layer Security Protocol Version 1.3	TLS (RFC 8446)	1.3 (2018)	IETF	Secure communication protocol referenced in Arrowhead X.509 profiles for establishing secure connections.	(x509-profiles, 2021), (E. Rescorla, 2018)
Datagram Transport Layer Security Version 1.3	DTLS (RFC 9147)	1.3 (2022)	IETF	Secure communication protocol referenced in Arrowhead X.509 profiles for constrained/UDP secure connections.	(x509-profiles, 2021), (E. Rescorla, H. Tschofenig, and N. Modadugu, 2022)
MQTT Version 5.0	MQTT	5.0 (2019)	OASIS	Listed among major SOA communication protocols supported for interoperability and translation.	(Arrowhead, 2022), (Tools, 2020), (OASIS, 2019)
Constrained Application Protocol	CoAP (RFC 7252)	2014	IETF	Listed among major SOA communication protocols supported for interoperability and translation.	(Arrowhead, 2022), (Tools, 2020), (Z. Shelby, 2014)
OPC Unified Architecture	OPC UA (IEC 62541)	IEC 62541 series	IEC	Explicitly listed as interoperability target and industrial communication standard in Arrowhead documentation.	(Arrowhead, 2022), (Tools, 2020), (IEC, 2025)
Product data representation and exchange	STEP (ISO 10303)	ISO 10303 series	ISO	Mentioned in Arrowhead interoperability context for integration with industrial data standards.	(Arrowhead, 2022), (ISO, 2024)
Use case methodology - Part 2	IEC 62559-2	2015	IEC	Arrowhead standardisation report states use-case template is based on IEC 62559-2:2015.	(Tools, 2020), (IEC, 2015)

Security for industrial automation and control systems	IEC 62443	IEC 62443-4-2:2019 (series)	IEC / ISA	Listed among cybersecurity standards considered in Arrowhead security/standardisation context.	(Tools, 2020) (IEc, 2019)
Information security management systems — Requirements	ISO/IEC 27001	2022	ISO/IEC	Listed among cybersecurity standards considered in Arrowhead security/standardisation context.	(Tools, 2020) (ISO/IEC, 2022)
Integration of life-cycle data for process plants	ISO 15926	ISO 15926 series	ISO	Mentioned in Arrowhead Tools material as relevant for translation between industrial standards.	(Jerker Delsing, 2022), (ISO, 2018)
Structuring principles and reference designations	IEC/ISO 81346	IEC 81346-1:2022	IEC / ISO	Referenced in Arrowhead Tools material as starting point for engineering structuring principles.	(Jerker Delsing, 2022), (ISO, 2022)
Systems Modeling Language	SysML 1.6	2019	OMG	Arrowhead provides SysML 1.6 profile/library to support architecture and engineering process alignment.	(Delsing, 2021), (Organization, 2019)
Architecture description	ISO/IEC/IEEE 42010	2011	ISO/IEC/IEEE	Explicitly referenced in Arrowhead documentation discussions as target conformance for reference model/meta-model.	(github, 2021) (ISO, 2022)
Function blocks for industrial-process measurement and control systems	IEC 61499	IEC 61499 series	IEC	Eclipse 4diac Arrowhead library uses standard types from IEC 61499 for Arrowhead framework types.	(4diac, 2018) (IEC, 2016)

3.3 Review Ongoing Standards Development Relevant to AI, IoT, and Industrial Automation, Including Human Collaborative Aspects

A good overview on ongoing standardisation activities in ISO/IEC JC1 SC42 can be achieved by looking at the “standards under development” in Section 4. Furthermore, two key aspects should be emphasized:

1. Several standardisation groups outside ISO/IEC JTC1 SC42 are addressing the collaborative aspects Humans-AI machines
2. In the context of existing standardisation domains with upcoming implementations of AI and autonomous decision concepts, e.g. in Smart Manufacturing, evolution has led to new WGs last year and this year. Because of “Industry 5.0”, as addressed by AIMS5.0, these have been joined by partners. In such cases, long-term impact of project results is likely.

A few examples should serve as indication from different domains in which partners have joined at least on national level (not claiming to be complete):

- **ISO TC 204 Intelligent transport systems:**
  - **ISO/DTR 12786 "Intelligent transport systems — Big data and artificial intelligence supporting intelligent transport systems — Use cases"**

- **IEC Industrial Automation and Control:** (IEC TC65, SC65A):
- **IEC TC65 WG 31 Industrial Agents and multi-agent Systems:**
  - **Standard IEC 63718 Agentic AI in industrial automation**
  - **IEC SC65A WG24 Human-machine collaboration**–
    - **Standard IEC 63662** - Human-machine collaborations Part 1: Coordination of multiple risk assessments
  - **IEC TC65 WG 23 Smart Manufacturing**
- **IEC TR 63283-3 ED1**: Industrial-process measurement, control and automation – Smart Manufacturing – Part 3: Challenges for Cybersecurity
- **IEC TR 63283(-4) ED1**(under development): Smart Manufacturing – Part 4: New technologies - (UC 14, UC1, 2, 7, 9, 10, 11, 12, 16, i.e. most smart manufacturing UCs) The identified new technologies relevant for AIMS5.0 are:
  - **AI**
  - Edge computing;
  - Cloud technology;
  - **Digital twin;**
  - **New communication protocols, 5G, TSN;**
  - **Big data and data analytics;**
  - **IoT and IIoT;**
  - **Privacy technology,** etc.

Each chapter has a subchapter on "Technology description", "Use case analysis" and "Standardization needs".

- **ISO TC 199 Safety of machinery:**
  - **ISO TR 22100-5** — Relationship with ISO 12100 - Implications of artificial intelligence machine learning.

(Collaborative, human interactive) Robotics (ISO TC 299) (e.g. UC 6, UC 8, UC 13)

- **ISO 5363:2024** - Test methods for exoskeleton-type walking RACA robot
- **ISO TS 15066: 2016** - Collaborative robots
- **ISO/PAS 5672:2023** - Collaborative applications — Test methods for measuring forces and pressures in human-robot contacts
- **ISO 13482:2014** - Safety requirements for personal care robots (to be replaced by ISO FDIS 13482:2025)
- **ISO_WD 25785-1_(ed1)** - Safety requirements for industrial mobile robots with actively controlled stability (legged, wheeled, or other forms of locomotion) Part 1: robots (under development) – Humanoid Robots
- **ISO/CD 18646-7 [Under development]** - Robotics — Performance criteria and related test methods for service robots — Part 7: Travelling around humans (without affecting human behaviour – ref 13482 too)
- **ISO/FDIS 21423** - Autonomous mobile robots for industrial environments — Communications and interoperability
- ISO AWI 15066-1 - JWG ISO TC299 (WG8) & ISO TC199 (K270.01) - Collaborative safety — Physical contact — Part 1: Biomechanical thresholds and data

Another standardization area is IEC TC56, Dependability, where partners have addressed work on IEC 63697 ED1, Dependability in Realization and Utilization of low volume production and not-tested or partly testable items: ensuring the compliance with the design, and the maintenance of IEC 62741:2015, Demonstration of dependability requirements — The dependability case. The second group of standards is relevant for semiconductor- and hardware reliability and dependable processes.

3.4 Next Steps and Continuation Plan

Standardisation is a medium- to long-term process, leading far beyond the duration of a European research project in the Horizon Programme. It needs long term commitment of key partners in industry and research, which is guaranteed in AIMS5.0, since many partners are active in related and following projects of Horizon Europe and Chips-JU and in all of them active in standardization. The standardisation activities referenced in this deliverable and in D8.3, the final standardisation report part, indicate the ongoing processes and standardisation areas.

- Continuation of the collaboration with CEN/CENELEC to refine the list of standards relevant to CRA and AI act requirements.
- Continuation of the collaboration with International Standardisation Organisations (ISO, IEC, ISO/IEC) and ETSI.
- Continuation of bringing ARROWHEAD related results to standardisation as indicated before.

Section 5.3 provides an overview of standardisation recommendations to fill gaps in WP3 Architecture. These recommendations constitute a point of engagement in ongoing standardization in

- CEN/CENELEC JTC21,
- IEC TC65 (IEC 62443 Industrial cybersecurity, and IEC 62541 (OPC UA - AI model Arrowhead interface)),
- ISO/IEC JTC1 SC42 (AI),
- OMG SysML v2 (model-based system engineering),
- ISO TC199 (Machinery safety),
- ISO TC 299 (Robotics) and
- ISO 50001 (Energy management systems).

For further information, see D8.3, final standardisation report.

4. Architecture Analysis Based on Use Cases

Chapter 4 translates the regulatory and standardisation landscape of Chapters 2 and 3 into a concrete architectural assessment. It evaluates the extent to which the WP3 Eclipse Arrowhead-based architecture, described in detail in D3.2, fulfils the requirements of the AIMS5.0 use cases and identifies where use-case experience generates new standardisation evidence or exposes gaps in existing standards. The nine capability dimensions in Section 4.1 correspond directly to requirement categories that intersect with the CRA and AI Act obligations analysed in Chapter 2. The use case-level standardisation analysis in Section 4.2 maps onto the standards landscape in Chapter 3, particularly Sections 3.2.1 and 3.2.2. Findings from both subsections are synthesised in Section 5.2.

4.1 Architecture Fulfilment of UC Requirements

The architectural fulfilment analysis presented in this section builds on the regulatory and standardisation foundations established in Chapters 2 and 3. The cybersecurity requirements of the CRA (Section 2.1) and the high-risk AI system obligations of the AI Act (Section 2.2) define the compliance envelope within which the WP3 architecture must operate. The harmonised standards landscape described in Section 2.4, together with the ISO/IEC JTC1 SC42 standards mapping in Section 3.2 and the Eclipse Arrowhead standards baseline in Section 3.2.2Provide the normative references within which the nine capability dimensions below are evaluated. Readers are directed to Section 5.2.1 for the resulting regulatory compliance mapping and to Section 5.2.2 for the corresponding architectural improvement guidelines.

This section analyses the extent to which the WP3 microservice cyber architecture, built on the Eclipse Arrowhead framework and described in detail in (Consortium, AIMS5.0 (D3.2), 2025), fulfils the architectural requirements expressed by the AIMS5.0 use cases. Requirements were collected through a structured process documented in (Consortium, AIMS5.0 (D3.1), 2024)/ (AIMS5.0 Consortium (D3.4), 2024), yielding 45 architecture-level requirements (20 public, 25 sensitive). These were further articulated in the use case deliverables (AIMS5.0 Consortium (D5.1), 2024) and (AIMS5.0 Consortium (D6.1), 2023). WP6 (Tier 2, UC09–UC20) contributed 110 requirements and 66 specifications across its 12 use cases, as documented in D6.1. WP5 (Tier 1, UC01–UC08) followed a complementary planning methodology based on KPIs and innovation project definitions, as documented in D5.1. It is worth noting that several requirements were gathered beyond the scope of the use cases but still within the project. Such as the Sentinel Surveillance System, as part of task 3.2.1, for testing and evaluating MLOps practices in Arrowhead-based ecosystems and validating new features that address the collected requirements. This section, however, focuses only on use-case-related requirements as described previously. The analysis organises these requirements into nine architectural capability dimensions and maps each to the corresponding components of the realised architecture.

Note: Five selected Use Cases are discussed in detail. A general discussion on standardisation involvement, use, knowledge and participation is provided for all Use Cases in D8.3.

4.1.1 Overview of Use Case Architectural Requirement Categories

The use cases impose requirements that collectively span nine dimensions, as shown in Table 2.

Table 2 Use case Requirement Categories

#	Requirement Category	Representative Use Cases	Requirement Examples
R1	**Service discovery and dynamic composition**	UC02 (AI Enhanced Value Chain), UC03 (Servitization), UC10 (AI-MES)	Dynamic binding of AI services to consumers; loosely coupled microservice integration
R2	**AI integration and MLOps lifecycle**	UC01 (Green AI), UC05 (Machine Tool AI), UC06 (Robotic Feeding), UC15 (ML Models)	Model training, versioning, deployment and monitoring at edge/fog/cloud
R3	**Multi-tier edge/fog/cloud deployment**	UC05 (IDEKO/SAVVY), UC07 (Luminaire DT), UC08 (TTMS/AMR), UC13 (AMHS)	AI inference at edge; model management at fog; archival and fleet management in cloud
R4	**Security, authentication and access control**	UC11 (Indoor Farming), UC16 (RF Production), UC18 (Supply Chain)	Certificate-based identity; authorisation enforcement per service; physical tag authentication
R5	**Real-time and deterministic networking**	UC08 (AMR TTMS), UC09 (Wafer Fab Scheduling), UC13 (OHT Predictive Maintenance)	Sub-millisecond control loops; guaranteed end-to-end latency; TSN backbone
R6	**Digital twin and simulation support**	UC04 (BMW Production-Logistics), UC07 (Luminaire DT), UC14 (Virtual Commissioning)	Physics-coupled simulation; training data generation; pre-shipment virtualisation
R7	**Semantic and protocol interoperability**	UC02 (Knowledge Distribution), UC10 (RAMII/MES), UC18 (Supply Chain Ontology), UC19 (DRO/NXP)	OPC UA/MQTT/CoAP translation; ontology-based data harmonisation; cross-site consistency
R8	**Human-centric and explainable AI**	UC07 (Human-Augmented Assembly), UC08 (BCI Exoskeleton), UC12 (Human-in-the-Loop XAI)	SHAP-based explanations; gesture recognition; skill-adaptive operator interfaces
R9	**Sustainability and energy awareness**	UC01 (Green AI), UC09 (Energy-Aware Scheduling), UC17 (Contamination Management)	ISO 50001-compliant monitoring; AI-driven peak shaving; green tool strategies

4.1.2 Fulfilment by Architectural Capability Dimension

The following sections examine each requirement category and identify the relevant use cases and requirements.

4.1.2.1 R1 – Service Discovery and Dynamic Composition

The Eclipse Arrowhead Service Registry, Orchestration System, and Authorisation System collectively provide the three fundamental SOA properties required by the use cases: look-up (UC02 sub-case C requires intelligent microservice discovery for Kafka-driven analytics), late binding (UC03 requires dynamic model registration on highly constrained edge devices), and loose coupling (UC10 requires independently evolvable MES-to-AI interface components within the RAMII concept). The Orchestrator's composition capability directly addresses the requirement in UC08 for dynamic task-level coordination among three Omron LD-60 AMRs. The Choreographer support system further enables multi-step workflow coordination across loosely bound services, meeting the automation requirements of UC05 (multi-layer AI at machine tool level). The architecture, therefore, fully supports R1. The service-oriented architecture patterns underlying this dimension align with the IEC 62559-2 use case methodology (Section

3.2.2, Table 1) and are relevant to the transparency and information provision requirements of AI Act Art. 13 (Section 2.2.2.2).

4.1.2.2 R2 – AI Integration and MLOps Lifecycle

The AI-gym, documented in D3.2 Section 4It provides a three-layer architecture that directly fulfils the MLOps requirements expressed in UC01, UC05, UC06, and UC15. The Apache Zeppelin-based development layer covers the model development requirements in UC15 (productionised ML models with versioning and rollback). The Arrowhead Adapter layer covers service registration of trained models, responding to UC06's requirement that independently developed YOLO v8 / PPO modules be composable as services. The MLOps CI/CD pipeline (Jenkins, Roboflow, Model Manager) fulfils UC01's requirement for continuous model retraining triggered by new labelled data, as well as the automatic deployment requirement validated in the SSN winery pilot (D3.2 Section 3.2.1). The AI-gym's integration with the Arrowhead IIoT data layer (the third tier) fulfils UC11's requirement for closed-loop environmental control using a fine-tuned GPT-2 model for temperature prediction, which was operationally validated in the greenhouse demonstrator. R2 is substantially fulfilled; the main residual gap is the absence of a standardised model audit trail and data lineage mechanism for regulated environments (relevant to UC16 and UC12 sub-project 1). The model audit trail gap identified here maps directly to AI Act Arts. 10 and 12 (Section 2.2.2) and to the dataset governance standards ISO/IEC 5259 series and ISO/IEC 42005:2025 listed in Section 3.2.1. The residual gap is addressed in Guideline 1 (Section 5.2.2).

4.1.2.3 R3 – Multi-Tier Edge/Fog/Cloud Deployment

The three-tier deployment architecture (Savvy SmartBox at edge, Dell PowerEdge R660xs at fog, cloud cluster) directly supports the deployment topology required by UC05, UC07, UC08, and UC13. The SmartBox (Intel Celeron N2930, 8 GB RAM) fulfils UC13's requirement for Edge AI anomaly detection on MEMS microphones attached to OHT shuttles, evaluated against the hardware feasibility constraints of traditional ML (Random Forest, SVM). For UC08, the TTMS web-based modules for traffic management and task assignment are deployed at fog level, communicating via ActiveMQ relays with edge AMRs. For UC07's intelligent scheduling sub-use-case, the Arrowhead inter-cloud Gatekeeper/Gateway mechanism meets the requirement for secure cross-site data exchange between the manufacturing site and cloud-based digital twin environments. Three autonomous Arrowhead Local Clouds (edge, fog, cloud) ensure that each tier maintains independent operation, fulfilling the resilience requirements expressed in UC03 for zero-administration failover. R3 is fully supported by the architecture; the remaining gap is the absence of a formally specified service-level agreement (SLA) mechanism for tier-to-tier latency bounds. The inter-cloud security mechanisms correspond to the IEC 62443-3-3 and ISO/IEC 27001:2022 entries in the Table Table 1 (Section 3.2.2). The SLA gap is addressed in Guideline 5 (Section 5.2.2).

4.1.2.4 R4 – Security, Authentication, and Access Control

The architecture fulfils security requirements across multiple layers. At the network and transport level, the X.509 certificate profiles and TLS 1.3/DTLS 1.3 implementation provides the identity and mutual authentication required by UC11 (Arrowhead-controlled access to sensor actuator services) and UC18 (cross-company supply chain data exchange). At the physical and device level, the NFC/RFID inline personalisation system (CISC Semiconductor, SAM AV3, AES-128) fulfils UC12 sub-project 3's requirement for physical access control to FOUP-level logistics assets, with TAM2 challenge-response authentication completing within the specified duration. The ESPAR intelligent antenna system (GUT) with 4,096 beam patterns and Arrowhead-registered pattern selection service supports the UC08 and UC13 requirements for secure and reliable wireless communication in dynamic factory environments. The

Authorisation System's per-service access control enforcement meets the data sovereignty requirements expressed in UC02 sub-case A (consumer data pipeline privacy) and UC19 (DRO-based ontology access restriction). R4 is substantially fulfilled; the residual gap is the absence of a documented end-to-end threat model and attack surface analysis for the multi-tier deployment, which is being addressed in Section 4.3 (UC11 security analysis by AIT). The X.509/TLS implementation maps to the standards baseline in Section 3.2.2(Table 1). The end-to-end threat model gap is relevant to CRA Annex I Part I (Section 2.1.2) and AI Act Art. 15 (Section 2.2.2.2), and is addressed in Guideline 4 (Section 5.2.2).

4.1.2.5 R5 – Real-Time and Deterministic Networking

The TTTech time-triggered computation and communication framework, integrated with TSN and the iSMT hierarchical scheduler, directly addresses the real-time requirements in UC08 (AMR deadlock-free fast routing for task management decisions) and UC09 (wafer fab energy sensor data sets a minimum time resolution per Specification S9). The iSMT scheduler, using Satisfiability Modulo Theories with incremental context management demonstrates resource-efficient determinism at the fog layer. For UC13, the MEMS microphone platform requirements (IEC 60068-2-6 vibration, 10,000 g shock per IEC 60068-2-27) are met at the hardware level by the selected silicon microphone components, while edge AI inference on the anomaly detection pipeline is supported by the SmartBox's compute resources for traditional ML. R5 is substantially fulfilled for the use cases validated in Y2; formal end-to-end latency specification for control-critical loops (UC08 exoskeleton BCI response time, UC09 real-time sensor interruption) remains an open requirement. IEEE 802.1 TSN is identified as a key standard in Section 4.2.3 (UC08). The formal latency specification gap is addressed in Guideline 5 (Section 5.2.2).

4.1.2.6 R6 – Digital Twin and Simulation Support

The architecture's data pipeline (edge-to-fog-to-cloud) provides the infrastructure for digital twin workflows in UC04 (BMW Full-Digital-Twin via autonomous 3D scanning and Omniverse environment), UC07 (Signify luminaire assembly simulation), and UC14 (virtual commissioning of FMX AMHS vehicles). The Arrowhead Event Handler fulfils UC07's requirement for asynchronous event-driven simulation updates triggered by physical assembly state changes. The MLOps data flow supports UC04's requirement for AI training data generation from virtual twin environments prior to physical deployment. The multi-cloud Gatekeeper/Gateway mechanism enables the cross-site twin synchronisation needed in UC04's four-phase approach (physical scan → Omniverse DT → AI training → supply robot optimisation). R6 is partially fulfilled at the infrastructure level; the digital twin middleware layer (semantic model binding, simulation co-execution) is not natively part of the Arrowhead architecture and is provided by use-case-specific tooling (Omniverse, Stream Analyse, Signify DT framework). The Arrowhead SysML profile (Section 3.2.2, Table 1) provides the modelling foundation for digital twin architectural description; the simulation co-execution gap falls outside both the Arrowhead core and the current SC42 AI standards scope (Section 3.2.1). Digital Twin Standards are either from ISO TC184 SC4 (Industrial data) or ISO/IEC JTC1 SC41, IoT and Digital Twin.

4.1.2.7 R7 – Semantic and Protocol Interoperability

OPC UA (IEC 62541) integration provides the primary industrial protocol bridge required by UC05 (SAVVY SmartBox to SORALUCE machine tool CNC interface) and UC10 (RAMII MES harmonisation across heterogeneous equipment). MQTT v5.0 and CoAP support in the Arrowhead protocol translation layer fulfils UC02's Kafka-to-microservice interoperability requirement and UC03's constrained device streaming requirement (100 KB RAM minimum). The Digital Reference Ontology (DRO) integration with the Open Access Platform ((AIMS5.0 Consortium (D4.6), 2025)) addresses UC18 and UC19's requirements for cross-company semantic harmonisation of supply chain data, with ontology-based flexible data translation enabling static and dynamic

transformation procedures. The Industrial Data Ontology (IDO, ISO 23726-3) work within Arrowhead fPVN further supports the semantic interoperability ambitions of UC02 sub-case E (knowledge distribution via Semantic Web). R7 is partially fulfilled; full semantic interoperability at scale (dynamic ontology federation, runtime knowledge graph queries) depends on ongoing Arrowhead/OAP integration work planned for Y3. The OPC UA, MQTT, and CoAP entries in Table 1(Section 3.2.2) define the standards baseline. The ontology federation gap relates to ISO/IEC 21823-3 and the IDO (ISO 23726-3) work described in Section 5.1.1, and is addressed in Guideline 6 (Section 5.2.2).

4.1.2.8 R8 – Human-Centric and Explainable AI

The AI-gym's integration with the Arrowhead Event Handler enables human-in-the-loop workflows required by UC12 sub-project 1 (SHAP-based XAI for process variability transparency) and UC07 sub-use-case A (keypoint-based operator guidance). The multi-modal LLM-based TD-Interpreter (developed for timing diagram analysis in D3.2 Section 3.2.4 - (Consortium, AIMS5.0 (D3.2), 2025)) demonstrates an architectural pattern for LLM-assisted decision support that is generalisable to UC08's requirement for explainable AMR task decisions communicated to workers in natural language. UC08's BCI exoskeleton (brain-signal control for disabled workers) and audio-visual AMR interaction requirements impose specific real-time event handling constraints met by the Arrowhead Event Handler and the ESPAR antenna system. The Arrowhead-based privacy-preserving local LLM deployment pattern (llama.cpp / LLaVA 7B) addresses UC07's privacy-first keypoint detection requirement. R8 is partially fulfilled; operator-facing interface components and XAI visualisation frameworks are use-case-specific and not part of the core Arrowhead architecture. The human oversight gap is directly regulated by the AI Act Art. 14 (Section 2.2.2.2) and relates to ISO/IEC DIS 42105 and prEN 18229-1 listed in Sections 3.2.1and 3.1.1respectively. It is addressed in Guideline 2 (Section 5.2.2).

Relevant standards are listed in section 3.2.1 under “Ethical concerns”, “Trustworthiness” and “Controllability”.

4.1.2.9 R9 – Sustainability and Energy Awareness

The multi-tier data pipeline supports ISO 50001-compliant energy monitoring as required by UC09 (wafer fab batch scheduling) and UC01 (injection moulding green tool strategies). The SmartBox edge layer's data collection capability (Specification S10: zero-reference counter, fast RS485 transmission) fulfils UC09's sensor integration requirements. The MLOps pipeline supports the continuous retraining of energy forecasting models required by UC01 and UC09. The Arrowhead Orchestrator's dynamic service composition capability enables the "golden tool" strategy pattern, where energy-optimised process parameterisation services can be dynamically injected into production workflows. R9 is partially fulfilled at data collection and AI model deployment level; the scheduling optimisation algorithms (time-of-use tariff-aware dispatching rules) are use-case-specific components not provided by the core architecture. ISO 50001 is identified as the governing standard in Section 4.2.4 (UC09). The scheduling optimisation gap is addressed in Guideline 8 (Section 5.2.2). In section 3.2.1, **ISO/IEC TR 20226:2025** Information technology — Artificial intelligence — Environmental sustainability aspects of AI systems, is referenced.

4.1.3 Fulfilment Summary

Table 3 summarises the overall architectural fulfilment assessment across the nine requirement dimensions.

Table 3 Architectural fulfilment across the requirement dimensions

Category	Arrowhead Components	Fulfilment	Residual Gaps
R1 – Service discovery and composition	Service Registry, Orchestrator, Choreographer	Full	—
R2 – AI integration and MLOps	AI-gym, MLOps pipeline, Model Manager	Substantial	Model audit trail; data lineage for regulated environments
R3 – Multi-tier deployment	SmartBox / PowerEdge / Cloud, Local Clouds, Gatekeeper	Full	Formal SLA mechanism for tier-to-tier latency
R4 – Security and access control	X.509/TLS, Authorization System, NFC/RFID, ESPAR	Substantial	End-to-end threat model documentation
R5 – Real-time networking	TTTech, TSN, iSMT Scheduler	Substantial	Formal latency specification for control-critical loops
R6 – Digital twin support	Data pipeline, Event Handler, inter-cloud Gateway	Partial	DT middleware (semantic binding, simulation co-execution)
R7 – Semantic interoperability	OPC UA, MQTT/CoAP, DRO/OAP, IDO	Partial	Ontology federation; runtime knowledge graph integration
R8 – Human-centric and XAI	Event Handler, local LLM pattern, ESPAR	Partial	Operator interface components; XAI visualisation layer
R9 – Sustainability	Data pipeline, MLOps, Orchestrator composition	Partial	Domain-specific scheduling optimisation

Overall, the Eclipse Arrowhead-based microservice architecture fully or substantially addresses the core infrastructure requirements of the AIMS5.0 use cases — service composition, AI deployment, security, multi-tier data pipelines, and real-time networking. Partial fulfilment areas are concentrated in domain-specific middleware layers (digital twin co-execution, semantic federation, operator interfaces, and scheduling optimisation), which are addressed by use-case-level components that integrate with but are not part of the Arrowhead core. These residual gaps are consistent with the deliberate separation of concerns between the integration platform (WP3) and domain-specific application logic (WP1, WP5, WP6) and are expected to be further resolved in Y3 system-level validation activities as documented in (AIMS5.0 Consortium (D1.3), 2025).

4.2 Architectural Analysis for Standardisation in the Use Cases

Section 3.2 established the foundational standards on which the Eclipse Arrowhead architecture is built (Table 1), and Section 3.3, mapped the broader ISO/IEC JTC1 SC42 AI standards landscape. The present section extends that analysis from the use case perspective: it examines the architectural implementations carried out within AIMS5.0 use cases (UC02, UC05, UC08, and UC09 are treated as primary examples) and analyses how those implementations interact with the standards identified in Sections 3.1–3.3, where existing standards are applied or validated in practice, and where use case experience points to requirements for new or evolved standardisation. The regulatory obligations established in Chapter 2 — in particular, the CRA essential cybersecurity requirements (Section 2.1.2) and the AI Act high-risk regime (Section 2.2.2.2) — provide the compliance framing within which the architectural choices are assessed. Cross-cutting findings are summarised in Table 4 and feed directly into the regulatory compliance mapping in Section 5.2.1and the standardisation recommendations in Section 5.2.3.

The analysis follows a uniform structure for each use case: (1) description of the architectural context and the relevant system boundary; (2) standards implicated by the architectural

choices; (3) observed fulfilment or shortcoming in relation to those standards; and (4) inferred standardisation observations. A cross-cutting summary table closes the section.

4.2.1 UC02 – AI Enhanced Value Chain: Protocol Interoperability and Semantic Standards

Architectural context. UC02 (Philips Drachten / PCL, with RUG, TU/e, SEMAKU) deploys an SOA-based analytics infrastructure whose data distribution layer uses Apache Kafka for pub/sub messaging across machine and manufacturing sub-systems, while AI microservices communicate via the Arrowhead Service Registry and Orchestrator. Sub-use-case E introduces semantic knowledge distribution using Protégé-based ontologies aligned with the Digital Reference Ontology (DRO) from WP4. Sub-use-case A processes deep learning models (2D convolution, k-NN, XGBoost) over connected product sensor data. This sub-use-case engages the protocol standards listed in Table 1(Section 3.2.2): MQTT v5.0 and CoAP for lightweight messaging, and ISO/IEC 21823-3 for semantic interoperability. The CRA data minimisation requirement (Section 2.1.2, item 7) is also relevant to the consumer data pipeline.

Standards implicated. The Arrowhead architecture mediates between the Kafka-native data lake and the service-oriented AI microservice layer via MQTT v5.0 (OASIS) and CoAP (IETF RFC 7252) adapters, both listed in the Arrowhead standards baseline (Section 3.2.1). Protocol translation between these message-passing paradigms and the REST-over-TLS service invocation model native to Arrowhead raises conformance questions with respect to IEC 62559-2 (Use Case Methodology), which provides the template used across all AIMS5.0 use cases, and with ISO/IEC 21823-3 (IoT Interoperability — Semantic Interoperability), which underpins the ontology-based knowledge layer. The DRO ontology integration in sub-use-case E relies on sub-ontology access control enforced through the Arrowhead Authorization System, creating an architectural pattern where W3C OWL/RDF semantic standards are governed by an SOA-level authorization service — an interaction not presently covered by either standard in isolation.

Fulfilment observations. The MQTT and CoAP integration meets the basic protocol requirements of the production data pipeline. The Arrowhead Authorization System provides the access control mechanism required for data sovereignty in multi-company knowledge sharing, consistent with ISO/IEC 27001:2022 information security management principles. The semantic layer, however, lacks a standardised binding between the DRO ontology lifecycle (versioning, deprecation, extension) and the Arrowhead Service Registry, meaning that ontology updates are not automatically reflected in service descriptions.

Standardisation observation. UC02 demonstrates that service-oriented industrial architectures increasingly require a formal mechanism for linking semantic data models (ontologies, knowledge graphs) to SOA service metadata. This gap points to a need for standardisation at the intersection of ISO/IEC 21823-3 and service registry specifications, an area where Arrowhead's architecture, extended with the DRO and the IDO (proposed ISO 23726-3), is positioned to contribute concrete input.

4.2.2 UC05 – Multi-Layer AI in Machine Tool Domain: OPC UA Integration and Industrial Security

Architectural context. UC05 (IDEKO, SORALUCE, GOIMEK, SAVVY, MVC) deploys the Savvy SmartBox edge device as the Arrowhead Local Cloud gateway at machine-tool level, with the SmartBox interfacing to CNC equipment via OPC UA and feeding collected data to a fog-level AI-gym for predictive maintenance and process optimisation model development and deployment. The multi-layer architecture (D3.2 Section 3.2.2- (Consortium, AIMS5.0 (D3.2), 2025)) involves three autonomous Arrowhead Local Clouds (edge, fog, cloud), interconnected

via inter-cloud Gatekeeper/Gateway mechanisms. The OPC UA integration engages IEC 62541 as listed in Table 1 (Section 3.2.2). The multi-cloud security model is evaluated against IEC 62443-3-3 and IEC 62443-4-2 (Section 3.2.2), whose CRA relevance is established in Section 2.4.2.

Standards implicated. OPC UA (IEC 62541 series) is the primary industrial interoperability standard in this architecture: the SmartBox implements an OPC UA client interface consuming structured process data from the SORALUCE machine tool's OPC UA server, then translates it into Arrowhead service payloads. This bridging between IEC 62541 (OPC UA) and the Arrowhead REST/TLS service model establishes a concrete reference implementation for one of the most frequently cited interoperability requirements in industrial automation standardisation. The multi-cloud inter-cloud security (X.509 certificates + TLS 1.3, Gatekeeper authorisation logic) maps to the security requirements of IEC 62443-4-2 (Security for Industrial Automation and Control Systems – Component requirements) and IEC 62443-3-3 (System security requirements and security levels), both referenced in the Arrowhead standardisation baseline. The data collection pipeline from edge to fog also interacts with ISO/IEC 27001:2022 asset management and logging requirements.

Fulfilment observations. The OPC UA–to–Arrowhead translation layer demonstrates that the Arrowhead SOA model and IEC 62541 are composable in practice, with the SmartBox acting as the boundary system. Authentication at the SmartBox level (X.509 mutual TLS for both OPC UA secure channel and Arrowhead service calls) provides a layered security posture consistent with the defence-in-depth principle of IEC 62443-3-3. The AI-gym model deployment pipeline (Jenkins CI/CD, Model Manager, Arrowhead service registration) introduces a software update and deployment pathway that should be assessed against IEC 62443-4-1 (Secure product development requirements), particularly requirements for patch management and update integrity verification.

Standardisation observation. UC05 provides evidence that a structured translation profile between OPC UA (IEC 62541) and SOA service registries (such as Arrowhead's) would eliminate the need for bespoke adapter implementations in each deployment. The Arrowhead Tools project previously proposed such an integration; the UC05 implementation strengthens the case for formalising this as a normative interface profile within or alongside the IEC 62541 companion specification framework. Additionally, the multi-tier MLOps pipeline raises the question of whether IEC 62443-4-1 should be extended to address AI model lifecycle operations (training, validation, deployment, rollback) as first-class software update categories.

4.2.3 UC08 – AI Supporting Human and Manufacturing Cycles: Real-Time Networking and Human-AI Safety Standards

Architectural context. UC08 (SmartUniversal / SU, TUBITAK) is architecturally the most standards-demanding use case in AIMS5.0 from a safety and real-time perspective. It integrates three Omron LD-60 AMRs coordinated via the TTMS (Task & Traffic Management System), an AMR perception system with sensor fusion (LiDAR, camera, radar) and hand gesture recognition, and a BCI-controlled upper-body exoskeleton. The TTMS operates as an Arrowhead-registered microservice cluster. Real-time networking is provided by the TTTech time-triggered framework with TSN backbone and iSMT hierarchical scheduling (Section 3.2.4 of D3.2 - (Consortium, AIMS5.0 (D3.2), 2025)), integrated at the fog level.

Standards implicated. The real-time communication infrastructure relies on IEEE 802.1 Time-Sensitive Networking (TSN) standards — specifically IEEE 802.1Qbv (Enhancements for Scheduled Traffic) and IEEE 802.1Qcc (Stream Reservation Protocol enhancements) — which are the underlying standards for the TTTech framework's schedule table generation and frame management. The iSMT scheduler's Satisfiability Modulo Theories approach for hierarchical

CPU/VCPU allocation addresses deterministic compute requirements but is not yet covered by any published standard; it represents a candidate contribution to future IEC 61499 (Function blocks for distributed industrial systems) or to automotive-derived real-time scheduling standards such as AUTOSAR OS specifications adapted for industrial contexts. The AI Act high-risk classification of the BCI exoskeleton system is established under the framework set out in Section 2.2.2.2. The CRA essential requirements in Section 2.1.2apply simultaneously to the product's digital elements. The relevant harmonised standards under development — prEN 18229-1, prEN 18282 — are listed in Section 3.1.1.

The BCI-controlled exoskeleton and the AMR human gesture recognition system are directly in scope for the EU AI Act (Regulation 2024/1689): a BCI-based control system used in a professional work context is likely to qualify as a high-risk AI system under the AI Act's Annex III (AI systems intended to be used as safety components of products or systems), triggering the full high-risk compliance regime. The architectural requirements this imposes — continuous risk management system, technical documentation, logging and record-keeping, human oversight mechanisms, accuracy, robustness, and cybersecurity requirements (AI Act Articles 9–15) — must be mapped onto the Arrowhead-based architecture. The ESPAR intelligent antenna system (Section 3.2.3.2) contributes to the cybersecurity layer by providing adaptive physical-layer protection for the wireless communication between AMRs and the TTMS, an aspect relevant to IEC 62443-4-2 (wireless component security requirements) and to the CRA's essential cybersecurity requirements.

Fulfilment observations. The TTTech/TSN integration provides the deterministic communication infrastructure required for the deadlock-free AMR routing loops, meeting the functional requirements implied by the control cycle time constraints. The AI Act's logging and record-keeping requirements (Article 12) are partially addressed by the Arrowhead System Monitor and Event Handler, which can record service invocations and state transitions. However, the specific AI Act requirement for human oversight of high-risk AI systems, particularly the ability for an operator to override, interrupt, or correct the AI system's output, is not yet explicitly modelled as a service interface in the Arrowhead core. The exoskeleton BCI-to-Arrowhead integration also raises unanswered questions about data minimisation (CRA Annex I, requirement 7) in the context of continuous brain-signal data processing.

Standardisation observation. UC08 is the AIMS5.0 use case most directly affected by the convergence of the CRA, the AI Act, and industrial real-time networking standards. It constitutes a concrete reference scenario for the standardisation work being coordinated through CEN-CENELEC JTC 21 WG5 (cybersecurity for AI systems) and is relevant to the M/606 IEC 62443-based security profiles for industrial systems. The iSMT scheduler's demonstrated performance advantage over EDF provides quantitative evidence that could inform future revisions of real-time scheduling requirements in industrial standards. A formal model of the TTMS service architecture in Arrowhead DSL / SysML v2 notation, verified against TSN schedule constraints, would be a direct contribution to ongoing OMG SysML v2 standardisation activities (Section 3.1.1).

4.2.4 UC09 – Energy-Aware Scheduling in Wafer Fabrication: Energy Standards and Use Case Methodology

Architectural context. UC09 (FUH, IFD, IFAT, SYSTEMA) targets energy-aware batch scheduling in semiconductor wafer fabrication, deploying energy sensors at fab measurement points (Modbus/Ethernet connectivity), integrating energy data into a scheduling optimisation system with time-of-use tariff awareness, and providing ISO 50001-compliant visualisation and reporting. The sensor data pathway connects to the MES layer via the RAMII (Real-time Adaptive Manufacturing Information Infrastructure) concept, with AI algorithms performing dispatching rule optimisation. The IEC 62559-2 use case methodology referenced here is also the template

underpinning all AIMS5.0 use case specifications (Table 1, Section 3.2.2). ISO 50001 is the energy management standard whose interface with AI scheduling is identified as a standardisation gap, as further discussed in Guideline 8 (Section 5.2.2.8).

Standards implicated. The use case requirements are explicitly structured using IEC 62559-2 (Use Case Methodology, Part 2), the same template adopted across all AIMS5.0 use cases (Section 3.2.1), confirming IEC 62559-2 as an effective requirement engineering bridge between domain experts and architecture designers. Energy monitoring and peak shaving optimisation must conform to ISO 50001:2018 (Energy Management Systems), which is explicitly required by the UC09 use case partners. The sensor specifications (zero-reference counter capability, minimum time interruption, fast RS485 transmission, visualisation per IEC 61000-6-x/-4-x family) map to power quality monitoring standards. The Modbus/Ethernet sensor protocol is a widely deployed industrial communication standard without a formal IEC specification but with a de facto normative status in semiconductor manufacturing environments; it requires bridging to the Arrowhead service layer via a protocol adapter analogous to the OPC UA adapter in UC05.

Fulfilment observations. The Arrowhead architecture provides the data collection and service orchestration infrastructure needed for the sensor integration and AI scheduling service deployment. ISO 50001 compliance is achieved at the monitoring and reporting level through the data pipeline; the standard's Plan-Do-Check-Act management system cycle is supported by the AI-gym's model retraining and deployment loop, though explicit ISO 50001 conformity artefacts (energy review documentation, energy performance indicator registration) are not generated by the architecture automatically. The IEC 62559-2-based requirements structure of UC09 demonstrates that this standard effectively captures both functional and technical requirements for AI-integrated industrial automation use cases, lending support to the ongoing WP3 requirements collection methodology (Consortium, AIMS5.0 (D3.1), 2024)/ (AIMS5.0 Consortium (D3.4), 2024).

Standardisation observation. UC09 provides concrete evidence that IEC 62559-2 is fit for purpose as a requirement engineering standard for AI-enabled industrial systems, including those with energy management objectives. The integration between ISO 50001 energy management and AI-driven scheduling optimisation constitutes a novel application pattern that is not yet addressed by either standard. A standardised interface between ISO 50001 energy performance indicators and AI model inputs/outputs, potentially expressed via OPC UA companion specifications or Arrowhead service metadata, would accelerate the adoption of AI-based energy optimisation in regulated industrial environments. This is consistent with the ongoing M/606 work on energy-related product security profiles and with the AI Act's requirements for documentation and logging of high-risk AI systems used in industrial automation.

4.2.5 Cross-Cutting Standardisation Analysis Summary

The standardisation implications of these architectural findings are already discussed and mapped in Section 3, where Table 4 summarises the standards-relevant architectural findings across the four analysed use cases and maps them to standardisation actions or observations.

Table 4. Standards-relevant architectural findings across the four analysed use cases

Use Case	Architectural Pattern	Relevant Standard(s)	Arrowhead Element	Standardisation Observation
UC02 – AI Value Chain	Kafka-to-SOA protocol bridging; ontology-	MQTT v5.0, CoAP, W3C OWL/RDF,	Arrowhead Service Registry,	Formalise binding between semantic data models and SOA service metadata; ontology

	governed data sharing	ISO/IEC 21823-3, ISO/IEC 27001	Authorization System	lifecycle and registry synchronisation gap
UC02 – sub-case E	Cross-company knowledge distribution via DRO	W3C OWL/RDF, ISO/IEC 21823-3, IDO (ISO 23726-3)	DRO / OAP integration with Arrowhead Authorization	Input to ISO/IEC 21823-3 revision: SOA-level governance of shared industrial ontologies
UC05 – Machine Tool AI	OPC UA–to–Arrowhead bridge; MLOps over multi-tier Arrowhead clouds	IEC 62541, IEC 62443-3-3, IEC 62443-4-1, IEC 62443-4-2	SmartBox OPC UA adapter, Gatekeeper, AI-gym CI/CD	Propose normative OPC UA–to–Arrowhead interface profile; extend IEC 62443-4-1 for AI model lifecycle operations
UC08 – AMR + TTMS	TSN real-time networking; AI Act high-risk scope (BCI, exoskeleton)	IEEE 802.1Qbv/Qcc, IEC 61499, EU AI Act Arts. 9–15, IEC 62443-4-2, CRA	TTTech/iSMT scheduler, ESPAR antenna, Arrowhead Event Handler, System Monitor	iSMT scheduling performance data as input to future real-time scheduling standards; AI Act high-risk AI logging mapped to Arrowhead monitor services; input to JTC 21 WG5 (AI cybersecurity)
UC09 – Energy Scheduling	ISO 50001-compliant energy monitoring; AI-driven batch scheduling	ISO 50001, IEC 62559-2, IEC 61000-6-x/-4-x, Modbus	Data pipeline, AI-gym MLOps, Arrowhead Service Orchestrator	Validate IEC 62559-2 for AI-enabled industrial UCs; propose ISO 50001 to AI model interface via OPC UA companion spec
All UCs	Multi-tier Arrowhead Local Cloud deployment	IEC 62443-3-3 (security levels), X.509, TLS 1.3, ISO/IEC 27001	Gatekeeper/ Gateway, Certificate Authority, Authorization System	Arrowhead multi-tier inter-cloud security model as candidate reference implementation for IEC 62443-3-3 Level 2–3
All AI UCs	AI Act compliance scope	EU AI Act (2024/1689), CRA (Annex I), JTC 21 WG5	AI-gym, System Monitor, Event Handler	Architecture support for AI Act Articles 9–15 is partial; human oversight service interface and conformity documentation generation are open standardisation needs

4.3 Architectural Analysis for Standardisation involved in UC11

UC11 (AI-supported Industrial IoT for Indoor Food Production) demonstrates the integration of multiple emerging technologies: Artificial Intelligence for autonomous control, Internet of Things (IoT) for distributed sensing, cloud-edge architectures for knowledge management and decision-making, and microservice-based orchestration. The architectural analysis for standardisation in UC11 addresses the technical and regulatory requirements across four interconnected sub-scenarios: visual plant mass estimation, wireless communication optimization, microservice-based architecture for autonomous production control, and cybersecurity compliance with the EU Cyber Resilience Act (CRA).

4.3.1 System Architecture and Key Components

UC11 deploys a vertically organized architecture comprising three operational layers: the field layer containing sensors (soil, environmental parameters) and actuators (irrigation pumps, lighting, climate control); the edge layer hosting local processing, AI inference, and real-time response mechanisms; and the cloud layer supporting knowledge extraction, AI model updates, and enterprise integration. Sensor data flows continuously from the field to edge computing nodes, where MAPE-K (Monitor, Analyse, Plan, Execute, Knowledge) loops execute autonomous

control decisions. Environmental parameters monitored include pH, electrical conductivity (EC), light intensity, temperature, and humidity. The system is designed to operate autonomously but includes human override capabilities and fallback mechanisms to rule-based control when necessary.

4.3.2 Key Standardisation Activities and Technical Work

4.3.2.1 Security Analysis Framework and Threat Modelling

A comprehensive cybersecurity framework has been established based on ThreatGet, a systematic threat modelling and risk assessment tool. The framework aligns UC11 operations with the essential requirements of the EU Cyber Resilience Act (CRA). The initial high-level architectural model for UC11 documents the operational environment (field layer components, sensors, actuators) and the remote monitoring and control environment (network devices, servers, data stores). Security controls have been defined for critical components such as sensor ECUs, and the threat database identifies potential cyber risks across the full system lifecycle. The work was focused on ensuring a high level of CRA compliance of UC11, but also collection of insights regarding implementation of the CRA, which was used as input for the development of harmonized standards.

4.3.2.2 System Architecture Modelling and Service Orchestration

UC11 employs the Eclipse Arrowhead framework for service-oriented architecture and secure orchestration. The implementation leverages containerized microservices deployed on edge computing devices, enabling modularity and real-time responsiveness. Key architectural patterns include: (1) service discovery and dynamic orchestration through Arrowhead core services; (2) edge-based AI inference for low-latency decision-making; (3) separation of concerns between sensor data ingestion, analytics, planning, and actuation; and (4) secure inter-service communication with standardized encryption and authentication protocols. The MAPE-K feedback loop is implemented through Arrowhead event handling and service composition, creating a closed-loop autonomous control system. Standardisation and development of ARROWHEAD is ongoing as Eclipse activity.

4.3.2.3 Trustworthiness Analysis: AI Reliability, IoT Robustness, and Human Oversight

UC11 represents a distributed cyber-physical system in which AI-enabled control, IoT sensing, autonomous operation, and collaborative service orchestration are combined in a vertical farming environment. Trustworthiness in UC11 must be analysed not only from a cybersecurity perspective, but also with respect to the reliability, robustness, controllability, and transparency of the overall closed-loop control process. This is consistent with broader Industry 5.0 and AI Act requirements, which link trustworthiness to risk management, logging, transparency, human oversight, accuracy, robustness, and cybersecurity.

The main trustworthiness risk identified for UC11 is incorrect planning by the AI controller. In a continuously operating autonomous loop, such errors may lead to repeated inappropriate actions and can result in water and energy waste, crop yield reduction, and plant damage or loss. Risks emerge from multiple sources: (1) faulty or out-of-range sensor inputs; (2) inconsistent or outdated agronomic knowledge in the cloud knowledge base; (3) communication failures or latency between cloud and edge components; and (4) planning errors in the AI controller itself. Architecturally, UC11 addresses these risks through: (1) sensor validation and anomaly detection; (2) actuator command limits that restrict the physical impact of erroneous outputs; (3) fallback to rule-based control when AI-based decisions are deemed unreliable; and (4) human override capabilities allowing operators to intervene whenever necessary.

Human oversight remains essential. UC11 follows a model of autonomous operation with human takeover under exceptions. Operators monitor the system and may intervene whenever actuator behaviour appears inappropriate, with authority to stop or override activity and take manual control. This requires that operators can effectively detect abnormal behaviour, understand the source of control decisions, and exercise meaningful override authority. The MAPE-K architecture must therefore provide clear traceability from control actions back to sensor values, knowledge-base entries, and planning outcomes. This is particularly critical because the knowledge base is continuously updated whenever new farming guidelines become available. Trustworthiness thus depends not only on runtime control reliability, but also on the correctness and governance of cloud-based knowledge extraction and updates.

4.3.2.4 Standards and Regulatory Framework References

UC11 takes into account elements of multiple standardisation frameworks and regulatory requirements: (1) *EU Cyber Resilience Act (CRA)* – establishing secure-by-design principles, lifecycle vulnerability management, and attack surface minimisation; (2) *EU AI Act* – addressing risk management, transparency, human oversight, accuracy, and robustness of AI-enabled autonomous control; (3) *Industrial IoT and Edge Computing Standards* (IEC 61508, ISO 13849, ISO/IEC 27000 series) – ensuring functional safety, information security, and reliable operation of distributed systems; and (4) *Service-Oriented Architecture and Cloud Standards* (Eclipse Arrowhead, OpenStack, MQTT) – promoting interoperability, scalability, and secure service composition.

4.3.2.5 Standardisation Implications

UC11 provides a comprehensive testbed and reference implementation for the integration of emerging technologies (AI, IoT, autonomous systems, cloud-edge architectures, service-oriented design) within a regulated and complex operational domain. The architecture demonstrates how trustworthiness can be engineered through multiple complementary mechanisms:

- threat modelling and risk assessment (ThreatGet)
- secure-by-design principles aligned with the CRA
- microservice-based modularity enabling fault isolation and adaptive control
- MAPE-K feedback loops providing autonomous responsiveness
- human-centred oversight for exception handling and override.

From a standardisation perspective, UC11 highlights the need for integrated standards addressing the intersection of cybersecurity, functional safety, AI transparency and robustness, and human-machine interaction in autonomous systems. This overlaps and influences activities from project partners in AI Act and CRA related standardization development activities.

5. High-Level Evaluation and Synthesis

5.1 Outlook of WP3 Architecture Evaluation Results

As described in section 3.2 Eclipse Arrowhead already is based on a large set of well-established standards. For some certain areas it is expected that the Eclipse Arrowhead architecture will both make use of further standards and impact existing and new standards. The area identified are:

- Semantic interoperability and automation and scalability of information integration
- Automation of the engineering processes
- Orchestration along the Edge 2 Cloud Compute Continuum (E2CCC).

5.1.1 Semantic Interoperability and Automation and Scalability of Information Integration

This related to semantic interoperability exploiting the Industrial Data Ontology (IDO - ISO 23726-3) and its impact on knowledge graphs and modelling languages like SysML v2. The IDO does exist and proof of concept demonstrations end validations is in the works at multiple companies in the Paper & Pulp industry value network. This work is already impacting update work to the ISO 15926 standard made by companies like Stora Enso and Valmet.

A community building effort is launched as the Industrial Semantic Interoperability Summit June 9-11 in Oslo, https://www.dnv.com/events/industrial-semantic-interoperability-summit-2026-june/.

These activities are primarily supported by the Arrowhead fPVN project.

5.1.2 Automation of the Engineering Processes

Engineering processes for architecting and implementation of cyber-physical system architectures in industrial operations are currently affected by AI tools. Figure 2 provides a conceptual engineering process based on ISO 81346. Here are indicated areas where AI and formal tools already contribute to significant automation of engineering work.

Analysis of the change points in the direction of model-based system engineering (MBSE). In an MBSE system, designers and architects will be assisted by LLM tools. Downstream of this work a very high percentage of the code development and integration work will be automated. It is foreseen that such automation will continue to develop at a very fast pace for years to come.

AIMS5.0 WP3 contributes to MBSE tool technology and its standardisation through the Arrowhead DSL, which is subject to integration with the current SysML v2 standard. This is a cooperation with the Arrowhead fPVN project.

The AI assistants regarding capturing requirement and use case specification and transforming this into architecture proposal has been demonstrated within AIMS5.0, see the work by Hegedűs et.al. (Hegedűs, Tóth, Bancsics, & Varga, 2025).

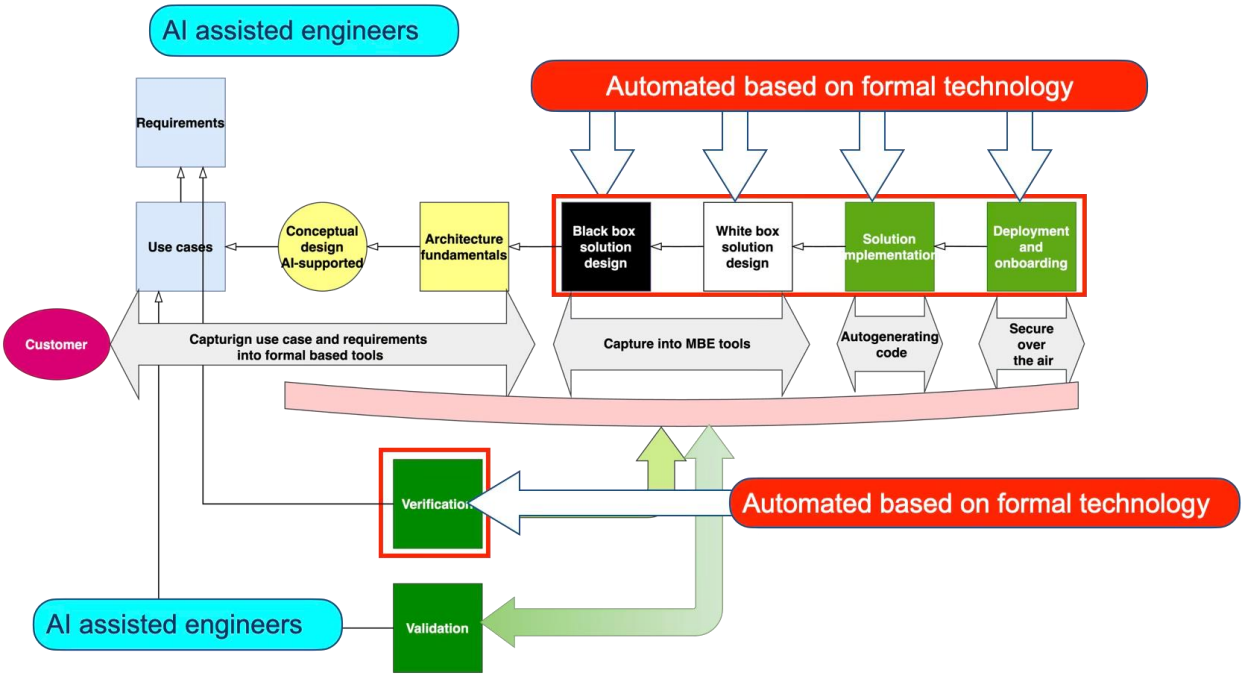

Figure 2 Conceptual engineering process for CPS automation systems, from early design to deployment, highlighting areas where AI and formal tools support engineering automation

5.1.3 Orchestration along the Edge 2 Cloud Compute Continuum

Along the E2CCC multiple types of orchestration will be needed. Examples thereof are:

- Service orchestration
- Compute orchestrations
- Deployment orchestration
- Network orchestration

The issues can be supported by the Arrowhead architecture through integration with related tools, e.g. ColonyOS.

A concrete integration between Eclipse Arrowhead and ColonyOS is undertaken in the COP-PILOT project: https://cop-pilot.eu. Such integration will support Service orchestration, Compute orchestration and Deployment orchestration. Open source tools for Network orchestration are, to our knowledge, not mature enough yet to enable a streamlined integration with Eclipse Arrowhead and ColonyOS to add network orchestration.

5.2 Cross-Reference with Regulatory and Standardisation Frameworks

The preceding sections of this chapter converge on two complementary perspectives on the AIMS5.0 architecture: functional requirements and interaction with relevant standards. Section 4.1 assesses the extent to which the Eclipse Arrowhead-based microservice architecture fulfils the functional requirements of the use cases, expressed across nine capability dimensions and summarised in Table 2. Sections 4.2and 4.3 examine how specific use case implementations interact with relevant standards, identifying where existing standards are validated in practice and where gaps in the standardisation landscape call for further action, as summarised in Table 3. Section 5.1 extends this view to three cross-cutting architectural challenges, semantic interoperability, automation of engineering processes, and orchestration along the Edge-to-Cloud Compute Continuum, for which the AIMS5.0 architecture is expected to influence future standards.

The present section brings these strands together by cross-referencing the architecture evaluation results with the regulatory and standardisation frameworks established in Chapters 2 and 3. The objective is twofold: first, to produce a structured compliance mapping that identifies where the WP3 architecture supports, partially supports, or does not yet address the essential requirements of the Cyber Resilience Act (CRA) and the EU Artificial Intelligence Act (AI Act); and second, to translate the residual gaps and standardisation observations into concrete guidelines for future architectural improvements and prioritised recommendations for engagement with European and international standardisation bodies.

The dual regulatory constraint created by the CRA and the AI Act, and the interactions between the two instruments, as analysed in Section 2.3. It is a structuring principle throughout. Where AI systems developed or deployed within AIMS5.0 use cases are embedded in products with digital elements, compliance must be cumulative across both instruments. The architecture guidelines and standardisation recommendations presented here are therefore formulated with awareness of this overlap, treating cybersecurity obligations derived from the CRA and those derived from Article 15 of the AI Act as jointly applicable rather than mutually exclusive.

5.2.1 Regulatory Compliance Mapping

Table 4 maps the requirement domains of the CRA and the AI Act to the corresponding components and mechanisms of the WP3 architecture. It identifies the residual gaps that emerge from the analysis in Chapter 4, and locates the source of each finding within this deliverable. The mapping is structured to follow the layered obligation structure of both instruments: CRA requirements address product cybersecurity properties (Annex I, Part I) and vulnerability handling processes (Annex I, Part II); AI Act requirements address the full high-risk compliance regime under Articles 9-15, which applies to the AI systems identified in Sections 4.2and 4.3as falling within high-risk scope, most notably the BCI-controlled exoskeleton system in UC08 and the AI-based access control and environmental control functions in UC11.

Table 4 Regulatory compliance mapping of the WP3 architecture to CRA and AI Act requirements

Requirement domain	*Regulatory instrument*	*Arrowhead WP3 architecture coverage*	*Residual gap*	*Source*
Cybersecurity-by-design: secure default configuration, encrypted communication, access control, attack surface minimisation	CRA Annex I, Part I (items 1–11)	X.509/TLS 1.3 and DTLS 1.3 for transport security; Arrowhead Authorization System for per-service access control; ESPAR adaptive antenna for physical-layer hardening	No machine-readable SBOM; no formally documented end-to-end threat model across the multi-tier deployment	§4.1.2.4 (R4), §4.2.3 (UC08), §4.3
Logging and monitoring of significant internal activities	CRA Annex I, Part I (item 12)	Arrowhead System Monitor; Event Handler records service invocations and state transitions	Logging is service-level; AI operation-specific audit records (model activations, decision outputs, anomaly detections) are not generated as a separate artefact	§4.1.2.2 (R2), §4.2.3 (UC08)
Vulnerability identification, SBOM, coordinated disclosure, security updates	CRA Annex I, Part II (items 1–8)	Arrowhead update deployment mechanisms in the AI-gym CI/CD pipeline; Model Manager supports versioning and rollback	No machine-readable SBOM in a standardised format (CycloneDX / SPDX); no coordinated vulnerability disclosure policy artefact linked to the deployed system	§4.1.2.4 (R4), §3.4
Risk manage-ment system	AI Act Art. 9	AI-gym metadata storage; Model Manager	No structured AI risk management system document; no automated	§4.1.2.2 (R2), §4.2.3 (UC08)

covering the full AI lifecycle		records training and deployment events	lifecycle risk tracking against identified risk scenarios	
Data governance and data quality measures	AI Act Art. 10	MLOps pipeline (Jenkins, Roboflow) manages training datasets; data collection pipeline from edge sensors is documented	Data lineage records are not maintained as formal artefacts; data quality assessments are not registered against the deployed model version	§4.1.2.2 (R2), §4.2.4 (UC09)
Technical documentation	AI Act Art. 11	Architecture documentation produced in D3.2; use case specifications in D5.1, D6.1	No integrated technical documentation artefact combining system architecture, risk management records, data governance, and performance metrics in the format required for conformity assessment	§4.2.3 (UC08), §4.3
Logging and record-keeping by the AI system	AI Act Art. 12	Arrowhead System Monitor and Event Handler provide service-level logs; AI-gym retains training metrics	AI-specific operational logs (inference inputs, outputs, confidence values, decision rationales) are not recorded as a conformity-relevant artefact tied to the deployed model	§4.1.2.2 (R2), §4.2.3 (UC08)
Transparency and provision of information to users and deployers	AI Act Art. 13	No dedicated transparency mechanism present in the core Arrowhead architecture	No user-facing transparency artefacts; no automated disclosure of AI system capabilities, limitations, or intended use conditions	§4.1.2.8 (R8)
Human oversight: ability to monitor, understand, and override AI outputs	AI Act Art. 14	Arrowhead Event Handler partially supports asynchronous notification of AI system state; local LLM deployment pattern supports operator-facing interaction	No dedicated human oversight service abstraction; no standardised override or interrupt interface defined at the Arrowhead service level	§4.1.2.8 (R8), §4.2.3 (UC08)
Accuracy, robustness, and cybersecurity of high-risk AI systems	AI Act Art. 15	AI-gym model evaluation covers accuracy metrics; IEC 62443-based security measures provide partial cybersecurity coverage; iSMT scheduler provides deterministic compute guarantees for UC08	No formal robustness assessment against adversarial inputs; no end-to-end threat model for AI-specific attack surfaces (adversarial perturbation, model poisoning)	§4.1.2.4 (R4), §4.2.3 (UC08), §4.3
Conformity assessment procedures prior to market placement	AI Act Arts. 16–29; CRA Arts. 24–32	Individual compliance contributions exist across architecture components	No integrated conformity assessment procedure combining CRA and AI Act obligations; CE marking preparedness is absent at system level	§2.3, §2.4

The mapping in Table 4 reveals a consistent pattern: the WP3 architecture provides strong coverage for infrastructure-level security requirements (transport encryption, access control, service composition) and substantially addresses operational requirements (multi-tier deployment, AI model lifecycle management, real-time determinism). The principal deficits are concentrated in four areas that cross both regulatory instruments: (1) formal documentation artefacts required for conformity assessment; (2) AI-specific logging aligned with Art. 12 obligations; (3) human oversight service abstractions required by Art. 14; and (4) SBOM and vulnerability handling governance required by CRA Annex I Part II. Each of these areas is addressed by the guidelines in Section 5.2.2 and the standardisation recommendations in Section 5.2.3.

5.2.2 Guidelines for Future Architectural Improvements

The following eight guidelines are derived directly from the residual gaps in Table 2 and the regulatory mapping in Table 4. Each guideline identifies the specific architectural mechanism to be introduced or extended, the requirement driver at the regulatory and standards levels, and the use-case evidence that motivates the intervention. The guidelines are ordered from highest regulatory urgency, those required for immediate CRA and AI Act compliance, to those that address forward-looking interoperability and sustainability ambitions.

5.2.2.1 Guideline 1 - Data Lineage and Model Audit Trail (R2, AI Act Arts. 10 and 12)

Motivation. The AI-gym MLOps pipeline manages model training, versioning, and deployment, but does not generate formally structured records of training data provenance, data quality assessments, or inference-time operational logs. Both AI Act Art. 10 (data governance) and AI Act Art. 12 (logging and record-keeping) require that these records exist as verifiable artefacts for high-risk AI systems. The gap is directly identified in Table 2 (R2: "model audit trail; data lineage for regulated environments") and affects UC15 (ML models in production), UC12 sub-project 1 (SHAP-based XAI), and UC16 (RF production), all of which involve AI systems embedded in regulated manufacturing processes.

Guideline. A model provenance service should be introduced as a dedicated component of the AI-gym, recording for each deployed model: (a) training dataset identifiers, versions, and quality assessment outcomes; (b) validation metrics at the point of deployment; (c) deployment event log including the authorising service invocation captured by the Arrowhead Authorization System; and (d) inference-time operational records including prediction outputs, confidence values, and any anomaly flags. The artefact format should be compatible with ISO/IEC 42005:2025 (AI system impact assessment), which defines a structured framework for documenting AI system risks and impacts, and aligned with the logging and record-keeping structure anticipated in prEN 18229-1 under development by CEN-CENELEC JTC 21. The model provenance service should be registered in the Arrowhead Service Registry as a standard system service, enabling automated querying of compliance artefacts for any deployed model instance.

5.2.2.2 Guideline 2 - Human Oversight Service Interface (R8, AI Act Art. 14)

Motivation. AI Act Article 14 requires that high-risk AI systems be designed to enable human oversight effectively, including the ability for designated individuals to monitor the AI system's operation, understand its outputs, and intervene or override the system where necessary. The Arrowhead Event Handler provides asynchronous notification of system state changes, and the local LLM deployment pattern (llama.cpp / LLaVA) supports natural-language interaction with AI system outputs. However, no standardised service abstraction for the oversight functions — monitor, pause, override, and audit — exists at the Arrowhead architectural level. This gap is directly identified in Table 2 (R8: "operator-facing interface components") and is most acutely relevant to UC08 (BCI exoskeleton, AMR task assignment) and UC11 (AI-based environmental control in indoor farming).

Guideline. A dedicated human oversight service abstraction should be defined as a standard Arrowhead service type, providing the following operations: (a) *observe*: expose AI system operational state, latest inference inputs and outputs, and confidence metrics in a machine-readable format consumable by operator dashboard components; (b) *suspend*: send a verified interrupt request that halts AI-driven actuation and transfers control to a defined safe state; (c) *override*: submit a validated human-authorised value to replace an AI system output for one or more decision cycles; and (d) *audit*: retrieve the AI system's operational log for a specified time window. The interface semantics should be aligned with the requirements being developed under prEN 18229-1 (AI trustworthiness framework — logging, transparency, and human

oversight) in CEN-CENELEC JTC 21 WG1 and WG2, and should be compatible with the ISO/IEC DIS 42105 guidance on human oversight of AI systems, which is currently under development in ISO/IEC JTC1 SC42 WG3. The oversight service should require authenticated invocation via the Arrowhead Authorization System, ensuring that override actions are traceable to authorised personnel.

5.2.2.3 Guideline 3 - SBOM Generation and Vulnerability Disclosure (CRA Annex I, Part II)

Motivation. CRA Annex I Part II requires manufacturers to identify and document all components included in a product, including through a software bill of materials (SBOM) in a commonly used, machine-readable format, and to establish a coordinated vulnerability disclosure (CVD) policy. The WP3 architecture currently provides no mechanism for generating SBOMs of deployed Arrowhead service configurations, nor for exposing a CVD channel linked to the deployed system. This is a direct compliance gap for any AIMS5.0 use case where Arrowhead-based system components are commercialised or made available on the EU market.

Guideline. The Arrowhead System Manager should be extended to auto-generate a machine-readable SBOM covering the service components registered in each Arrowhead Local Cloud, including software versions, dependency graphs, and the X.509 certificate identities of active service providers. The SBOM should be generated in CycloneDX or SPDX format as required by the CRA, and should be refreshed automatically on each service registration or update event captured by the Service Registry. A CVD notification service should be added as a standard Arrowhead system service, providing a structured channel through which vulnerability reports can be submitted and acknowledged, consistent with CRA Art. 14. The update distribution mechanisms already present in the AI-gym CI/CD pipeline (Jenkins, Model Manager) should be formally documented as the software update pathway in the SBOM artefact, satisfying the CRA's requirement for secure and timely update mechanisms.

5.2.2.4 Guideline 4 - End-to-End Threat Model and Attack Surface Documentation (R4, CRA Annex I Part I, AI Act Art. 15)

Motivation. Table 2identifies the absence of a documented end-to-end threat model as the primary residual gap in the security (R4) dimension, with the note that it is being partially addressed through the UC11 security analysis in Section 4.3. The CRA requires that products with digital elements be designed to minimise attack surfaces, and the AI Act requires high-risk AI systems to maintain appropriate cybersecurity (Art. 15). Both obligations require a formal threat analysis as the technical basis for security design decisions. Section 4.2.3 (UC08) further identifies that AI-specific attack surfaces — adversarial input perturbation, model poisoning through the CI/CD pipeline — are not yet addressed in the existing security analysis.

Guideline. A structured threat modelling exercise should be conducted across the full multi-tier Arrowhead deployment, covering the edge (SmartBox, sensor endpoints), fog (Dell PowerEdge cluster, AI-gym), cloud (inter-cloud cluster, Model Manager), and all inter-tier communication paths (Gatekeeper/Gateway, AI model update channels, SBOM distribution). The threat model should follow the STRIDE methodology and should incorporate TARA (Threat Analysis and Risk Assessment) in alignment with IEC 62443-3-3 (System security requirements and security levels), mapping identified threats to security levels SL1–SL3 across the different deployment zones. AI-specific threats — adversarial perturbation, data poisoning, model exfiltration — should be addressed explicitly in a dedicated sub-section, drawing on the ETSI TR 104 128 (Guide to Cyber Security for AI Models and Systems) published in May 2025 and the ETSI TS 104 224 (Explicability and transparency of AI processing). The threat model output should be registered as a security documentation artefact in the Arrowhead System Manager and referenced in the CRA and AI Act technical documentation.

5.2.2.5 Guideline 5 - Formal SLA and Latency Specification for Inter-Tier Communication (R3, R5, IEEE 802.1 TSN)

Motivation. Table 2 identifies two related residual gaps: the absence of a formal service-level agreement (SLA) mechanism for tier-to-tier latency bounds (R3) and the absence of formal end-to-end latency specifications for control-critical loops (R5). These gaps are relevant to UC05 (multi-tier AI-gym deployment), UC08 (BCI exoskeleton response time, AMR deadlock avoidance), UC09 (real-time sensor data interruption requirements), and UC13 (edge AI on OHT shuttles). The iSMT hierarchical scheduler and the TTTech TSN integration demonstrate that deterministic compute and communication are achievable in practice, but the performance guarantees are not currently expressed as architectural artefacts that other services can query or contractually depend upon.

Guideline. IEEE 802.1Qcc (Stream Reservation Protocol enhancements) should be adopted as the formal mechanism for declaring and verifying latency bounds on TSN-backed communication paths within and between Arrowhead Local Clouds. A new Arrowhead service metadata field — "latency contract" — should be defined, binding a service registration entry to the TSN stream parameters (maximum end-to-end latency, jitter budget, reservation bandwidth) that the underlying network guarantees for that service's communication path. The Arrowhead Orchestrator should be extended to consult latency contract metadata during service composition, rejecting compositions that would violate the declared latency bounds of participating services. This mechanism directly operationalises the formal SLA concept at the SOA level, enabling verification of real-time guarantees without requiring application developers to directly manage TSN schedule parameters.

5.2.2.6 Guideline 6 - Semantic Interoperability Layer for Ontology Lifecycle Management (R7, ISO/IEC 21823-3)

Motivation. Section 4.2.1 (UC02) identifies that the binding between the Digital Reference Ontology (DRO) and Industrial Data Ontology (IDO, ISO 23726-3 — work in progress) lifecycle management and the Arrowhead Service Registry is not formally specified, meaning that ontology updates are not automatically reflected in service descriptions. Table 2 identifies the R7 residual gaps as "ontology federation" and "runtime knowledge graph integration." Section 5.1.1 further emphasises that semantic interoperability is expected to have lasting standards impact through the IDO-based work with partners in the paper and pulp industry, and through the Industrial Semantic Interoperability Summit (Oslo, June 2026).

Guideline. A formal synchronisation protocol should be defined between the DRO/IDO ontology registry and the Arrowhead Service Registry, operating as follows: (a) when an ontology version is published or updated in the ontology registry, a notification event is raised and consumed by a dedicated Arrowhead "ontology sync" system service; (b) the sync service updates the semantic annotations of all registered services whose service definitions reference the affected ontology version; (c) services that depend on a deprecated ontology element are flagged with a "requires update" status in the Service Registry, triggering re-registration by the affected service providers. This mechanism closes the gap identified in UC02 and provides the architectural basis for the formal SOA-level governance of shared industrial ontologies that Section 4.2.1 identifies as a standardisation contribution opportunity for ISO/IEC 21823-3 (IoT Interoperability — Semantic Interoperability). The implementation should be developed in coordination with the Arrowhead fVPN project, which leads the IDO standardisation work.

5.2.2.7 Guideline 7 - AI Act Conformity Documentation Auto-Generation (AI Act Art. 11)

Motivation. AI Act Article 11 requires providers of high-risk AI systems to draw up and maintain technical documentation covering the general description of the AI system, the design specifications, the development process, the risk management records, the data governance

measures, the performance metrics, and the human oversight provisions. Producing and maintaining this documentation manually for the range of AI systems deployed across AIMS5.0 use cases (AI-gym, MLOps pipeline, BCI exoskeleton, XAI interfaces) is operationally unsustainable. Table 4 identifies the absence of an integrated technical documentation artefact as a direct conformity gap across all high-risk AI use cases.

Guideline. The AI-gym, System Monitor, and model provenance service (Guideline 1) should be extended to auto-generate AI Act Art. 11 technical documentation artefacts as a standard output of the model deployment workflow. Specifically, the deployment pipeline should produce: (a) a structured system description drawing on the Arrowhead Service Registry metadata for the services comprising the AI system; (b) a risk management record populated from the AI-gym's training and validation logs; (c) a data governance summary generated by the model provenance service from dataset identifiers and quality assessment records; (d) a performance and accuracy report exported from the AI-gym evaluation results; and (e) a human oversight record generated from the oversight service interface (Guideline 2) configuration. These artefacts should be generated in a machine-readable format aligned with the requirements being developed in prEN 18285 (AI conformity assessment framework) and prEN 18286 (Quality management system for EU AI Act regulatory purposes) under CEN-CENELEC JTC 21.

5.2.2.8 Guideline 8 - ISO 50001 Energy KPI Service Type (R9, ISO 50001:2018)

Motivation. Section 4.2.4 (UC09) identifies that the integration between ISO 50001 energy performance indicators (EnPIs) and AI-driven scheduling optimisation is not formalised at the architectural level: ISO 50001 compliance is achieved at the monitoring and reporting layer, but the Plan-Do-Check-Act cycle is not expressed as an architectural pattern that AI model deployments can formally participate in. Table 2 identifies the R9 residual gap as "domain-specific scheduling optimisation," but the deeper issue is the absence of a standard interface between energy management objectives and AI service metadata.

Guideline. A standard ISO 50001 energy KPI service type should be defined within the Arrowhead service metadata schema, enabling AI-gym–deployed energy optimisation models to register their objectives and performance indicators against ISO 50001-defined EnPIs. The service type should declare: (a) the set of EnPIs the service contributes to; (b) the current EnPI values as measured by the service; and (c) the AI model optimisation target expressed in EnPI-relative terms. The Arrowhead Orchestrator should be extended to support EnPI-aware service composition, enabling energy-optimised production workflows to be assembled dynamically from services that expose matching EnPI targets. This architectural pattern operationalises the "golden tool" strategy demonstrated in UC01 and UC09 and provides a reusable reference implementation for AI-based energy optimisation in ISO 50001-governed industrial environments.

5.2.3 Standardisation Recommendations

The guidelines in Section 5.2.2 identify concrete architectural mechanisms required to close the compliance and interoperability gaps in the WP3 architecture. Each of these mechanisms also constitutes a potential contribution to or engagement point with active standardisation work. This section organises the resulting standardisation recommendations by standards body, following the landscape established in Chapter 3. These recommendations complement and feed into the standardisation activities reported in D8.3 (final standardisation report, WP8),they do not replace it, but provide the architecture-grounded technical input that strengthens the project's standardisation contributions.

5.2.3.1 CEN-CENELEC JTC 21 (AI Act Harmonised Standards)

The AI Act Commission Implementing Decision of 23 June 2025 requests CEN-CENELEC to develop harmonised standards for the ten technical areas identified in Chapter 2, Section 2.4.1. The AIMS5.0 WP3 architecture provides concrete reference material for several of these areas:

- *prEN 18229-1 (AI trustworthiness — logging, transparency, human oversight)*. The human oversight service interface defined in Guideline 2 and the model audit trail defined in Guideline 1 constitute a reference architecture for the operational mechanisms required by this standard. The Arrowhead Event Handler and System Monitor, as instantiated in UC08 and UC11, should be submitted as worked examples to CEN-CENELEC JTC 21 WG2 (Operational Aspects).
- *prEN 18229-2 (AI trustworthiness — accuracy and robustness)*. The AI-gym model evaluation pipeline, validated across UC01, UC05, UC06, and UC15, provides a worked example of accuracy and robustness measurement at edge-to-cloud scale. The threat model output required by Guideline 4 should be contributed to JTC 21 WG5 (Cybersecurity for AI Systems) as industrial AI cybersecurity evidence, particularly for adversarial robustness requirements.
- *prEN 18284 (dataset governance) and prEN 18286 (QMS for EU AI Act)*. The model provenance service defined in Guideline 1 and the conformity documentation auto-generation pipeline in Guideline 7 provide practical implementations of dataset governance and quality management requirements. These should be contributed to JTC 21 WG3 (Engineering Aspects).
- *prEN 18285 (AI conformity assessment framework)*. The integrated technical documentation artefacts generated by Guideline 7 represent a candidate reference implementation for the conformity assessment procedures being developed in JTC 21.

5.2.3.2 IEC TC65 / IEC 62443 (Industrial Cybersecurity and CRA M/606)

The M/606 CRA work programme (April 2025) identifies IEC 62443-based security profiles as the primary vehicle for CRA harmonised standards in industrial and OT contexts. The WP3 architecture provides direct input to this work:

- *Extension of IEC 62443-4-1 for AI model lifecycle operations.* Section 4.2.2 (UC05) identifies that the AI-gym CI/CD pipeline — encompassing model training, validation, deployment, and rollback — constitutes a software update and deployment pathway that should be formally assessed against IEC 62443-4-1 (Secure product development requirements). The observed gap — that IEC 62443-4-1 does not currently address AI model lifecycle operations as first-class software update categories — should be submitted as a formal gap report to IEC TC65 WG10, with the UC05 implementation serving as the motivating use case.
- *IEC TC65 WG23 (Smart Manufacturing) and WG31 (Industrial Agents / Agentic AI)*. The UC02 protocol interoperability findings (Kafka-to-SOA bridging, DRO/OAP integration) are directly relevant to IEC TR 63283-3 (Smart Manufacturing — Cybersecurity challenges) and the emerging IEC 63718 (Agentic AI in industrial automation). The Arrowhead AI-gym and Orchestrator architecture constitutes a reference implementation for the multi-agent AI orchestration concepts being standardised in WG31.

5.2.3.3 IEC TC65 / IEC 62541 (OPC UA)

Section 4.2.2 (UC05) identifies that a normative OPC UA–to–Arrowhead service registry binding profile would eliminate the need for bespoke adapter implementations across deployments and would strengthen the standardisation contribution of the Arrowhead Tools ecosystem:

- *Normative OPC UA–to–Arrowhead interface profile*. The SmartBox OPC UA adapter implementation in UC05 should be submitted as input to the IEC TC65 SC65E working group responsible for OPC UA companion specifications, proposing a normative binding

between IEC 62541 OPC UA server endpoints and Arrowhead Service Registry entries. The profile should specify how OPC UA node identifiers map to Arrowhead service definitions, how OPC UA security channels align with Arrowhead X.509 certificate profiles, and how OPC UA subscriptions map to Arrowhead Event Handler notifications.
- *OPC UA AI model metadata information model*. An extension of OPC UA information models to expose AI model metadata (type, version, training dataset identifier, performance KPIs) as OPC UA nodes would enable Arrowhead-registered AI services to integrate with existing OPC UA clients without additional adaptation. This is motivated by the AI-gym-to-UC05 data flow and supports the ISO 50001 energy KPI service type in Guideline 8.

5.2.3.4 ISO/IEC JTC1 SC42 (AI Standards)

Chapter 3 provides a comprehensive mapping of the ISO/IEC JTC1 SC42 standards landscape. The WP3 architecture results are relevant contributions to several active work items:
- *ISO/IEC DIS 42105 (Guidance for human oversight of AI systems)*. The human oversight service interface in Guideline 2 provides a service-oriented architectural realisation of human oversight concepts. The AIMS5.0 implementation — instantiated in UC08 and UC11 — should be contributed to ISO/IEC JTC1 SC42 WG3 as a worked example of human oversight architecture in industrial AI deployment contexts.
- *IEC SC65A WG24 Human-machine collaboration- Standard IEC 63662 - Human-machine collaborations Part 1: Coordination of multiple risk assessments*. This standard under development complements the ISO/IEC JTC1 SC42 AI-standards (see section 3 and this section 5.2.3) on human oversight, on functional safety of AI systems (SC42 WG03) and on human-machine teaming (SC42 WG04) from the industrial viewpoint. AIMS5.0 implementations will contribute to various aspects as mentioned above.
- *ISO/IEC 42005:2025 (AI system impact assessment)*. The model provenance service in Guideline 1 and the conformity documentation pipeline in Guideline 7 implement a subset of the ISO/IEC 42005 impact assessment framework. The alignment between these architectural artefacts and the ISO/IEC 42005 structure should be documented and submitted as feedback to SC42 to validate the standard's applicability to service-oriented industrial AI deployments.
- *ISO/IEC AWI TS 22440 series (Functional safety and AI systems)*. The safety-critical AI deployments in UC08 (BCI-controlled exoskeleton, AI-based AMR coordination) and UC11 (AI-based environmental control) represent high-relevance application scenarios for the emerging ISO/IEC AWI TS 22440-1/-2/-3 series, which replaces ISO/IEC TR 5469:2024. The UC08 architectural analysis in Section 4.2.3 and the UC11 trustworthiness analysis in Section 4.3 should be contributed to the SC42 WG3 working group as input to the requirements (Part 1) and guidance (Part 2) documents.
- A further assessment on AI-standards in relationship to use cases is documented in D 8.3, and for the human-related and ethics aspects in D7.3.

5.2.3.5 OMG SysML v2 (Model-Based Systems Engineering)

Section 5.1.2 identifies model-based systems engineering as a high-impact area for the WP3 architecture, and Section 3.1 records the Arrowhead DSL / SysML v2 library presentation at the OMG Technology Meeting (Reston, VA, March 2026):
- *Arrowhead DSL as a contributed SysML v2 profile*. The Arrowhead DSL and core system library, presented at the March 2026 OMG meeting and built on the SysML v2 examples distributed with the SysML v2 drafts and first release, should be formalised as a contributed profile to the OMG SysML v2 standard. The UC05 OPC UA bridge pattern and the UC08 TTMS service cluster architecture should be prioritised as primary modelling examples, providing reusable reference models for industrial system-of-systems

architecture documentation and strengthening the contribution to the OMG standardisation process.

5.2.3.6 ISO TC 199 (Safety of Machinery) and ISO TC 299 (Robotics)

The UC08 use case, integrating a BCI-controlled upper-body exoskeleton with AMR coordination, creates a direct engagement point with two converging standardisation domains:

- *ISO TR 22100-5 (AI implications for machinery safety).* The UC08 architecture provides a documented example of AI-based actuation control for a wearable exoskeleton in a professional industrial environment, directly relevant to the scope of ISO TR 22100-5. The architecture's partial fulfilment of AI Act Art. 14 human oversight requirements — as identified in Table 4, should be submitted as evidence of current industry implementation challenges requiring standardisation guidance.
- *ISO AWI 25785-1 (Safety requirements for industrial mobile robots — legged, wheeled, or other forms of locomotion) and ISO/FDIS 21423 (Autonomous mobile robots — Communications and interoperability).* The UC08 AMR coordination architecture (TTMS microservice cluster, ESPAR wireless communication, TSN real-time backbone) constitutes a reference implementation for the communication and interoperability requirements being standardised in ISO TC 299. The iSMT hierarchical scheduler's demonstrated performance advantage over EDF scheduling provides quantitative evidence that could inform real-time scheduling requirements in ISO AWI 25785-1.

5.2.3.7 ISO 50001 (Energy Management Systems)

Section 4.2.4 (UC09) identifies that the integration between ISO 50001 energy performance indicators and AI-driven batch scheduling constitutes a novel application pattern not yet addressed by either standard:

- *Standardised interface between ISO 50001 EnPIs and AI model service metadata.* The ISO 50001 energy KPI service type defined in Guideline 8 should be proposed as the basis for a standardised interface, potentially formalised as an OPC UA companion specification. This contribution would accelerate the adoption of AI-based energy optimisation in ISO 50001-governed industrial environments and is consistent with the sustainability and Industry 5.0 objectives that are central to the AIMS5.0 project mandate.

6. Conclusions

Deliverable D3.3 has presented the outcomes of the regulatory analysis, standardisation mapping, and architectural evaluation activities conducted within WP3 of the AIMS5.0 project. The regulatory analysis has shown that the Cyber Resilience Act and the EU AI Act are both highly relevant for AI-enabled industrial systems and that they interact in areas such as product safety, cybersecurity, risk management, conformity assessment, and post-market monitoring. The report further shows that these regulatory developments are accompanied by active standardisation work, including activities under CEN/CENELEC JTC 21 and the CRA-related standardisation programme.

The standardisation mapping has shown that the Eclipse Arrowhead architecture is grounded in a broad set of established international standards and is expected to make use of further standards and influence existing and new standards in areas such as semantic interoperability, model-based systems engineering, edge-to-cloud orchestration, and industrial cybersecurity. Active engagement with CEN/CENELEC, ISO/IEC JTC1 SC42, IEC TC65, ETSI, and OMG is identified in the document as an important route for consolidating AIMS5.0 WP3 results into standardisation contributions.

The architectural analysis has examined the extent to which the WP3 microservice architecture fulfils use case requirements across nine capability dimensions and has led to a set of architectural guidelines and standardisation recommendations linked to relevant standards bodies, including CEN/CENELEC JTC 21 (AI for the AI-Act), IEC TC65 (Industrial Measurement, control and automation), IEC SC65A (System aspects of IEC TC65), ISO TC 184 (Automation systems and integration), ISO TC 199 (Safety of machinery), ISO TC299 (Robotics), ISO/IEC JTC1 SC42 (AI), and OMG SysML v2. These results provide architecture-grounded technical input that complements the standardisation engagement reported in D8.3. This deliverable has also shown close collaboration with WP7 (Acceptance, trust and ethics for industrial AI) regarding human-related and ethical aspects. Finally, the deliverable recognises that standardisation is a medium- to long-term process extending beyond the duration of AIMS5.0. The continued involvement of key partners in related Horizon Europe and Chips-JU projects provides a basis for sustaining these activities beyond the project lifetime.

7. References

4diac. (2018). *How to Use Eclipse 4diac's Arrowhead Library*. Retrieved from Eclipse: https://eclipse.dev/4diac/doc/communication/arrowhead.html

Abdelkader Magdy Shaaban, C. S. (2025). A ThreatGet-Based Framework for Aligning System Security with the Cyber Resilience Act. *International Conference on Computer Safety, Reliability, and Security*. Retrieved from https://link.springer.com/chapter/10.1007/978-3-032-02018-5_8

Ádám Kővári, Y. G. (2025). Let's Have a Chat with the EU AI Act. *NOMS 2025-2025 IEEE Network Operations and Management Symposium*. Retrieved from https://ieeexplore.ieee.org/document/11073655/authors#authors

AIMS5.0 Consortium (D1.3). (2025). *D1.3 – Test and validation of edge platform components and environment (V1.1)*. Retrieved from AIMS5.0: https://www.aims50.eu/index.php/publications/public-deliverables

AIMS5.0 Consortium (D3.4). (2024). *D3.4 – Preliminary micro service requirements and first architecture concepts – SEN part (V1.3)*. Retrieved from AIMS5.0.

AIMS5.0 Consortium (D4.6). (2025). *D4.6 – Report on Procedures to Integrate Data into the Open Access Platform and Allow Accessing the Data via the Open Access Platform (V1.1)*. Retrieved from AIMS5.0.

AIMS5.0 Consortium (D5.1). (2024). *D5.1 – Definition of the Innovation Project and planning (V1.0)*. Retrieved from AIMS5.0.

AIMS5.0 Consortium (D6.1). (2023). *D6.1 – Detailed report about Tier 2 use case requirements and specifications for Y1 for sustainability, productivity, resilience and human centricity (V0.13)*. Retrieved from AIMS5.0.

Arrowhead. (2022). *Eclipse Arrowhead Ecosystem*. Retrieved from Arrowhead: https://arrowhead.eu/wp-content/uploads/2022/06/aht-invitation-final.pdf

Belal Abu Naim, Y. G. (2024). A Self-assessment Tool to Encourage the Uptake of Artificial Intelligence in Digital Workspaces. *NOMS 2024-2024 IEEE Network Operations and Management Symposium*. Retrieved from https://ieeexplore.ieee.org/document/10575125/authors#authors

CBI. (2026, Feburary). *The European market potential for cybersecurity products and services*. Retrieved from CBI: https://www.cbi.eu/market-information/outsourcing-itobpo/cybersecurity/market-potential

CEN CENELEC. (2026). *Working Groups & Projects | CEN-CENELEC JTC 21*. Retrieved from JTC21 AI CEN-CENELEC: https://jtc21.eu/working-groups/

CEN, CENELEC and ETSI Work Programme . (2025, April). *M/604- Cyber Resilience Act*. Retrieved from https://cyberstand.eu/sites/default/files/2025-04/WorkProgramme_CENCLCETSI.pdf

CEN-CENELEC. (2025). *Analysis of the CRA W*. Retrieved from https://www.stan4cra.eu/_files/ugd/d3d362_f5e6daa7f2fc4850b076310c59a305c1.pdf

Commission, E. (2025, June). *ANNEXES to the Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards high-risk AI systems in support of Regulation (EU) 2024/1*. Retrieved from https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)3871&lang=en

Commission, European. (2020). *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*. Retrieved from Assessment List for Trustworthy Artificial Intelligence (ALTAI) for Self-Assessment: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

Commission, European. (2025, May). *COMMISSION IMPLEMENTING DECISION of 23.6.2025 on a standardisation request to the European Committee for Standardisation and*

theEuropean Committee for Electrotechnical Standardisation as regards high-risk AI systems in support of Regulation (EU) 2024/1689. Retrieved from https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)3871&lang=en

ComplianceHub. (2025, October). *EU Cyber Resilience Act Implementation Guide: Building Secure Products for Europe's Digital Future*. Retrieved from ComplianceHub: https://compliancehub.wiki/eu-cyber-resilience-act-implementation-guide-building-secure-products-for-europes-digital-future/

Consortium, AIMS5.0 (D3.1). (2024). *D3.1 - Preliminary micro service requirements and first architecture concepts (V1.3)*. Retrieved from AIMS5.0: https://www.aims50.eu/index.php/publications/public-deliverables

Consortium, AIMS5.0 (D3.2). (2025). *D3.2 – Final micro service architecture requirements and architecture realization (V1.0)*. Retrieved from AIMS5.0: https://www.aims50.eu/index.php/publications/public-deliverables

Delsing, J. (2021). *SysML 1.6 profile and library*. Retrieved from Arrowhead: https://arrowhead.eu/core_systems/sysml-2-profile/

E. Rescorla. (2018, August). *RFC 8446 The Transport Layer Security (TLS) Protocol*. Retrieved from RF-Editor: https://www.rfc-editor.org/info/rfc8446

E. Rescorla, H. Tschofenig, and N. Modadugu. (2022, April). *RFC 9147 The Datagram Transport Layer Security (DTLS) Protocol*. Retrieved from RFC-Editor: https://www.rfc-editor.org/info/rfc9147

ENISA. (2024). *ENISA THREAT LANDSCAPE 2024*. Retrieved from https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

European Commission (EC) - AI Act. (2024). *laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (AI Act)*.

European Commission (EC) - CRA Act. (2024). *Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*. Official Journal of the European Union.

European Commission. (2024). *Artificial Intelligence Act*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

Foundation, E. (2021). *Eclipse Foundation*. Retrieved from Eclipse Arrowhead 4.4.0 release notes: https://projects.eclipse.org/projects/iot.arrowhead/releases/4.4.0

github. (2021). *ISO/IEC/IEEE 42010 conformance*. Retrieved from github: https://github.com/eclipse-arrowhead/documentation/issues/1

Hegedűs, C., Tóth, Á., Bancsics, M., & Varga, P. (2025). Multi-Agentic Plan-and-Solve Engine for Managing System of Systems via Natural Language. *IEEE Symposium on Network Operations and Management*. doi:https://ieeexplore.ieee.org/document/11073647

Hogan Lovells. (2024, November). *The EU Cyber Resilience Act: Implications for Companies*. Retrieved from Hogan Lovells: https://www.hoganlovells.com/en/publications/the-eu-cyber-resilience-act-implications-for-companies-

IEC. (2015). *IEC 62559-2: Use case methodology - Part 2: Definition of the templates for use cases, actor list and requirements list*. https://webstore.iec.ch/en/publication/22349.

IEC. (2016). *IECEE Test Report Form 60730-2-9I*. Retrieved from https://webstore.iec.ch/en/publication/24158

IEc. (2019). *IEC 62443-4-2: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*. https://webstore.iec.ch/en/publication/34421: IEC.

IEC. (2025). *OPC unified architecture - Part 1: Overview and concepts* . https://webstore.iec.ch/en/publication/81513: IEC.

ISO. (2018). *ISO 15926-13:2018 - Industrial automation systems and integration — Integration of life-cycle data for process plants including oil and gas production facilities - Part 13:*

Integrated asset planning life-cycle. Retrieved from https://www.iso.org/standard/70694.html

ISO. (2019). *ISO 8601-1:2019 Date and time — Representations for information interchange Part 1: Basic rules*. Retrieved from ISO: https://www.iso.org/standard/70907.html

ISO. (2022). *IEC 81346-1:2022 - Industrial systems, installations and equipment and industrial products — Structuring principles and reference designations - Part 1: Basic rules*. Retrieved from https://www.iso.org/standard/82229.html

ISO. (2022). *ISO/IEC/IEEE 42010:2022 - Software, systems and enterprise — Architecture description*. Retrieved from https://www.iso.org/standard/74393.html

ISO. (2024). *ISO 10303-1:2024: Industrial automation systems and integration — Product data representation and exchange*. https://www.iso.org/standard/83105.html: ISO.

ISO/IEC. (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO/IEC. Retrieved from https://www.iso.org/standard/27001

ITU-T. (2019). *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

Jerker Delsing. (2022). *Arrowhead Tools*. Retrieved from https://tools.arrowhead.eu/wp-content/uploads/sites/2/2022/06/Arrowhead-Tools-Author-Jerker-Delsing.pdf

Mockapetris, P. (1987). *STD 13 - RFC 1035*. Retrieved from RFC Editor: https://www.rfc-editor.org/info/rfc1035

OASIS. (2019, March). *MQTT Version 5.0: OASIS Standard*. Retrieved from Docs-OASIS: https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

Organization, O. S. (2019, December). *SysML® — OMG Systems Modeling Language*. Retrieved from OMG: https://www.omg.org/spec/SysML/1.6

Pillsbury. (2025, December). *The EU's Cyber Resilience Act: New Cybersecurity Requirements for Connected Products and Software*. Retrieved from Pillsbury: https://www.pillsburylaw.com/en/news-and-insights/eu-cyber-resilience-act-requirements-products-software.html

Smith, A. L. (2026). *EU AI Act Harmonised Standards Mapping*. Retrieved from AI-Act-Standards: https://web.archive.org/web/20260000000000*/https://ai-act-standards.com/

Tools, A. (2020). *Deliverable D10.2 Standardisation report year 1*. https://tools.arrowhead.eu/wp-content/uploads/sites/2/2022/06/Deliverable-D10.2-Standardisation-report-year-1.pdf.

x509-profiles. (2021). Retrieved from github: https://github.com/arrowhead-f/x509-profiles

Yasin Ghafourian, M. T. (2024, October). Engineering Secure, Trustworthy, and Ethically Sound AI-Based Computer Systems. *ERCIM News*. Retrieved from https://ercim-news.ercim.eu/en139/r-i/engineering-secure-trustworthy-and-ethically-sound-ai-based-computer-systems

Z. Shelby, K. H. (2014, June). *RFC 7252 - The Constrained Application Protocol (CoAP)*. Retrieved from RFC-Editor: https://www.rfc-editor.org/info/rfc7252

8. Appendices

8.1 Appendix A – Abbreviations

Abbreviation	Meaning
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMR	Autonomous Mobile Robot
ARROWHEAD	Arrowhead Framework for IoT and Industrial Automation
ASIC	Application-Specific Integrated Circuit
AWI	Approved Work Item
AW CD	Approved Work Committee Draft
CD	Committee Draft
CE	Conformité Européenne (European Conformity)
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
Chips-JU	Chips Joint Undertaking (EU Semiconductor Programme)
CISC	Complex Instruction Set Computing
CoAP	Constrained Application Protocol
CRA	Cyber Resilience Act
CD TS	Committee Draft Technical Specification
DIS	Draft International Standard
DRO	Digital Reference Ontology
EC	European Commission
EEA	European Economic Area
ESPAR	Electronically Steerable Parasitic Array Radiator
ETSI	European Telecommunications Standards Institute
FOUP	Front-Opening Unified Pod
FPGA	Field-Programmable Gate Array
HTTP	HyperText Transfer Protocol
IEC	International Electrotechnical Commission
IDO	Industrial Data Ontology
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
JTC	Joint Technical Committee
JWG	Joint Working Group
ML	Machine Learning
MLOps	Machine Learning Operations
MQTT	Message Queuing Telemetry Transport
NFC	Near Field Communication
OASIS	Organization for the Advancement of Structured Information Standards
OASIS MQTT	MQTT Protocol defined by OASIS
OMG	Object Management Group
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technology
prEN	European Pre-Norm (draft standard)
PWI	Preliminary Work Item
RAM	Random Access Memory
REST	Representational State Transfer
RFID	Radio Frequency Identification
RTO	Research and Technology Organization
SAG	Strategic Advisory Group
SAI	Securing Artificial Intelligence
SAM	Secure Access Module
SBOM	Software Bill of Materials
SC	Subcommittee
SIEM	Security Information and Event Management
SOA	Service-Oriented Architecture

SVM	Support Vector Machine
SysML	Systems Modelling Language
TAM	Technology Acceptance Model
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical Report
TS	Technical Specification
UC	Use Case
UDP	User Datagram Protocol
VPN	Virtual Private Network
WG	Working Group

8.2 Appendix B: Current list of ISO/IEC SC42 AI standards

Standards and projects under SC 42 (2026-04-20): AI (36 published + 50 under development) and Big Data (5 published)

Artificial Intelligence (36) published (Artificial Intelligence (36) published (RED: published 2026, violet: published 2025)

- ISO/IEC 4213:2022 Information technology — Artificial Intelligence — Assessment of machine learning classification performance
- ISO/IEC 5259-1:2024 Artificial Intelligence — Data quality for analytics and ML — Part 1: Overview, terminology, and examples
- ISO/IEC 5259-2:2024 Artificial Intelligence — Data quality for analytics and ML — Part 2: Data quality measures
- ISO/IEC 5259-3:2024 Artificial Intelligence — Data quality for analytics and ML — Part 3: Data quality management requirements and guidelines
- ISO/IEC 5259-4:2024 Artificial Intelligence — Data quality for analytics and ML — Part 4: Data quality process framework
- **ISO/IEC 5259-5:2025** Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 5: Data quality governance framework
- ISO/IEC 5338:2023 Information technology — Artificial intelligence — AI system life cycle processes
- ISO/IEC 5339:2024 Information Technology — Artificial Intelligence — Guidelines for AI applications
- ISO/IEC 5392:2024 Information technology — Artificial intelligence — Reference architecture of knowledge engineering
- ISO/IEC TR 5469:2024 Artificial intelligence — Functional safety and AI systems
- **ISO/IEC TS 6254:2025** Information technology — Artificial intelligence — Objectives and approaches for explainability of ML models and AI systems
- ISO/IEC 8183:2023 Information technology — Artificial intelligence — Data life cycle framework
- ISO/IEC TS 8200:2024 Information technology — Artificial intelligence — Controllability of automated artificial intelligence systems
- ISO/IEC TS 12791:2024 Information technology — Artificial intelligence — Treatment of unwanted bias in classification and regression machine learning tasks
- **ISO/IEC 12792:2025** Information technology — Artificial intelligence — Transparency taxonomy of AI systems
- ISO/IEC TR 17903:2024 Information technology — Artificial intelligence — Overview of machine learning computing devices

- **ISO/IEC TR 20226:2025** Information technology — Artificial intelligence — Environmental sustainability aspects of AI systems
- **ISO/IEC TR 21221:2025** Information technology - Artificial intelligence - Beneficial AI systems
- ISO/IEC 22989:2022 Information technology - Artificial intelligence — Artificial Intelligence Concepts and Terminology
- ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
- ISO/IEC 23894:2023 Information technology — Artificial Intelligence — Guidance on Risk Management
- ISO/IEC TR 24027:2021 Information technology — Artificial Intelligence (AI) — Bias in AI systems and AI aided decision making
- ISO/IEC TR 24028:2020 Information technology — Artificial Intelligence — Overview of trustworthiness in artificial intelligence
- ISO/IEC TR 24029-1:2021 Artificial Intelligence — Assessment of the robustness of neural networks — Part 1: Overview
- ISO/IEC 24029-2: 2023 Artificial Intelligence — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods
- ISO/IEC TR 24030:2024 Information technology — Artificial Intelligence — Use cases (**Withdrawn version 2021)**
- ISO/IEC TR 24368:2022 Information technology — Artificial Intelligence (AI) — Overview of ethical and societal concerns
- ISO/IEC TR 24372:2021 Information technology — Artificial Intelligence — Overview of computational approaches for AI systems
- ISO/IEC 24668:2022 Information technology — Artificial intelligence — Process management framework for big data analytics
- ISO/IEC TS 25058:2024 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Guidance for quality evaluation of artificial intelligence (AI) systems
- ISO/IEC 25059:2023 Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI-based systems
- ISO/IEC 38507:2022 Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations
- ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system
- **ISO/IEC 42005:2025** Information technology — Artificial intelligence — AI system impact assessment
- **ISO/IEC 42006:2025** Information technology — Artificial intelligence — Requirements for bodies providing audit and certification of artificial intelligence management systems
- **ISO/IEC TS 42119-2: 2025** Artificial intelligence —Testing of AI - Part 2: Overview of testing AI systems

Other responsibility:

- ISO/IEC AWI TS 29119-11:2020- Software and systems engineering — Software testing — Part 11: Guidelines on the testing of AI-based systems (under responsibility of ISO/IEC JTC1 SC 7)

Big Data (5) published, plus one under ISO/IEC JTC1 SC27 (Cybersecurity)

- ISO/IEC 20546:2019 Information technology - Big data - Overview and vocabulary
- ISO/IEC 20547-1:2020 Information technology — Big data reference architecture — Part 1: Framework and application process
- ISO/IEC TR 20547-2:2018 Information technology — Big data reference architecture — Part 2: Use cases and derived requirements
- ISO/IEC 20547-3:2020 Information technology — Big data reference architecture — Part 3: Reference architecture
- ISO/IEC 20547-4:2020 Information technology — Big data reference architecture — Part 4: security and privacy (**developed** by **ISO/IEC JTC1 SC27,** IT security, cybersecurity and privacy protection)
- ISO/IEC TR 20547-5:2018 Information technology — Big data reference architecture — Part 5: Standards roadmap#

Under Development (50) (change of status included: DTS, DTR, DIS, FDIS)

Currently under publication: Change of status (to CD, DIS, etc. marked too in colour!)

Note: DTS, DTR, FDIS expected to be published soon! (RED: new 2026;violet new 2025)

- ISO/IEC CD 4213 Artificial intelligence - Performance measurement for AI classification, regression, clustering and recommendation tasks
- ISO/IEC **TR** 5259-6 Data quality for analytics and machine learning (ML) — Part 6: Visualization framework for data quality
- ~~ISO/IEC AWI TS 17847: Information technology — Artificial intelligence — Verification and validation analysis of AI systems~~ - replaced by 42119-3
- ISO/IEC **CD** TR 18988: Artificial intelligence — Application of AI technologies in health informatics
- ISO/IEC **CD** TS 22440-1 - Artificial intelligence — Functional safety and AI systems — Part 1: Requirements
- ISO/IEC **CD** TS 22440-2 - Artificial intelligence — Functional safety and AI systems — Part 2: Guidance
- **ISO/IEC CD TS 22440-3** - Artificial intelligence — Functional safety and AI systems — Part 3: Examples of application
- ISO/IEC CD TS 22443 Information technology — Artificial intelligence— Guidance on addressing societal concerns and ethical considerations.
- ISO/IEC AWI 22989-2 - Artificial intelligence —Concepts and terminology - Part 2: Healthcare
- ISO/IEC 22989:2022/DAmd1 - Information technology - Artificial intelligence — Artificial Intelligence Concepts and Terminology - Amendment 1
- **ISO/IEC 22989:2022/AWI Amd2** - Information technology - Artificial intelligence — Artificial Intelligence Concepts and Terminology - Amendment 2

- ISO/IEC 23053:2022/DAmd1 - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) – Amendment 1
- **ISO/IEC 23053:2022/AWI Amd2** - Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) – Amendment 2
- ISO/IEC CD TR 23281 – Artificial intelligence — Overview on AI tasks and functionalities related to natural language processing.
- ISO/IEC CD 23282 - Artificial intelligence — Evaluation methods for accurate natural language processing systems
- ISO/IEC **DIS** 24029-3 Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 3: Methodology for the use of statistical methods
- **ISO/IEC AWI TR 24030** Information technology — Artificial intelligence (AI) — Use cases
- **ISO/AWI TR 24492** Standardization needs for the application of artificial intelligence in the financial services industry
- ISO/IEC DIS 24970 Artificial intelligence – AI system logging
- ISO/IEC **DIS** 25029 Artificial intelligence – AI-enhanced nudging
- **ISO/IEC AWI 25058** Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Measurement and guidance for quality evaluation of AI systems
- ISO/IEC DIS 25059 Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality models for AI-based systems
- ISO/IEC AWI TS 25223 Information technology – Artificial intelligence – Guidance and requirements for uncertainty quantification in AI systems
- ISO/IEC **CD** TS 25258 Information technology – Artificial intelligence – Hybrid AI inference framework for AI systems
- ISO/IEC AWI TR 25523 Information technology – Artificial intelligence – Overview of data profiles for analytics and ML
- **ISO/IEC AWI TS 25566** Terminology and concepts for domain engineering of AI systems
- **ISO/IEC WD TS25568 -** Information technology — Artificial Intelligence — Guidance on addressing risks in generative AI systems
- **ISO/IEC AWI TS 25569** - Artificial Intelligence — Implementation guidance on de-identification of data used in Machine Learning (ML)
- **ISO/IEC AWI TS 25570** - Information Technology — Artificial Intelligence — Reliability assessment of AI systems
- **ISO/IEC AWI TS 25571** - Artificial Intelligence — Example template for documenting ethical issues of an AI system
- **ISO/IEC AWI 25589** Information technology — Artificial intelligence — Framework for human-machine teaming
- **ISO/IEC AWI 25590** - Information technology — Artificial intelligence — Guidance for output data quality of generative AI applications
- **ISO/IEC AWI 25623** Artificial intelligence — Machine learning (ML) model description framework
- ~~**ISO/IEC AWI 25651** - Information technology — Artificial intelligence — Guidance on the implementation of ISO/IEC 42001 (AI management system)~~ - **replaced by ISO/IEC AWI 42003**
- **ISO/IEC AWI 25704** Artificial Intelligence — Process assessment model for AI system life cycle processes
- **ISO/IEC AWI TS 25864** Information technology – Artificial Intelligence (AI) – Resilience assessment of AI systems
- **ISO/IEC AWI 25870** Artificial intelligence — Reporting framework for AI incidents
- ISO/IEC AWI 25872-1 Artificial intelligence — Knowledge enhancement for pretrained machine learning models — Part 1: Framework

- **ISO/IEC AWI TS 26312** Information technology — Artificial intelligence — Identification and treatment of bias in AI by healthcare organizations
- **ISO/IEC AWI TS 26320** Information technology — Artificial intelligence — Corpus development and maintenance for natural language processing systems (NEW April 2026)
- **ISO/IEC AWI 42003** - Information technology — Artificial intelligence — Guidance on the implementation of ISO/IEC 42001 (AI management system)
- ISO/IEC **CD** 42007 Information technology — Artificial intelligence — High-level framework and guidance for the development of conformity assessment schemes for AI systems
- ISO/IEC **DIS** 42102 - Information technology — Artificial intelligence — Taxonomy of AI system methods and capabilities
- ISO/IEC **CD** TR 42103 Information technology — Artificial intelligence — Overview of synthetic data in the context of AI systems
- ISO/IEC DIS 42105 - Information technology — AI— Guidance for human oversight of AI system
- ISO/IEC **TR** 42106 Information technology — Artificial intelligence — Overview of differentiated benchmarking of AI system quality characteristic
- ISO/IEC **CD** TR 42109 Information technology — Artificial intelligence —Use cases of human-machine teaming
- ISO/IEC **CD** TS 42111 Information technology — Artificial intelligence —Guidance on light-weight AI systems
- ISO/IEC DTS 42112 Information technology — Artificial intelligence —Guidance on machine-learning model training efficiency optimization
- ISO/IEC DTS 42119-3.**2** Artificial intelligence —Testing of AI - Part 3: Verification and validation analysis of AI systems
- **ISO/IEC AWI TS 42119-7** Artificial intelligence — Testing of AI — Part 7: Red teaming
- **ISO/IEC AWI TS 42119-8** Artificial intelligence — Testing of AI — Part 8: Quality assessment of prompt-based text-to-text systems that utilize generative AI

NEW PWI (Preliminary Work ITEM): "Governance and management of human oversight of AI systems**"**

NEW PWI: ISO/IEC PWI 25880 "Information technology — Artificial intelligence — Guidance for organizational implementation of human-machine teaming concept"

NEW NWIP: Artificial Intelligence - Framework for structured multi-agent interaction in AI systems (MAS) (April 20, 2026).