Haiku
Human AI teaming Knowledge and Understanding for aviation safety

Deliverable N.7.1

State of the art in safety, human factors, and security (SHS) assurance processes in aviation

Authors:

Elisa Spiller, Filippo Tomasello, Paola Lanzi, Nikolas Giampaolo (DBL)

Abstract:

This document is the second iteration of D7.1 - State of the Art in Safety, Human Factors and Security (SHS) Assurance Processes in Aviation within the HAIKU project. It analyses and updates the legal, regulatory and ethical framework for the development and implementation of AI-based solutions in the aviation sector. In particular, the document provides a comprehensive overview of the recent developments introduced by the EU AI Act (reg. (EU) 2024/1689), its impact on the aviation regulatory framework and the implementation strategy undertaken by EASA. It also collects and examines the main technical and industrial standards currently being developed for these technologies in aviation.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

Information Table

Deliverable Number	7.1
Deliverable Title	State of the art in safety, human factors, and security (SHS) assurance processes in aviation
Version	2.0
Status	Final
Responsible Partner	DBL
Contributors	Elisa Spiller, Filippo Tomasello, Paola Lanzi, Nikolas Giampaolo
Contractual Date of Delivery	31.08.2024
Actual Date of Delivery	31.08.2024
Dissemination Level	PU

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

Document History

Version	Date	Status	Author	Description
1.0	28.02.2023	Final	Filippo Tomasello | DBL Paola Lanzi | DBL Elisa Spiller | DBL Nikolas Giampaolo | DBL	Final - 1st iteration
1.1	11.04.2024	Draft	Elisa Spiller | DBL	TOC
1.2	28.06.2024	Draft	Elisa Spiller | DBL	Draft added: §§ 2, 3.1, 3.2, 3.3, 3.4
1.3	02.08.2024	Draft	Elisa Spiller | DBL Paola Lanzi | DBL	Draft added: § 1
1.4	12.08.2024	Draft	Filippo Tomasello | DBL	Draft added: §§ 4-5
1.5	19.08.2024	Draft	Elisa Spiller | DBL	Draft added: § 6
1.6	26.08.2024	Draft	Elisa Spiller | DBL Paola Lanzi | DBL	Internal Review
1.7		Draft	Simone Pozzi | DBL Vanessa Arrigoni | DBL	Review and quality check
2.0	31.08.2024	Final	Elisa Spiller | DBL Filippo Tomasello | DBL Paola Lanzi | DBL	Final - 2nd iteration

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

List of Acronyms

Table 1. List of Acronyms

Acronym	Definition
AI	Artificial Intelligence
AIA	AI Act (i.e., Reg. (EU) 2024/1689)
AIIA	AI Industry Alliance
AILD	AI Liability Directive (i.e., COM/2022/496 final)
AIMS	AI Management System
ALTAI	Assessment list for Trustworthy Artificial Intelligence
AMC	Acceptable Mean of Compliance
ANS	Air Navigation Service
ASTM	American Society for Testing and Materials
ATM	Air Traffic Management
BR	Basic Regulation (i.e., Reg. (EU) 2018/1139)
CSF	Cyber Security Framework
DAL	Design Assurance Level
DG	Directorate-General
DO	Document
EAR	Easy Access Rules
EASA	European Union Aviation Safety Agency
EC	European Commission
ED	EUROCAE Document

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

EP	European Parliament
EPRS	European Parliament Research Service
ER	Exploratory Research
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
Exec. Ord.	Executive Order
FAA	Federal Aviation Administration
FDIS	Final Draft International Standard
FOD	Foreign Object Debris
FRIA	Fundamental Rights Impact Assessment
GAO	Government Accountability Office
GM	Guidance Material
HAIKU	Human AI teaming Knowledge and Understanding for aviation safety
HLEG-AI	High Level Expert Group for AI
HP	Human Performance
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organisation for Standards
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
JTC	Joint Technical Committee
KPA	Key Performance Area
KPI	Key Performance Indicator

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

KSA	Knowledge, Skills, Attitudes
LBK	Logic Based Knowledge
M	Month
MASPS	Minimum Aviation System Performance Standards
ML	Machine Learning
MLEAP	Machine Learning Application Approval Project
MoC	Mean of Compliance
MSS	management system standard
New PLD	New Product Liability Directive (i.e., COM/2022/495 final)
NICE	National Initiative for Cybersecurity Education
NIST	National Institute for Standards and Technology
OHS	Occupational Health and Safety
OSTP	Office of Science and Technology Policy
PDCA	Plan-Do-Check-Act [framework]
PLD	Product Liability Directive (i.e., Dir. (EEC) 85/379)
PRC	People's Republic of China
RTCA	Radio Technical Commission for Aeronautics
S3JU	SESAR 3 Joint Undertaking
SAE	Society of Automotive Engineers
SC	Sub Committee
SDO	Standard Development Organisation
SESAR	Single European Sky ATM Research
SHS	Safety, Human Factor, Security

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

SOAR	State of the Art Report
SQuaRE	Systems and software Quality Requirements and Evaluation
SSH	Social Science and Humanities
SW	Software
TR	Technical Report
UAM	Urban Air Mobility
UAS	Unmanned Air/Aircraft System
UC	Use Case
US	United States of America
WG	Working Group
WH	White House

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

Table of contents

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

List of Tables

List of Figures

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

1. Introduction

1.1. Scope of the document

This document is the second iteration of HAIKU D7.1 "State of the art in safety, human factors, and security (SHS) assurance processes in aviation". It reports on the progress achieved within Task T7.1 "State of the art and regulatory landscape", also in light of the numerous significant developments that occurred from February 2023 (M6) to August 2024 (M24).

In line with the purposes of T7.1, the document focuses on the current ethical and legal framework and a State-of-the-Art Report (SOAR) of regulations and consensus-based industry standards for the introduction of Artificial Intelligence (AI) in civil aviation. The first iteration of this deliverable (released at M6 in February 2023) provided a comprehensive analysis of the legal and regulatory framework, embracing all the aviation domains covered by the HAIKU use cases: aircraft operations, aerodrome safety, Air Traffic Management (ATM), Urban Air Mobility (UAM) and Health and Occupational Safety (OHS) at aerodromes. In this second iteration, instead, the attention converges on the main regulatory or standardisation events occurring meanwhile. In particular, considering the scope of the project, the attention converges on the European Union (EU) system, especially focusing on the impact of the EU AI Act (i.e., Reg. (EU) 2024/1689) for aviation and EASA AI Roadmap 2.0 (EASA, 2023), as complemented by the final report of the Machine Learning Application Approval Research Project (MLEAP) in May 2024 (EASA, 2024(b)).

According to the editorial strategy adopted for the first version of D7.1, to keep it focussed on legal, ethical and regulatory aspects, this deliverable does not include information about the best practices concerning SHS assurance processes in aviation. This activity has in fact been moved to D7.2, which will present the analysis of the best practices for SHS assurance process and the acceptable means of compliance on SHS to be applied and validated in the HAIKU use cases.

1.2. Structure of the document

The document is divided in 5 sections, as follows:

- **Section 1** includes the present **introduction**, describing the scope and the structure of the document.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

- **Section 2** introduces the concept of **AI Trustworthiness in aviation**, thus redefining this principle according to the specific needs of the sector.
- **Section 3** presents the updated version of the **regulatory framework for AI in civil aviation**, providing a general overview of the EU strategy and a systematic analysis of the main novelties occurring meanwhile.
- **Section 4** provides the newly **introduced industry standards on AI and on application of AI in aviation**.
- **Section 5** reports the **conclusion and the take-away messages**.

2. AI Trustworthiness in aviation

The regulatory landscape for artificial intelligence is undergoing rapid change and is expected to continue developing in the near future, driven by lessons learned from experience. In the aviation sector, it is crucial to consider the diverse jurisdictional and regulatory approaches, from those with broad applicability across all areas of human activity to highly specific and sector-specific AI applications, guided by methodologies and reasoning tailored to the aviation domain.

To comprehensively address the evolution of the regulatory framework since the first iteration of this deliverable, HAIKU centred on the pivotal principle that currently unifies the major international approaches to AI regulation: **trustworthiness**. The research conducted within the project aims to enhance and deepen the understanding of this concept, to propose proportionate and suitable practices in the aviation domain.

2.1. Trust and AI trustworthiness

Trust is a multifaceted concept that is interpreted in varying ways across different disciplines (Devitt, 2018). However, despite differing perspectives, it is an essential component of robust relationships, where integrity and reliability are consistently emphasised.

There is no single accepted definition of this concept in the literature. For example, among the other several standard development organisations (SDOs), in the United States (US) the National Institute of Standards and Technology (NIST) defines trust as "the confidence that one element has in another that the second element will behave as expected". At the international level, **ISO/IEC 25010** sets out an enhanced definition of this concept, specifying that **trust means the extent to which the user is persuaded that the product will behave as intended**.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

As a result, **trustworthy AI is a framework designed to ensure that a system deserves and earns the trust of the user by providing verifiable evidence that it meets its specified requirements**. It therefore aims to meet user and stakeholder expectations in a measurable way.

2.2. Legal Perspectives on AI Trustworthiness

Given the international dimension of aviation, HAIKU conducted a comparative analysis of leading regional and international approaches, with a particular focus on the EU, US and China. The analysis demonstrates that **the concept of trustworthiness is a key element in many legal and regulatory frameworks**. In essence, the objective is to provide guidance on the development of regulatory frameworks for AI, with a focus on **key principles such as fairness, explainability, accountability, privacy, and acceptance** (Kaur et al., 2022).

First in the world, the EU has proposed ethical guidelines for trustworthy AI and is progressing towards specific legislative measures to proactively define technology design, technical and organisational requirements, and to safeguard safety, security and fundamental rights (EC, 2018; EU, 2022; EU, 2024). The main milestone achieved between the first and second iterations of this deliverable is the adoption of the EU AI Act (shortened: AIA). As a Regulation, it will be directly applicable at national level. In addition, the European Commission (EC) has been mandated to adopt further detailed implementing rules to operationalise the general provision in practice.

Looking at the US framework, there is a gradual alignment of federal legislation with the funding principles of AI trustworthiness, especially in terms of prevention of algorithmic bias, privacy, transparency and accountability (Madhavan et al., 2020). This approach is promoted by the White House (WH) Office of Science and Technology Policy (OSTP) through the Blueprint for an AI Bill of Rights in 2022 (WH-OSTP, 2022). It has been consolidated for the management and operations of the federal government through the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, issued on 30 October 2023 (Exec. Ord. No. 14110, 88.FR.75191(2023)). Federal agencies are responsible for implementing these principles and guidelines in accordance with their institutional mission and the specific needs of their sectors (EP, 2024).

Analogous direction is also evident in the China approach (EP, 2021). Through the Artificial Intelligence Industry Alliance (AIIA) (Luong & Arnold, 2021), the Chinese government is fostering a closer collaboration among local governments, academic

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

institutions, and companies, with the aim of promoting a trustworthy approach to AI based on reliability, controllability, transparency and explainability, data protection, clear responsibilities, and diversity and tolerance (CAICT, 2021, 6). These efforts and related guidelines culminated in a preliminary draft of the Chinese AI Law Strategy in early 2024, and the process is still ongoing (Yang, 2024).

2.3. AI Trustworthiness for aviation

In light of the above, worth noting that for advanced technologies, a risk- and performance-based regulatory approach is typically adopted. In this approach, legally binding regulations should define the objectives to be achieved, while consensus-based industry standards provide guidance on how to achieve compliance.

In this context the International Organisation for Standardisation (ISO) has introduced methodologies that emphasise fairness, transparency, accountability and controllability to promote trust in AI systems (ISO, 2023). Beyond the EU, at national level, the NIST has developed frameworks to assess and improve user trust in AI systems (NIST, 2023). In the United States, the Government Accountability Office (GAO) has issued guidelines to promote the responsible use of AI although industry standards for voluntary application cannot mitigate the current absence of legally binding rules on AI in the USA (GAO, 2021; GAO, 2024).

Given the specific characteristics and needs of the aviation sector, the concept of trustworthiness has been readily accepted. Indeed, the latter is based on milestone values of aviation safety culture such as safety, security, technological robustness, reliability, accountability. Additional emphasis is placed on the expectations for transparency and explainability, as well as on the importance of human oversight (Kirwan, 2024; Kabashkin et al., 2023). These requirements form the common foundation that the sector adheres to, even at the international level. Compliance with these principles, though implemented through different standards, represents an initial alignment of technologies, systems, and concepts with shared expectations. EASA is working in this direction within the AI Roadmap 2.0. The Federal Aviation Administration (FAA) is undertaking a similar path with the Roadmap for Artificial Intelligence Safety Assurance (FAA, 2024).

Currently, the European approach to regulation has achieved the highest level of maturity and detail in the practical implementation of these aspects in design, development, and validation of AI applications. Given the nature and objectives of

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

HAIKU, the analysis will primarily focus on these references, including additional insights from other regulatory contexts, as necessary.

3. Regulatory framework for AI in civil aviation

3.1. EU AI regulatory framework

The European Union has adopted in 2018 a comprehensive strategy for the regulation of AI (EC, 2018; EC, 2020). This strategy covers three fronts: political, economic and regulatory.

The primary objective is to promote the human-centred development of AI solutions while balancing the goal of strengthening innovation and economic leadership and competitiveness. This approach applies both to solutions intended for the general public and to applications developed for specific sectors (EC, 2020).

To achieve these goals, the EU and its member states are implementing multi-year investment and funding plans tailored to sector-specific needs (HLEG-AI, 2020(b)). The objective is to prioritise projects and initiatives in research, design, and development that promote a systemic approach to AI solutions. **This entails ensuring that the primacy of technical aspects is complemented by thorough ethical and social considerations** (EC, 2023). These considerations are crucial for accurately assessing, evaluating, and guiding the individual and collective impacts of new solutions, possibly from their initial design phases (HLEG-AI, 2019; HLEG-AI, 2020(a)).

Building on these premises, the regulatory approach is based on hard law — mandatory rules and requirements that are essential for compliance purposes. This framework is complemented by a range of soft law instruments, which offer guidelines and methodologies to support proactive compliance efforts. Generally, it is assumed that such systems must possess three general characteristics, maintained throughout their entire lifecycle:

- they must be **legal**, meaning compliant with all applicable laws and regulations;
- they must be **ethical**, aligning with the social values and ethical principles of the relevant context (in this case, the European context); and
- they must be **robust**, both from a technical and social standpoint, proactively preventing the risk of unintentional harms.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

Accordingly, the cornerstones of this strategy includes not only the already adopted AI Act[1] (AIA), but also the proposed AI Liability Directive[2] (AILD), the new Directive on Product Liability[3] (PLD) voted by the European Parliament on 12 March 2024 (waiting for the final Council position) and the principles and methodologies for ethical risk assessment proposed by HLEG-IA with ALTAI[4].

For the purpose of this document, the main contributions of these references can be summarised as follows.

3.1.1. The AI Act

The **AIA** (into force since 01 August 2024), is the cornerstone of the regulatory architecture and aims to establish **general rules for AI system safety and respect for fundamental rights**. The regulation contains key provisions for the development and market introduction of AI-based systems, **prioritising a proportionate risk-based approach**. It sets out obligations and responsibilities for the various actors involved in the value and use chain of AI.

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 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 (Artificial Intelligence Act).

[2] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM/2022/496 final).

[3] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products (COM/2022/495 final).

[4] In its Communication of 25 April 2018 and 7 December 2018, the European Commission set out its vision for artificial intelligence (AI), which supports "ethical, secure and cutting-edge AI made in Europe". Three pillars underpin the Commission's vision: (i) increasing public and private investments in AI to boost its uptake, (ii) preparing for socio-economic changes, and (iii) ensuring an appropriate ethical and legal framework to strengthen European values. To support the implementation of this vision, the Commission established the High-Level Expert Group on Artificial Intelligence (AI HLEG), an independent group mandated with the drafting of two deliverables: (1) AI Ethics Guidelines and (2) Policy and Investment Recommendations. The HLEG also produced an Auto-assessment List for Trustworthy Ai (ALTAI), to facilitate the effective use of the ethics framework in practice. For more information about ALTAI, please, see: HLEG-IA, THE ASSESSMENT LIST FOR TRUSTWORTHY ARTIFICIAL INTELLIGENCE (ALTAI) for self-assessment, Brussels, 17th July 2020. The user-friendly application of this methodology is also supported by the MyALTAI portal: https://altai.insight-centre.org.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

Stricter requirements are imposed for high-risk systems, in particular those intended to perform safety functions or those requiring certification or conformity assessment due to their intended use.

The principles established by this Regulation are of general value and **will be refined and implemented by sector-specific regulations, for sectors with specific safety requirements**, **such as aviation rules developed by EASA.**

3.1.2. The AI Liability Directive

The **AILD** (proposal) establishes a **fault-based regime**, providing rules for non-contractual liability due to AI-induced harm to non-professional users. It applies when specific liability regimes do not cover the situation and covers damage caused by AI systems, regardless of their classification under AI law.

Importantly, the Directive introduces a rebuttable presumption of causation, simplifying victims' proof of harm caused by AI. If a victim can demonstrate **fault in failing to meet obligations related to their harm and a likely connection with AI actions**, courts may presume this fault caused the harm. National courts can order disclosure of evidence for high-risk AI systems suspected of causing harm. The defendant can rebut this presumption only by proving compliance with their solutions and that their fault did not cause damage.

Despite its residual nature, this approach clarifies **the burden of proof for operators in complying with AI Act requirements and underscores court disclosure powers in AI-related harm cases**.

3.1.3. The new Product Liability Directive

The new **PLD** (proposal already voted by the EP) establishes a **no-fault liability regime** for damage caused by products intended for private use, including software and AI. Manufacturers and economic operators who can substantially modify products can be held liable for **defects**, even if they emerge after the product is placed on the market, such as **software updates, cybersecurity vulnerabilities or machine learning failures**.

The new PLD requires manufacturers to disclose necessary information in court when the injured person provides enough evidence to support a plausible compensation claim. This establishes **a presumption of defectiveness and causal link, particularly if the manufacturer fails to provide requested safety compliance information, the damage is due to an obvious product malfunction, or technical complexity makes**

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

proving liability difficult (as with AI). Economic operators can rebut this presumption with the development risk defence by proving that the state of technical knowledge at the time was such that the defect could not have been detected**.**

Despite its residual nature, this approach clarifies **operators' responsibilities for AI Act compliance and proactive risk prevention in design, manufacturing, and warning defects, while also emphasising court disclosure powers in AI-related harm cases**.

For aviation it is important to observe Article 5 of the new PLD, confirming the approach of the old Dir. (EEC) 85/379, ensures compensation not only to the consumer (i.e. the person who purchased a product on the market) but to any natural person who has suffered damage caused by a defective product ('the injured person'). In case of drones, for instance, the injured person may not be only the remote pilot or any other employee of the UAS operator, but also any third party (e.g. non-involved people on the ground) who has suffered damage caused by the crash of a drone.[ES1]

3.1.4. Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment

The **Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment**, developed by the HLEG-AI in 2021 and subsequently made available by the EC via a dedicated interactive online platform, is a tool designed to facilitate the practical application of the HLEG-AI Ethics Framework for a Trustworthy AI.

It aims to **guide the design, development and deployment phases throughout the system lifecycle, starting from the early planning stages**. **This assessment is strongly recommended for all AI applications, regardless of their risk level under the AI Act.**

The tool provides a set of general questions to help assess the ethical implications of design and organisational decisions related to specific AI applications. It addresses all seven requirements outlined by the HLEG-AI: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental wellbeing, and accountability.

Given its broad and comprehensive approach, the Framework covers aspects and issues of varying relevance in different contexts. Therefore, **the EC encourages**

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

sectoral authorities and stakeholders to engage in discussions to adapt ALTAI to the specific needs of different sectors.

3.2. AI Act and Civil Aviation

As anticipated, the AIA represents the cornerstone of a comprehensive regulatory framework that will develop in a very detailed manner over the coming years, progressively addressing the specific needs of various sectors (including aviation).

In general, the most important contributions of this regulation to the current regulatory framework consist of providing a legal definition of AI and establishing a proportionate risk-based regulatory approach. The AIA further defines general principles for the development and implementation of technologies that are safe and respectful of fundamental rights. Eventually, the document proposes clear directives on how to coordinate the general regulation with sector-specific regulations, including aviation.

3.2.1. The legal definition of AI

According with the new AIA, AI is intended as:

> *"a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, contents, recommendations, or decisions that can influence physical or virtual environments" (Article 3(1)).*

As the text highlights (recital 12), this definition is based on a set of characteristics that distinguish AI from simpler traditional software or Information Technology (IT) systems or programming approaches. These key features can be explained as follows:

- **Automation**, refers to the fact that AI systems run on machines.
- **Autonomy**, meaning that they have some degree of independence of actions from human involvement and of capabilities to operate without human intervention.
- **Adaptiveness,** clarifying that AI could exhibit after deployment self-learning capabilities, allowing the system to change while in use.
- **Inferencing**, intended as the capacity of obtaining the outputs which can influence physical and virtual environments, and to a capability of AI systems to

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

derive models or algorithms, or both, from inputs or data, transcending deterministic data processing by enabling learning, reasoning or modelling.

Against this background, the definition of AI should not cover systems that are based on the rules defined solely by natural persons to automatically execute operations, such as deterministic systems.

3.2.2. A proportionate risk-based regulatory approach

Aligned with this definition of the technological element, the EU has adopted a risk-based approach to introduce a proportionate and effective set of binding rules for AI systems. This approach tailors the content of the rules and the stringency of the requirements to the intensity and scope of the risks posed by AI systems.

The AIA provides clear insights for the classification of prohibited AI practices and high-risk AI systems. Generally, the reference criteria for classification include what follows.

Prohibited AI practices include the development or use of techniques, models, systems or applications having **severe individual and social consequences and unacceptable impacts on fundamental rights and democratic values** (Article 5)[5].

High-risk AI systems generally concern systems that are intended to be used as a **safety component of a product, or systems that are considered to be a product** themselves and that must undergo a third-party conformity assessment before being placed on the market or put into service (Article 6(1)). Systems intended for aviation are also included in this category. The independent third-party responsible for certification or licensing, in case of aviation, may be an aviation authority (EASA or national), a notified body (Article 3(22)) or a qualified entity (Article 69), depending on the applicable aviation rules. In any case, AI systems other than those that are safety components of products, or that are themselves products, are considered as **high-risk**

[5] For example, the AIA generally prohibits subliminal, manipulative or deceptive techniques designed to significantly distort individual or collective behaviour; AI systems that exploit any of the vulnerabilities of a natural person or a particular group of persons; decontextualised and disproportionate social scoring practices and predictive policing to assess or predict an individual's risk of committing an offence, AI systems that create or expand facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage, emotion inference systems and practices in the workplace and educational settings, biometric categorisation systems based on sensitive personal information, the use of 'real-time' remote biometric identification systems in public spaces for law enforcement purposes, unless and to the extent that such use is strictly necessary and subject to judicial review.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

if, in light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, considering both the severity of the possible harm and its probability of occurrence (Recital 52).

Moreover, the AIA classifies high-risk **systems used in particularly sensitive areas and for delicate purposes**, considering their impacts on fundamental rights related to human dignity, liberty and security of person, privacy, education and employment, access to essential services and justice (Annex III)[6]. Where an AI system used in particularly sensitive areas and for delicate purposes performs profiling of natural persons, it should always be considered high-risk.

In these cases (Annex III), a system shall be considered to be **not high-risk where it does not pose a significant risk of harm to natural persons, including by not materially influencing the outcome of decision making** (Article 6(3)). This derogation shall apply in case the AI system is intended:

- to perform a narrow procedural task,
- to improve the result of a previously completed human activity,
- to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review;
- to perform a preparatory task to an assessment relevant for the sensitive purposes.

Providers who consider that an AI system is not high-risk on the basis of the conditions referred to above should draw up documentation of the assessment before that system is placed on the market or put into service. They should also provide that documentation to national competent authorities upon request and are obliged to register the AI system in the EU database (Article 6(4)).

[6] More specifically, the list includes: critical infrastructures (e.g. transport), that could put the life and health of citizens at risk; educational or vocational training, that may determine the access to education and professional course of someone's life (e.g. scoring of exams); safety components of products (e.g. AI application in robot-assisted surgery); employment, management of workers and access to self-employment (e.g. CV-sorting software for recruitment procedures); essential private and public services (e.g. credit scoring denying citizens opportunity to obtain a loan); law enforcement that may interfere with people's fundamental rights (e.g. evaluation of the reliability of evidence); migration, asylum and border control management (e.g. automated examination of visa applications); administration of justice and democratic processes (e.g. AI solutions to search for court rulings).

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

Accordingly, the AIA establishes specific requirements for high-risk AI systems and obligations for their operators (Articles 6 and followings), and mandates transparency obligations for specific AI systems (Article 52). The regulation also encourages providers of non-high-risk AI systems to create code of conduct to foster the voluntary application of some or all of the mandatory requirements applicable to high-risk AI systems, adapted to the lower risk of their solutions (Recital 165).

3.2.3. Fundamental Rights Impact Assessment

One of the most important novelties introduced by the final version of the AIA is the **Fundamental Rights Impact Assessment (FRIA)**. Only postulated in the initial version of the proposal, this is now part of the obligations of deployers of high-risk AI systems (Article 27).

Before deploying a high-risk system to be used in particularly sensitive areas and for delicate purposes (Annex III), deployers that are bodies governed by public law, or are private entities providing public services shall perform an assessment of the impact on fundamental rights that the use of such a system may produce.

Basically, the assessment consists in describing the process and the context where the high-risk system is implemented and used, as well as the period of time or the frequency of usage. The deployers have to identify the categories of natural persons and groups likely to be affected by its use in the specific context and the specific risks of harm likely to have an impact, also taking into account the information given by the provider. Eventually, the assessment has to include a description of the implementation of human oversight measures, according to the instructions for use and the organisational and technical measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

In case the implementation of these systems also required a data protection impact assessment (Reg. (EU) 2016/679, Article 35; Dir. (EU) 2016/680, Article 27), the FRIA prescribed by the AIA complements that data protection impact assessment.

This assessment is required for the first use of the high-risk AI system and at any time the information used for the former are no longer updated. The results of the assessment have to be notified to notify the market surveillance authority. This assessment is not necessary only for high-risk systems for the safety of critical infrastructures.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

3.2.4. The role of ethics for AI trustworthiness

As mentioned, in addition to the risk-based approach guiding the formulation of binding rules, according to the AIA it is essential to consider ethical principles delineated in the framework by the HLEG-AI and the proposed system by ALTAI (Recital 27).

These principles are pivotal for ensuring alignment with Union values and a human-centric approach in AI development. In a nutshell, every AI system, tailored to its risk level and sector-specific needs, should prioritise human oversight to prevent unauthorised use and minimise unintended harm. It must adhere strictly to privacy and data protection standards to maintain data integrity and transparency. Promoting diversity, ensuring equal access, and eliminating discriminatory biases are essential for responsible AI deployment. Additionally, AI development should prioritise sustainability and societal well-being, evaluating their effects on individuals and democratic principles.

These ethical guidelines should inform the development, implementation, and use of all AI applications, irrespective of their risk level. They should serve as the foundation for sector-specific regulations addressing unique technical and safety requirements, as well as for codes of conduct governing low-risk AI applications.

To ensure that AI delivers these expected social and environmental benefits, research and development of AI solutions should aim to improve accessibility for people with disabilities, address socio-economic inequalities or meet environmental goals. To achieve these outcomes, the AIA emphasises the principle of interdisciplinary collaboration, combining technical KPIs with additional KPIs aimed at promoting non-discrimination, accessibility, consumer, environmental and digital rights (Recital 142).

3.2.5. Guidelines for general purpose and generative AI models

The AIA also addresses the regulation of general purpose AI models, intended as AI models trained with a large amount of data using self-supervision at scale, that display significant generality. They are capable of competently performing a wide range of distinct tasks and can be integrated into a variety of downstream systems or applications (Article 3(63)). This category also encompasses generative AI models for flexible generation of various contents, such as text, audio, images or video accommodating a wide range of distinctive tasks (Recital 99).

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

The Regulation sets out specific rules for general purpose AI models when they present **high-impact capabilities and pose systemic risks**[7]. Providers of general-purpose AI models have an important role and responsibility within the AI value chain, as their models form the basis for various downstream systems. This requires a thorough understanding of the models' capabilities for effective integration and compliance. Therefore, the AIA aims to implement appropriate safety and transparency measures, requiring accurate model evaluation in accordance with standardised protocols, assessing and mitigating possible systemic risks, ensuring an adequate level of cybersecurity protection and maintaining up-to-date documentation and providing information on the general-purpose AI model to downstream providers (Articles 53 and 55).

The obligations for providers of general purpose AI models start when these models are placed on the market. AI models used solely for research, development and pre-market prototyping are excluded from these definitions, but must comply with the Regulation once they are placed on the market. These obligations do not apply where a model is used only for internal processes that are not essential for the provision of a product or service to third parties and where the rights of natural persons are not affected (Recitals 97 and 101).

[7] As per Article 51, these models are assumed to have high-impact capabilities when the cumulative amount of computation used for its training measured in floating point operations is greater than 10. A general-purpose AI model shall be classified as a general-purpose AI model with systemic risk if it has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks or following a qualified alert from the scientific panel, also taking into account the input and output modalities of the model, such as text to text (large language models), text to image, multimodal, the number of parameters of the model, the quality or size of the dataset, for example measured in tokens, the amount of computation used to train the model, measured in floating point operations, or indicated by a combination of other variables such as estimated cost of training, estimated time required for training, or estimated energy consumption for training; the input and output modalities of the model, such as text-to-text (large language models), text-to-image, multimodality, and the state of the art thresholds for determining high impact capabilities for each modality, and the specific type of inputs and outputs (e.g. biological sequences); and the benchmarks and assessments of the model's capabilities, including consideration of the number of tasks it can perform without additional training, its adaptability to learn new, different tasks, its degree of autonomy and scalability, the tools it has access to; whether it has a high impact on the internal market by virtue of its reach, which shall be presumed if it has been made available to at least 10 000 registered business users established in the Union; the number of registered end-users.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

3.2.6. The AI Act in Civil Aviation

In light of the foregoing, it is crucial to assess the potential application of the principles and regulations introduced by the AI Act within the aviation sector.

In principle, this sector should fall within the categories typically associated with high-risk applications, including those used as safety components in other products certified by independent third parties, critical infrastructure, and transportation.

More specifically, considering high-risk systems used in particularly sensitive areas and for delicate purposes in aviation, particular attention should be paid at solutions aimed at:

- **remote biometric identification**, excluding identity confirmation[8];
- **emotion recognition**, excluding systems used to detect the state of fatigue of professional pilots or drivers for the purpose of accident prevention[9];
- **security management and operation of critical digital infrastructure[10];**
- **decisions on working conditions**, including working relationships, promotion or dismissal, allocation of tasks, performance monitoring and evaluation[11];
- **law enforcement** and **management of migration, asylum and border control[12]**.

However, it is important to note that the new regulation applies conditionally to solutions previously subject to the 'old approach' to product regulation. This includes, among others, two significant regulations within the aviation sector: (i) Regulation (EC) No 300/2008 on common rules in the field of civil aviation security, and (ii) Regulation (EU) 2018/1139 establishing common rules in the field of civil aviation safety and establishing EASA (referred to as the "Basic Regulation" (BR)).

Generally, considering civil aviation safety and security, the AIA specifies that the requirements and obligations prescribed for high risk applications **do not apply directly, but must be taken into account when adopting detailed measures concerning technical specifications and procedures for the approval and use of safety or security related equipment** (Articles 102 and 108). This is the basis for EASA to develop specific rules on safety of AI applications in aviation.

[8] Annex III, 1(a).
[9] Annex III, 1(c) and Recital 18.
[10] Annex III, 2.
[11] Annex III, 4(b).
[12] Annex III, 6 and 7.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

In such contexts, the EC reserves the right to conduct periodic evaluations and reviews of the AI Act, including the potential adoption of implementing or delegated acts concerning sectoral Union harmonisation legislation. Furthermore, due to the unique characteristics of these sectors, the possibility of establishing an AI regulatory sandbox is considered. Consequently, **despite being classified as high-risk, AI systems regulated under the BR do not have to comply by default with the essential requirements established in the AIA.**

The new AIA has hence brought about significant revisions to the BR, necessitating that the EC/EASA account for the essential criteria applicable to high-risk AI systems in specific instances:

- When adopting, implementing and delegating acts concerning airworthiness (Articles 17 and 19 of the BR as amended by the AIA).
- When adopting, implementing and delegating acts in relation to ATM/ANS providers and entities involved in the design, production or maintenance of ATM/ANS systems and their components (Articles 43 and 47 of the BR as amended by the AIA).
- When adopting implementing and delegated acts concerning unmanned aircraft (Articles 57-58 of the BR as amended by the AIA).

These changes ensure that AI-related considerations are integrated into the regulatory framework governing aviation safety. They mandate the Commission to incorporate the specific requirements and implications for high-risk AI systems, as outlined in the new AIA, into the formulation and implementation of regulations within the aviation sector.

It is thus reasonable to conclude that the essential standards defined in the AI Act for high-risk systems will play a significant role in the future adaptation of the certification framework set out in the BR to regulate high-risk AI-based applications in the aviation sector.

3.3. EASA AI Roadmap

In line with the mandate given to EASA by the AIA (Article 108), the Agency is undertaking progress based on its own AI Roadmap for aviation. As anticipated, the document was initially published in 2020 and later updated in 2023. Eventually, it has been complemented with a series of concept papers (EASA, 2021; EASA, 2024(a)) and more specific guidance in the first public deliverable for MLEAP research project (EASA, 2024(b)).

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

The roadmap outlines how EASA will progressively define and implement the regulatory framework for AI in the aviation sector, specifying which technologies will be classified as AI for the Agency's activities and detailing the application of a risk-based approach in this area. Above all, on an iterative basis, EASA is going to establish usable objectives and test a series of anticipated means of compliance that can proactively contribute to aligning the development of technologies and concepts with the technical, design, and operational requirements that will be needed for certification.

3.3.1. The scope of technologies covered by the Roadmap

Considering the definition of AI proposed by the AI Act, from a technical perspective, the EASA's roadmap currently considers a wide range of approaches, both individually and in hybrid combinations. **Specifically, the main emphasis is currently on machine learning, including deep learning**.

Statistical approaches and Logic- and Knowledge-Based (LKB) systems are also included, provided that, from a practical standpoint, they can generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with, for a given set of human-defined objectives.

Currently, **generative AI is only tangentially referenced in the EASA roadmap as part of hybrid systems.** However, this topic has not yet been comprehensively covered. The tradition of regulatory authorities in civil aviation is in fact to be very cautious with disruptive innovations, therefore moving step-by-step in parallel with accrued experience.

3.3.2. AI trustworthiness in aviation

From a regulatory standpoint, the goal of the roadmap is to implement the approach and principles established by the AI Act within the aviation sector, adapting several implementing regulations or delegated acts and related guidance to meet the specific needs of the aviation industry to exploit AI applications.

From a systematic perspective, in the roadmap EASA has anticipated the intention of introducing adjustments, not only in the airworthiness domain, but across all aviation domains, because in fact AI applications are expected to be introduced in all domains.

The envisaged adjustments, are planned to be carried out in in two steps:

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

- Step 1: development of a **transversal Part-AI** containing the three major blocks of rules, anticipated in the EASA Concept paper and harmonised with the usual structure of EU aviation rules:
    - requirements for authorities (Part-AI.AR) to oversee development, implementation and operational use of AI;
    - requirements for organisations (Part-AI.OR), which means any company or other entity providing aviation products or services, because in the modern approach to aviation safety[13] organisations are at least as important as human individuals; and
    - technical requirements for AI trustworthiness (Part-AI.TR) which in fact will be applicable through all aviation domains and not just aircraft design.
- Step 2: analysis, per domain, of those requirements that are domain-specific and those that need to be complemented to provide an adequate regulatory basis for deploying the new Part-AI. In other words, possible adjustments to existing EU common rules on aviation safety to better accommodate AI with domain specific provisions.

In any case, as usual in the EU aviation regulatory framework, the legally binding rules adopted by the EC will be complemented by Acceptable means of Compliance (AMC) and Guidance material (GM) published by EASA and by consensus-based industry standards published by SDOs.

This approach is summarised in the Figure below:

[13] ICAO, 2018, Safety Management Manual, Doc 9859, 4th edition.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

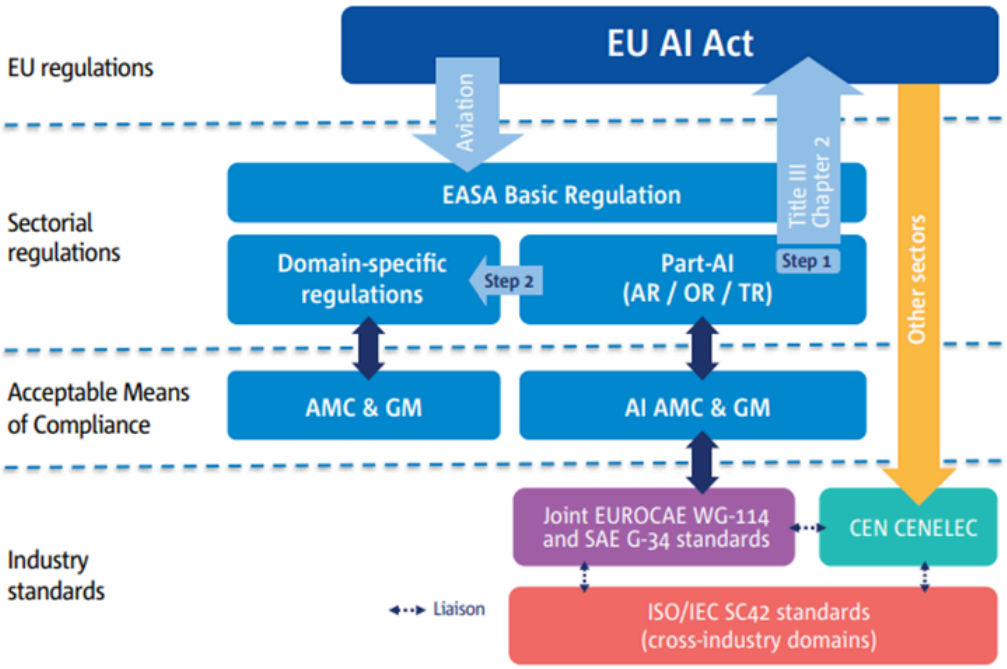

Figure 1. EASA Anticipated regulatory structure for AI (EASA, 2023)

Until the end of August 2024 no public draft of the new EASA Part-AI is available. However, EASA Special Condition SC-AI-01 of April 2022, referring to the released Concept paper on AI, already allows industry to apply for certification of products, parts or systems containing AI constituents.

Beyond safety, the roadmap and the concept papers guiding its development and implementation have explicitly outlined how EASA intends to incorporate as well the ethical and legal principles defined in the broader European AI strategy to operationalize the concept of trustworthy human-centred AI within the aviation sector.

As a preliminary step before examining the technical KPAs that inform the development of new technological solutions, EASA introduces a preliminary trustworthiness assessment. This assessment integrates an evaluation of the safety, security, and ethical impacts of the proposed AI application.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

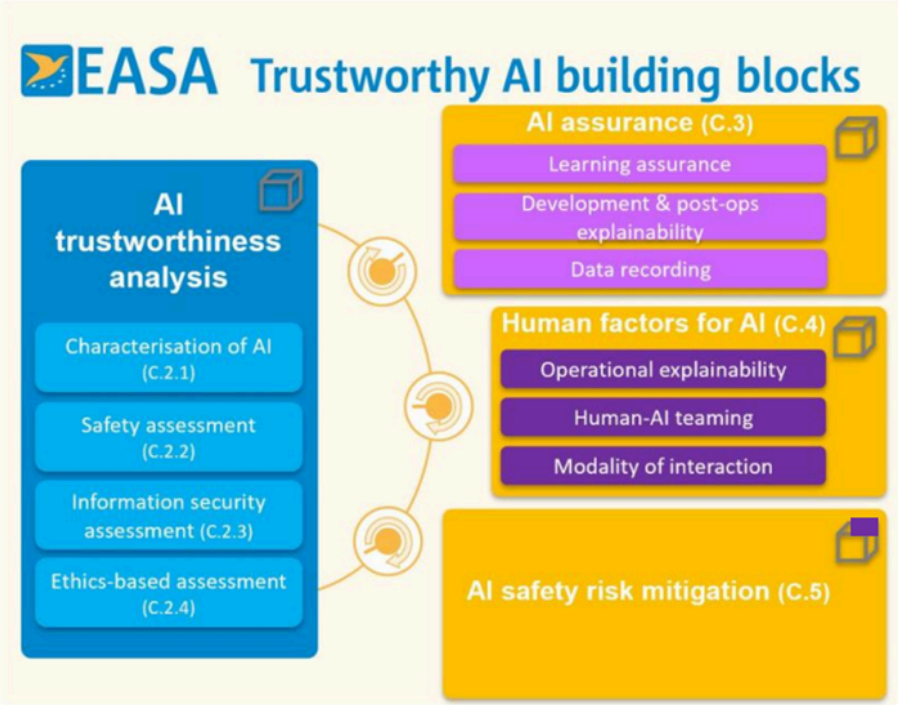

Figure 2. EASA AI trustworthiness building blocks (EASA, 2024(a))

As outlined in the figure above, the approach is structured into 4 complementary building blocks.

Trustworthy AI analysis aims to establish a connection with the EU Ethical Guidelines HLEG-AI, 2019) and introduces a preliminary gate analysis to the three additional technical components. This assessment is always required and should be performed in its full spectrum for any AI application (EASA, 2024(a), 10).

3.3.3. Levels of risk and levels of automation

The second significant contribution proposed by EASA for the regulation of AI in the aviation sector is the introduction of a classification system. This system distinguishes AI systems based on the contribution they make and the authority they assume in interactions with human operators and the surrounding environment. Depending on the extent to which functions and tasks are delegated to AI, different safety, security, and Human Performance (HP) requirements are envisaged, following a proportional progressive criterion. This approach aims to proactively contribute to a better risk mitigation strategy from the early stages of design.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

The roadmap classifies AI applications into three levels, represented as follows:

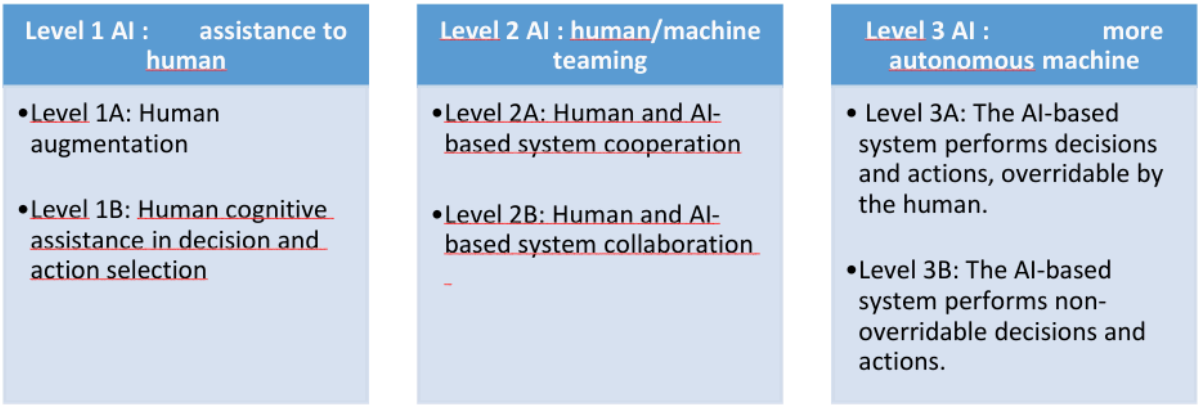

Figure 3. EASA Classification of AI applications (EASA, 2024(a))

The main difference between Level 1 and Level 2 AI applications is in the implementation of decisions. In Level 1, the end user makes all decisions and actions with the assistance of the AI. In Level 2, the AI can automatically select and implement actions, but the end user retains full oversight and override capabilities.

It is important to clarify that within Level 2, regarding human-AI teaming, the roadmap distinguishes between cooperation and collaboration. In case of cooperation, the AI-based system assists the end user in achieving their goals through a predefined task allocation. It provides feedback on decisions and actions but does not require shared situational awareness. Instead, in case of collaboration, both the human end user and the AI-based system work together towards a shared goal, adjusting strategies and task allocations in real-time. Collaboration involves shared situational awareness and requires effective communication to achieve mutual objectives.

Accordingly, the difference between Level 2 and Level 3 AI is the level of authority granted to the AI system. At Level 2, the AI has partial authority under the full supervision of the human end user. At Level 3, the AI has full authority, either with remote human end-user supervision (Level 3A) or completely independent (Level 3B).

Future guidance on Level 3 will need to address the accountability implications of this transfer of authority, while Levels 1 and 2 remain consistent with current aviation practices, in which ultimate responsibility is assigned to humans.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

3.4. SESAR European ATM Master Plan

In parallel with the EASA AI Roadmap, it is worth considering the work in progress based on the new SESAR European ATM Master Plan. The document does not only define the objectives of funded research in civil aviation for the five year period running from 2025-2030. The plan also covers and explores the main methodological issues emerging to face new innovation challenges.

In this regard, it is interesting to note how SESAR is fostering a comprehensive and integrated reading of the AI levels in the taxonomy provided by EASA (SESAR, 2024, 10). The aim of this different approach is to converge on the level of automation achieved by the different applications considering the impact of the technological innovations on the main human cognitive and operational functions.

As shown in the figure below, the levels described by EASA are indeed associated with corresponding automation levels, explaining what human and AI tool capacities are at each level and the content of respective tasks and interactions.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

Figure 4. SESAR proposed new Levels of Automation Taxonomy and correspondence to EASA AI Levels (SESAR, 2024).

More specifically, these are the main features of each of the levels of automation considered and the expectations about AI contributions to the processes at issues.

- At Level 1A (EASA), AI acts as "**human augmentation**" with "**low automation**" (Level 0, S3JU), where human operators retain full decision-making and execution responsibilities.
    - **Expectations towards automation**: gathering and exchanging data; analysing and preparing all available information for the human operator.
    - **Expectations towards the human operator:** taking all decisions and implementing them (with or without execution support).
- At Level 1B (EASA), AI functions as "**human assistance**" with a focus on "**decision support**" (Level 1, S3JU) enabling humans to make informed decisions based on overviews of feasible options provided by the system.
    - **Expectations towards automation**: supporting the human operator in action selection by providing a solution space and/or multiple options.
    - **Expectations towards the human operator:** implementing the actions (with or without execution support).
- At Level 2A (EASA), AI facilitates "**human-AI cooperation**" as a "**resolution support**" system (Level 2, S3JU), where humans evaluate and refine solutions proposed by automation.
    - **Expectations towards automation**: proposing the optimal solution in the solution space and implementing the actions when due and if safe, acting under human direction.
    - **Expectations towards the human operator:** validating the optimal solution or coming up with a different solution and providing direction to the automation for implementation.
- At Level 2B (EASA), AI fosters "**human-AI collaboration**" at a "**conditional automation**" level (Level 3, S3JU), allowing humans to assign tasks to either the automation or themselves.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

- **Expectations towards automation**: selecting the optimal solution and implementing the respective actions when due and if safe, acting under human supervision.
- **Expectations towards the human operator:** supervising automation and overriding or improving the decisions that are not deemed appropriate.

- At Level 3A (EASA), AI operates in a "**safeguarded**" or "**confined" automation** mode (Level 4, S3JU), functioning autonomously but supervised by humans upon request or when operating outside its designated domain.
  - **Expectations towards the automation**: taking all decisions and implementing all the actions silently within the confines of a predefined scope, requesting the human operator to supervise its operation if outside the predefined scope.
  - **Expectations towards the human operator:** safeguarding automation behaviours.

- At Level 3B (EASA), AI operates **fully autonomously without human supervision** (Level 5, S3JU).
  - **Expectations towards automation**: acting without human supervision or safeguarding.
  - **Expectations towards the human operator:** no human operator required.

4. Industry standards on AI and on application of AI in aviation

The reader here will find an overview of the applicable industrial standards on AI and on application of AI in aviation.

4.1. Standards for management of AI safety

4.1.1. Standards for management of AI safety

At global level, the most important group developing consensus-based industry standards on AI is the Joint ISO/IEC Technical Committee JTC 1 and in particular its Sub-Committee SC 42, in fact tasked to develop international standards in the area of

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

AI and to provide guidance to other SCs of JTC 1 and in general to all IEC, and ISO committees developing AI applications.

In general ISO has developed several standards to help mitigate the risks connected to AI and maximise the benefits from AI applications.

This set of international standards includes ISO/IEC 22989, establishing terminology for AI and describing main concepts in the field of AI as well as ISO/IEC 23053, which establishes an AI and ML framework for describing a generic AI system using ML technology.

After release of the first iteration of this deliverable, SC 42[14] has achieved significant progress, publishing the following 10 international standards, whose scope includes also aviation AI applications:

1. ISO/IEC 5392:2024 Information technology – Artificial intelligence – Reference architecture of knowledge engineering
2. ISO/IEC 5339:2024 Information technology – Artificial intelligence – Guidance for AI applications
3. ISO/IEC 5338:2023 (December) Information technology – Artificial intelligence – AI system life cycle processes
4. ISO/IEC 25059:2023 (June) Software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Quality model for AI systems
5. ISO/IEC 42001:2023 (December) Information technology – Artificial intelligence – Management system
6. ISO/IEC 8183:2023 (July) Information technology – Artificial intelligence – Data life cycle framework
7. ISO/IEC 5259-1:2024 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 1: Overview, terminology, and examples
8. ISO/IEC 5259-3:2024 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 3: Data quality management requirements and guidelines
9. ISO/IEC 5259-4:2024 Artificial intelligence – Data quality for analytics and machine learning (ML) – Part 4: Data quality process framework

[14] The complete Standards by ISO/IEC-JTC 1/SC 42 Artificial intelligence catalogue is available at this link.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

10. ISO/IEC 24029-2:2023 (August) Artificial intelligence (AI) – Assessment of the robustness of neural networks – Part 2: Methodology for the use of formal methods

ISO/IEC 5259 Part 2 – Artificial intelligence – Data quality for analytics and machine learning (ML) – Data quality measures, is currently under development, with the Final Draft International Standard (FDIS) under consultation. Because the FDIS is the last stage of development of ISO standards, publication may be expected around the end of 2024.

In particular, ISO/IEC 42001 is a management system standard (MSS) guiding implementation of policies and procedures for the sound governance of an organisation in relation to AI, using the well known Plan-Do-Check-Act (PDCA) methodology, widely used in quality and safety management systems. Rather than looking at the details of specific AI applications, whose range is huge and today largely unpredictable, ISO/IEC 42001 provides a practical way of managing AI-related risks and opportunities across an organisation. This international standard is designed to be applicable across various AI applications and contexts, including aviation.

ISO/IEC 42001 therefore specifies requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organisations to ensure responsible development and use of AI systems.

ISO/IEC 42001 is the world's first published AI management system standard, providing guidance for this rapidly changing field of technology. It addresses the unique challenges AI poses, such as ethical considerations, transparency, and continuous learning. For organisations, it sets out a structured way to manage risks and opportunities associated with AI, balancing innovation with governance. Additional guidance on AI-related risk management is provided by ISO/IEC 23894.

These requirements can be implemented by organisations of any size involved in developing, providing, or using AI-based products or services, including commercial companies, relevant for public sector agencies as well as no-profit entities.

An AI management system, as specified in ISO/IEC 42001, is a set of interrelated or interacting elements of an organisation intended to establish policies and objectives, as well as processes to achieve those objectives, in relation to the responsible development, provision or use of AI systems.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

The ISO/IEC 42001 standard offers organisations the comprehensive guidance they need to use AI responsibly and effectively, even if the technology is rapidly evolving, through an integrated approach to managing any AI project, from risk assessment to effective treatment of these risks.

In addition, ISO TC 20 (aerospace) SC 16 (UAS) has established Advisory Group AG 6 on UAS Autonomy powered by AI Technology. The final AG 6 report should be available around the end of 2024. It may recommend development of international standards for use of AI in relation to drones by SC 16.

4.1.2. EUROCAE WG 114

On 04 June 2019, the European Organisation for Civil Aviation Equipment (EUROCAE) Council established the working group (WG) 114 to work jointly with SAE Committee G-34 on AI applied in safety critical systems.

The purpose of WG 114 is to establish common standards, guidance material and any related documents required to support the development and the certification or approval of aeronautical safety-related products based on AI technology.

The objectives of the working group are to:

- Develop a first technical report establishing a comprehensive statement of concerns versus the demonstration of conformity of AI-based products in relation to the regulatory requirements.
- Develop and publish EUROCAE Technical Reports for developing and certifying/approving AI technology embedded into and/or for use with aeronautical systems in both aerial vehicles and ground systems.
- Act as a key forum for enabling safe and appropriate adoption and implementation of AI technologies that are embedded in or interact with aeronautical systems.
- Enable all aviation stakeholders (e.g., aerospace, airport, ATC manufacturers) and regulatory agencies to consider and implement appropriate approaches to the certification/approval of AI-based, safety-related products.

Therefore, in 2021, EUROCAE has published ER-022 containing the statement of concerns around AI applications.

Currently WG 114 is working on:

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

- ER-027 on the taxonomy of AI used in aeronautical safety-related systems; and
- ED-324 on the process standard for development and certification or approval of aeronautical products implementing AI.

Although these two deliverables were planned to be respectively published at the end of 2023 and at the end of 2024, no draft has yet reached the level of maturity necessary for 'open consultation' which is the last stage of the EUROCAE development procedure.

Basically, in 5 years, WG 114 has produced only a statement of concern, but not yet usable documents.

Besides WG 114, which focuses on safety-related applications of AI, EUROCAE has published in April 2024 ED-235A containing Minimum Aviation System Performance Standards (MASPS) for Foreign Object Debris (FOD) detection systems. In this version A od ED-235, the possibility of applying AI to FOD detection is covered. This can be considered the first standard by EUROCAE covering AI, although for an application of low criticality.

4.2. Standards and tools for AI software development

EASA AMC 20-115D, using the performance-based approach, recognises the following standards published by the EUROCAE or by the US Radio Technical Commission for Aeronautics (RTCA) as MoC for SW development:

a) EUROCAE ED-12C and RTCA DO-178C on Software Considerations in Airborne Systems; and related supplementary standards listed here below
b) EUROCAE ED-215 and RTCA DO-330 on Software Tool Qualification;
c) EUROCAE ED-216 and RTCA DO-333 on Formal Methods for SW development;
d) EUROCAE ED-217 and RTCA DO-332 on Object- Oriented Technology and Related Techniques; and
e) EUROCAE ED-218 and RTCA DO-331 on Model-Based Development and Verification.

The cornerstone of ED-12C is the assignment to each SW component of a Design Assurance Level (DAL) based upon the contribution of SW to potential failure conditions as determined by the system safety assessment process by establishing how an error in a SW component relates to the system failure condition(s) and the severity of that

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

failure condition(s). In turn the DAL establishes the rigour necessary to demonstrate compliance with the standard.

ED-12C and equivalent DO-178C recognise five levels of SW DAL, which apply also to development of AI based software. None of the standards mentioned in this paragraph has been modified in the period between the first and this second iteration of the present document.

4.3. Standards and tools for AI software development

4.3.1. Easy Access part-IS

All IT systems are prone to cyber-security attacks, including those based on AI elements. According to EUROCAE ED-202A of 2014 a cyber-attack is constituted by the path, interface, and actions by which an attacker executes a cyber-attack.

Already on 01 July 2020 (EASA, 2020), EASA has introduced some provisions, at the level of 'soft rules' to reduce the probability and effects of cyber-attacks, among which AMC 20-42, whose scope was however limited to design of aeronautical products and related parts.

A more comprehensive approach is now in force, based on which all aviation organisations will be mandated, by 22 February 2026, to apply an Information Security Management System (ISMS) based on EC delegated Reg. (EU) 2022/1645 and Reg (EU) 2023/203.

The most significant event in this respect, occurred between the first and the second iteration of this deliverable, has been the issuance by EASA, on 12 June 2024, of so called Easy Access Rules (EAR) on Part-IS which facilitate stakeholders to connect rules with means of compliance and guidance material (EASA, 2024).

These EARs make reference in several paragraphs to industry standards. The most relevant are summarised herein in the following paragraphs.

4.3.2. Information security management system (ISMS)

A cornerstone of the legal provisions in Part-IS is the establishment of an Information Security Management System (ISMS) by all organisations involved in production of aeronautical products or their constituents or providing aviation services.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

Several GM in the EASA EAR recognise the international standard ISO/IEC 27001 which is a widely adopted standard for ISMS, specifying generic requirements for establishing, implementing, maintaining and continually improving an ISMS.

ISO/IEC 27001 also includes requirements for the assessment and treatment of information security risks. The requirements are applicable to all entities, regardless of type, size or nature. The conformity of an ISMS with the ISO/IEC 27001 standard can be certified by an accredited certification body. ISO/IEC 27001 is compatible with other management system standards (e.g., quality, safety, etc.) and so it can be part of an integrated management system, which allows an entity to operate a single management system that meets the requirements of multiple management system standards (e.g. quality, compliance monitoring, aviation safety, privacy, occupational health and safety, etc.).

ISO/IEC 27001 allows entities to define their own scope of audit and their own organisational risk appetite. This, in turn, leads to information security requirements that provide the ISMS with criteria for the acceptability of information security risks in line with the entity's risk appetite.

The requirements for an ISMS specified in the EC Regulations mentioned above are in most parts consistent and aligned with ISO/IEC 27001. However, the EC common rules introduce provisions specific to the context of aviation safety.

Therefore, if an ISO/IEC 27001-based ISMS is already operated by an entity for a different scope and context, it can easily be adapted and extended to the scope and context of EC Part-IS in a straightforward manner based on an analysis of the scope and possible gaps.

To take credit from ISO/IEC 27001 certifications to achieve compliance with Part-IS, aviation safety needs to be included in the organisational risk management, with the relevant risk acceptance level determined based on the EC Regulation applicable to the offered product of provided service.

Therefore, careful determination of the scope of the ISMS related to aviation safety risks is needed, as it might differ from the one related to the other organisational risks. To allow demonstration of compliance with Reg. (EU) 2023/203, careful delineation between aspects of the ISMS related to aviation safety risks and other organisational risks may be required.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

4.3.3. Information security risk assessment

Information security risk assessment is one component of ISMS.

Part-IS does not require the use of any specific information security framework, such as ISO, NIST or others to develop the risk assessment or in general to implement risk management. Each framework offers different benefits and none of these frameworks is perfect for an individual aviation organisation. Security risk management should hence be customised and tailored to meet the overall needs of the organisation as well as the specific need to consider aviation safety aspects.

Organisations whose information security frameworks have achieved industry certifications can provide this information as supporting artefacts; however, these organisations should show the applicability of the industry certification to the scope of Part-IS. EASA EAR suggests that general guidance on risk management, including risk assessment, can be found in ISO/IEC 27005 and ISO/IEC 31000 as well as NIST SP 800-30.

Organisations may also wish to in addition consider aviation-specific guidance as defined in the risk management chapter of the latest version of EUROCAE ED- 201A and, as appropriate to the specific operating environment, in the chapters of EUROCAE ED-204A, EUROCAE ED-205A and EUROCAE ED-206 covering risk management and including response and recovery from a cyber-attack.

The risk classification levels for potential occurrence of the threat scenario and severity of the safety consequences listed below may be applied; however, this does not prevent the organisation from developing additional intermediate categories if it deems this necessary for risk assessments. The organisation should specify and document the applied, entity-specific classification levels with an accurate qualitative or quantitative definition in terms of a range or interval of numerical values in order to enable a sufficiently calibrated, consistent estimation, evaluation and communication within the competent authority or with the interfacing entities.

The potential of occurrence of the threat scenario may be expressed as an interval of likelihoods including the duration of the observation. Supporting documentation and methods can be found in EUROCAE ED-203A, Chapter 3.6 which references the evaluation of the potential of occurrence of the threat scenario in the Security Risk Assessment of EUROCAE ED-202A.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

In fact, although EUROCAE ED-202A and EUROCAE ED-203A were originally developed for aircraft information security risk assessment, the generic principles developed in those documents can be adapted to other frameworks when deemed useful.

4.3.4. Competency of personnel for cyber-security

Several GM in the EASA EAR on Part-IS address personnel requirements, including for training.

A training programme on information security should start from the identification of the competence required by the personnel for each role, followed by the identification of the gaps between the existing competence and the required one.

To develop the list of competencies in terms of Knowledge, Skills and Attitudes (KSA), an organisation, instead of developing its syllabus from scratch, may use, as initial guidance, an existing cybersecurity competence framework such as the US NICE (National Initiative for Cybersecurity Education) based on the US NIST Cybersecurity Framework (NIST CSF).

However, it should be noticed that existing cybersecurity/information security competence frameworks such as the NICE typically focus primarily on the protection of standard information technologies.

Therefore, the list of competencies may need to be adapted to the aviation technologies or integrated with the processes used in the organisation.

The bridging of the identified gaps should be seen as the objective of the training programme, which should further include the scope, content, methods of delivery (e.g. classroom training, e-learning, notifications, on-the-job training) and frequency of training that best meet the organisation's needs considering the size, scope, required competencies, and complexity of the provided services.

Of course, as information security/cybersecurity evolves due to the rise of new threats, the organisation should periodically review the adequacy of the training programme.

4.4. Standards and tools for AI software development

The most relevant international standard for the taxonomy of automation/autonomy is Joint ISO/SAE PAS 22736:2021, already taken as a starting point for the JARUS activities on the matter.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

In addition, already in 1970, the American Society for Testing and Materials (ASTM) published Technical Report TR1-EB containing early proposals for a taxonomy of automation and autonomy. The latest edition of this TR1-EB of 2019, still provides a summary and proposed requirements framework for autonomous and highly complex systems. The TR was jointly prepared by ASTM Technical Committees F37 on Light Sport Aircraft, F38 on UAS, F39 on Aircraft Systems, and F44 on General Aviation aircraft. Its aim is to serve as a guide to development of other standards and practices associated with autonomous systems in aviation.

However, ASTM TR1-EB is not the most relevant on the subject either in JARUS or Europe, since it is largely aligned with mentioned ISO/SAE J3016.

In any case, in 2024 no consolidated and globally harmonised taxonomy of autonomy/automation, encompassing AI/ML as well, exists.

On this topic, EUROCAE WG 114 is developing ER-027 on the taxonomy of AI used in aeronautical safety-related systems. This WG, established through the ToR approved by the EUROCAE Council in 2019, is working jointly with SAE G-34, which offers the opportunity to align the taxonomy across the entire transport sector. Unfortunately no mature draft of ER-027 yet exists in August 2024. It is recommended that EASA suggests to EUROCAE WG 114 to develop a comprehensive taxonomy, including all the rows in the Table in Annex A to this document.

5. Conclusions and take-away messages

This second iteration of the analysis of the legal and regulatory framework for AI in aviation highlights important aspects, which can be useful for the upcoming and future developments of HAIKU, as well as of the UCs being examined in the project.

Firstly, it is notable that within just one year, there have been significant consolidations of the regulatory framework, both in the EU and abroad. The concept of trustworthy AI, its funding ethical principles, as well as the related technical and operational requirements are widely accepted, becoming the cornerstones of technological innovation in this field. Some cultural discrepancies can emerge concerning socially sensitive topics, particularly regarding the scope and strength of human rights protection. Despite these differences, there are common principles that guide the development and regulation of AI across various contexts, especially in terms of data quality, data governance, system accountability, human oversight, and fairness.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

This approach is the hallmark of the new EU AIA. In light of the mandate given to the EC and EASA, this regulation will extensively impact the whole aviation regulatory ecosystem. EASA anticipated a deep review of the current legislation and regulation, that will be gradually amended according to the specific sectoral needs regarding AI. Meanwhile the operators have to carefully follow the evolution of this review process, embracing a proactive approach to compliance. In order to maximise R&D efforts and investments, it is essential to develop a dynamic approach to the design, planning, development and deployment of these systems, progressively incorporating the rules and standards that can promote trustworthiness in practice.

According to the guidance provided by EASA, a comprehensive validation framework for AI-based solutions should take into account both technical and non-technical aspects. As outlined by the AI Trustworthiness building block, traditional technical KPAs on safety and security need to be enhanced with specific requirements and KPIs on AI assurance and AI safety mitigation risks. Moreover, technologies and concepts design have to be complemented by assessment focused on the human component, both considering human factors and ethics. Particular attention should be paid to AI categorisation, considering for each solution the proper level of automation in light of the corresponding level of risks and the quality of human-AI interactions. Ethics assessment should be carried out in parallel, since it can provide meaningful insights on societal and individual perception of the impacts of a given solution and facilitate the proactive approach to risk management, compliance and acceptability.

The effective achievement of these objectives is currently supported by the tools provided by EASA as deliverables of its AI Roadmap 2.0, as well as by the international standards that are gradually developed by several SDOs.

In general, a possible shortcoming is that the proliferation of different standards may lead to excessive compliance burdens, resulting in wasted resources and missed opportunities. In this regard, it is expected a closer coordination of the initiatives respectively carried out by EASA and EUROCAE, especially considering the timely achievement of ISO/IEC in terms of AIMS.

ISO/IEC indeed are devoting considerable effort to develop international standards for AI, which can have a large application even to aviation. Since EASA is working on a comprehensive regulatory strategy for the whole sector, it is expected the Agency will soon clarify their value and usability at the level of AMC/GM, in particular supporting Part-AI.OR. Considering the concurrent initiative EUROCAE WG 114 is carrying forward, it is also suggested to coordinate as much as possible general requirements to ISO/IEC

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

standards and limit WG 144 scope of action to provisions specific to aviation, complementary to ISO/IEC requirements.

Moreover, looking at the upcoming development and validation activities planned in HAIKU, it is worth to be noted that EASA does not prescribe any specific standard for SWAL/DAL in case of ATM/ANS systems, conversely recommending ED-12C for airborne software and for SW at aerodromes. It is hence proposed to use ED-12C throughout the HAIKU use cases, regardless of whether they focus on airborne or ground-based AI SW. Furthermore, given that an ISMS would not be required until 2026, and in any case not until TRL 8 or 9, it is recommended that the following steps be taken:

a) HAIKU use cases using inter alia aeronautical information consider ED-201A;
b) HAIKU use cases developing AI airborne applications consider ED-203A;
c) HAIKU use cases developing AI applications for ATM/UTM consider ED-205A; and
d) Any HAIKU partner intending to operationally implement the outcomes of the Project , should plan to comply with ISO/IEC 27005 for ISMS.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

6. References

China Academy of Information and Communications Technology (CAICT; 中国信息通信研究院; 中国信通院) & JD Explore Academy (京东探索研究院). (2021, July 9). **White Paper on Trustworthy Artificial Intelligence (可信人工智能白皮书)**. Georgetown University Center for Security and Emerging Technology. https://cset.georgetown.edu/wp-content/uploads/t0390_trustworthy_AI_EN.pdf

Commission Implementing **Regulation (EU) 2023/203** of 27 October 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards **requirements for the management of information security risks with a potential impact on aviation safety for organisations** covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 https://eur-lex.europa.eu/eli/reg_impl/2023/203/oj

Commission Delegated **Regulation (EU) 2022/1645** of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards **requirements for the management of information security risks with a potential impact on aviation safety for organisations** covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj

Council **Directive 85/374/EEC** of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning **liability for defective products** https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01985L0374-19990604 (Consolidated Text of 1999)

Devitt, K. S. (2018). **Trustworthiness of autonomous systems**. In Foundations of Trusted Autonomy (pp. 161-184). Springer.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

https://doi.org/10.1007/978-3-319-64816-3_9

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the **processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties**, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
https://eur-lex.europa.eu/eli/reg_del/2022/1645/oj

EASA. (2020, July 1). **ED Decision 2020/006/R - Aircraft cybersecurity**.
https://www.easa.europa.eu/en/document-library/agency-decisions/ed-decision-2020006r#:~:text=The%20objective%20of%20this%20Decision,board%20electronic%20networks%20and%20systems.&text=by%20following%20a%20proportional%20approach.

EASA. (2021, December 20). **EASA Concept Paper 'First usable guidance for Level 1 machine learning applications'**. Proposed Issue 01.
https://www.easa.europa.eu/en/newsroom-and-events/news/easa-releases-its-concept-paper-first-usable-guidance-level-1-machine-0#group-easa-downloads

EASA. (2023, May). **Artificial Intelligence Roadmap 2.0. Human-centric approach to AI in aviation**.
https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-roadmap-20#group-easa-downloads

EASA. (2024(a), March 6). **EASA Concept Paper: guidance for Level 1 & 2 machine learning applications.** Proposed Issue 02.
https://www.easa.europa.eu/en/document-library/general-publications/easa-artificial-intelligence-concept-paper-issue-2#group-easa-downloads

EASA. (2024(b), May 31). **EASA Machine Learning Application Approval Research Project**. EASA.
https://www.easa.europa.eu/en/newsroom-and-events/news/artificial-intelligence-easa-publishes-final-report-machine-learning

EASA. (2024, June 12). **Easy Access Rules for Information Security** (Regulations (EU) 2023/203 and 2022/1645) - Revision from June 2024. EASA.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-information-security-regulations-eu-2023203

EC, **Single Market Compliance System - SMCS**. European Commission. https://webgate.ec.europa.eu/single-market-compliance-space/home

EC. (2018, April 25). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS **Artificial Intelligence for Europe** (COM/2018/237 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

EC. (2020, February 19). **WHITE PAPER On Artificial Intelligence** - A European approach to excellence and trust (COM/2020/65 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1724163174272&uri=CELEX%3A52020DC0065

EC. (2022, September 28). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on **liability for defective products** (COM/2022/495 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495

EC. (2022, September 28). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting **non-contractual civil liability rules to artificial intelligence (AI Liability Directive)** COM/2022/496 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496

EC & DG for Research and Innovation. (2023). **Integration of social sciences and humanities in Horizon 2020** – Participants, budgets and disciplines 2014 - 2020 – Final monitoring report. EU Publications Office. https://data.europa.eu/doi/10.2777/075642

EP, EPRS, & Jochheim, U. (2021, September). **China's ambitions in artificial intelligence**. https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/696206/EPRS_ATA(2021)696206_EN.pdf

EP, EPRS & Szczepański, M. (2024, January). **United States approach to artificial intelligence**.

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf

EU. Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the **Digital Decade Policy Programme 2030**. https://eur-lex.europa.eu/eli/dec/2022/2481/oj

EU. (2024, February 26). **AI Pact | Shaping Europe's digital future.** Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/ai-pact

Executive Order on **Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence** (Executive Order on Artificial Intelligence) (88 FR 75191; 2023-24283 ed.). (2023, November 1). https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

FAA. (2024, July 23). **FAA Roadmap for Artificial Intelligence Safety Assurance**. https://www.faa.gov/media/82891

GAO. (2021, June 30). **Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities**. Government Accountability Office. https://www.gao.gov/products/gao-21-519sp

GAO. (2024, January 30). **Artificial Intelligence: GAO's Work to Leverage Technology and Ensure Responsible Use**. Government Accountability Office. https://www.gao.gov/products/gao-24-107237

HLEG-AI. (2019). **Ethics Guidance for a Trustworthy AI**. EU Publications Office. https://data.europa.eu/doi/10.2759/346720

HLEG-AI. (2020(a), September 14). **The Assessment List for a Trustworthy AI (ALTAI)**. EU Publications Office. https://data.europa.eu/doi/10.2759/002360

HLEG-AI. (2020(b), September 14). **Sectoral Considerations on the Policy and Investment Recommendations for Trustworthy Artificial Intelligence**. EU Publications Office. https://data.europa.eu/doi/10.2759/733662

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

ICAO. (2018). **Safety Management Manual**, Doc 9859 (4th ed.). https://skybrary.aero/articles/icao-safety-management-manual-doc-9859

ISO. (2023, December). **ISO/IEC 42001:2023 - AI management systems**. ISO. https://www.iso.org/standard/81230.html

Kabashkin, I., Misnevs, B., & Zervina, O. (2023, October 25). **Artificial Intelligence in Aviation: New Professionals for New Technologies**. Applied Sciences, 13(21), 11660. https://doi.org/10.3390/app132111660

Kaur, D., Uslu, S., Rittichier, K. J., & Durresi, A. (2022, January 18). **Trustworthy Artificial Intelligence: A Review**. ACM Computing Surveys (CSUR), 55(2), 1-38. https://doi.org/10.1145/3491209

Kirwan, B. (2024, April 9). **The Impact of Artificial Intelligence on Future Aviation Safety Culture**. Future Transportation, (4), 349–379. https://doi.org/10.3390/futuretransp4020018

Luong, N., & Arnold, Z. (2021, May). **China's Artificial Intelligence Industry Alliance Understanding China's AI Strategy Through Industry Alliances**. Georgetown University Center for Security and Emerging Technology. https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-Artificial-Intelligence-Industry-Alliance-1.pdf

Madhavan, R., Kerr, J. A., Corcos, A. R., & Isaacoff, B. P. (2020, September-October). **Toward Trustworthy and Responsible Artificial Intelligence Policy Development**. IEEE Intelligent Systems, 35(5), 103-108. 10.1109/MIS.2020.3019679. https://ieeexplore.ieee.org/document/9237282

NIST. (2023, January). **AI Risk Management Framework** | NIST. National Institute of Standards and Technology. https://www.nist.gov/itl/ai-risk-management-framework

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 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 (**Artificial Intelligence Act**)

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689

Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on **common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency**, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91.
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1139

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on **common rules in the field of civil aviation security** and repealing Regulation (EC) No 2320/2002
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008R0300

SESAR. (2024, April 22-23). **European ATM Master Plan Stakeholder consultation workshop pre-read material**.
https://www.sesarju.eu/sites/default/files/documents/events/ATM%20MP%20workshop%20pre-read%20material_2024.04.08_FINAL.pdf

WH-OSTP. (2022, October). **Blueprint for an AI Bill of Rights**: Making Automated Systems Work for the American People. The White House.
https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf

Yang, Z. (2024, January 17). **Four things to know about China's new AI rules in 2024**. MIT Technology Review.
https://www.technologyreview.com/2024/01/17/1086704/china-ai-regulation-changes-2024/

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332

This project has received funding by the European Union's Horizon Europe research and innovation programme HORIZON-CL5-2021-D6-01-13 under Grant Agreement no 101075332