Deliverable N. 7.1

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

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

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

Abstract

This deliverable presents the results of Task 7.1 "State of the art and regulatory landscape", as produced in the first 6 months of the HAIKU project. An updated version will be produced at M24 (August 2025).

In accordance with the approach adopted by the EU and the HAIKU Consortium, the document presents a comprehensive review of the current legal and regulatory state of the art for the introduction of Artificial Intelligence (AI) in aviation. In particular, in the first part of the document, the readers will find a general overview about the EU AI ethical and regulatory strategy e, from both a medium and long-term perspective. The second part comprises an exhaustive and detailed analysis of the current legal and regulatory framework for civil aviation, with insights about the application of the norms now in force to the AI systems development and deployment in this domain. These two parts are complementary, considering the general first, in order to come to the specific.

The legal and regulatory framework presented in the document confirms how a proactive and future-proof compliance approach may substantially benefit the development and deployment of AI systems in and for aviation. For this reason, the document includes also a set of operational tables on EU AI Legislative Initiative Requirements, to be used in the design and validation of the HAIKU use cases as guidelines to ensure the consistency of the proposed operational concepts and AI-powered technologies with the legal and regulatory framework.

Information Table

Deliverable Number	7.1
Deliverable Title	State of the art in safety, human factors, and security (SHS) assurance processes in aviation
Version	1.0
Status	Final
Responsible Partner	Deep Blue
Contributors	Eurocontrol
Contractual Date of Delivery	28.02.2023
Actual Date of Delivery	28.02.2023
Dissemination Level	Public

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
0.1	25.10.2022	Draft	F. Tomasello (DBL) E. Spiller (DBL) N. Giampaolo (DBL) P. Lanzi (DBL)	ToC
0.2	27.01.2023	Draft	F. Tomasello (DBL) E. Spiller (DBL) N. Giampaolo (DBL) P. Lanzi (DBL)	Initial version
0.3	07.02.2023	Draft	F. Tomasello (DBL) E. Spiller (DBL) N. Giampaolo (DBL) P. Lanzi (DBL)	Internal review
0.4	24.02.2023	Consolidated Draft	S. Pozzi (DBL) V. Arrigoni (DBL) B. Kirwan (ECTL) J. Hird (ECTL) F. Tomasello (DBL) E. Spiller (DBL) N. Giampaolo (DBL) P. Lanzi (DBL)	Internal review
1.0	27.02.2023	Final version	F. Tomasello (DBL) E. Spiller (DBL) N. Giampaolo (DBL) P. Lanzi (DBL)	Submission

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

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 deliverable presents the results of Task 7.1 "State of the art and regulatory landscape", as produced in the first 6 months of the HAIKU project. In line with the purpose of the task, it presents the current ethical and legal framework and a State-of-the-Art Review (SOAR) in regulations and consensus-based industry standards for the introduction of Artificial Intelligence (AI) in civil aviation. In particular, the analysis includes considerations of 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. An updated version of this deliverable will be produced at M24 (August, 2025) in order to take into account possible evolutions of the SOAR for regulations and standards that may emerge during the project life cycle.

In order to keep it focussed on legal, ethical and regulatory landscape, this deliverable does not include information about the best practices concerning safety, human factors, and security (SHS) assurance processes in aviation. This activity will be reported in 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

This deliverable is divided in 17 parts: 9 sections (including the present introduction) and 8 Annexes (including references). This editing choice is motivated by two complementary needs: on the one hand, the comprehensiveness of the analysis; on the other, the accessibility of the contents for operative purposes.

In the main **Sections**, numerated from 1 to 8, the reader will find a discursive overview of the different issues here addressed. At the end, **the reader will have a general overview of the current legal and regulatory framework for the use of AI in civil aviation and relevant recommendations for the design of the use cases of the HAIKU project**. Due to the nature and scope of the project, the analysis particularly focuses on EU law.

The SOAR is structured as follows:

1. **Introduction**, with the scope of the document and its structure;
2. **Background of trustworthy AI,** which highlights some essential starting points for an easy understanding of the approach of the European Union (EU) to and the pillars of its AI Strategy, in general and for aviation purposes;

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. **Ethical framework for using AI in aviation,** which explains the role of ethics and its normative function in the EU AI Strategy, also in light of the clarifications provided by EASA for the development and use of these technologies in aviation[1];
4. **EU legal framework for the use of AI**, which provides an overview of the EU AI Legislative Initiative, analyses the rationale informing the proposals for the EU AI Act, the EU AI Liability Directive and the revision of the Product Liability Directive (PLD) for addressing the new legal issues related to AI development, deployment and putting on market and into service;
5. **EU aviation legal framework for AI**, which analyses the current EU aviation law, pointing out and analysing the norms and requirements applicable to AI solutions;
6. **Provisions of other aviation authorities in the world**, which provides some comparative insights about the regulatory strategies considered and/or adopted by non-EU regulatory authorities for the use of AI in aviation;
7. **Industry standards on AI and on application of AI in aviation**, which spreads light on the relevant industry standards for the applications of AI in aviation, aligning the project research purposes with the practices and expectations of the industrial domain;
8. **From theory to practice**, which provides methodological and operational insights about the use of the checklists and the tables provided in the Annexes.
9. **Conclusion and recommendations**, explains the operational value of the deliverable and the contribution of this SOAR to the successful development of the project. In particular, here the reader will find operative "how to" questions aimed at facilitating a targeted and quick access to the previous sections and the use of the following Annexes.

In this regard, afterwards, the reader will find the **Annexes**, ordered from the letters A to H. These **parts mainly have an operative purpose and provide to readers useful tools to facilitate the navigation of the document and the design of the use cases in practice.**

After the list of acronyms [Annex A] and the definitions [Annex B], the contents are arranged as follows and can be jointly read with the discourse carried on in the related sections of the deliverable:

- **Annex C** provides an in-depth analysis of the EU AI Ethic Framework, including a plain explanation of the fundamental principles and the related ethics requirements. Here, you also find a customised version of the EU Auto-assessment List for Trustworthy AI (ALTAI) adapted to the specific features of HAIKU use cases [see: § 3.2];

[1] The analysis presented in this document mainly relies on the EASA Artificial Intelligence Roadmap 1.0 [11] and Concept Paper "First usable guidance for Level 1 machine learning applications" (Issue 01) [13]. The Consortium also takes into consideration the insights provided by EASA on the Concept Paper "Guidance for Level 1 & 2 machine learning applications" (Proposed Issue 02), officially published on Feb. 24th, 2023. However, a more detailed analysis of this last document will be provided in the second iteration of D7.1, also in light of the ongoing consultation.

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

- **Annex D** presents a taxonomy of automation/autonomy classification criteria adopted by EASA and JARUS. It also provides material insights for the correct assessment of human oversight on AI in aviation scenarios [see: § 3.3];
- **Annex E** reports the detailed analysis of the development and compliance requirements proposed by the AI Act, the AI Liability Directive, and the PLD.R. The outline is arranged through thematic operative tables to be used for use cases design and preliminary assessment of compliance [see: § 4];
- **Annex F** describes the regulatory and technical requirements provided by EU aviation law and regulation, also explaining how they shall be applied to AI systems [see: § 5];
- **Annex G**, eventually, reports the specific industrial standards applicable to AI in aviation [see: § 7].

The complete list of references is available in the Annex H.

2. Background of trustworthy AI

What is Artificial Intelligence (AI)? Many different definitions of AI can be found in literature as it is frequently intended in a multifaceted way, including computational models, technologies and systems.

In structuring the legal and ethical framework and the SOAR on regulations and standards, we faced the problem of having no univocal definition of AI to refer to, and decided to adopt the definition provided by the High-Level Expert Group on AI (HLEG) AI and the European Commission (EC). In this regard, «AI refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)» [91, p. 1].

Among the myriad possible AI applications, aviation is one of the most challenging, because of the inherent very rapid required response times and because of the potentially catastrophic consequences of a possible aviation accident.

According to the EU AI Strategy [47, p. 13], an environment of trust and accountability around the development and use of these technologies is needed. AI development and deployment has to be aligned with the values of respect for human dignity, freedom, democracy, equality and with the rule of law and respect for human rights, stated by the Article 2 Treaty of the European Union (TEU). In addition, these systems also must respect the ethical principles and the fundamental rights protected by the European Convention of Human Rights (ECHR) and the EU Charter of Fundamental Rights (EUCFR).

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

Against this background, a trustworthy AI should be lawful, ethical and robust.

More specifically, an AI-powered system is considered lawful if the system design, implementation and use are compliant with all applicable laws and regulations, including but not limited to those on aviation safety and cyber-security. Furthermore, AI is assumed to be ethical if the technology is able to ensure adherence to ethical principles and values throughout the system's entire life cycle. Eventually, AI should also be robust, both from a technical and social perspective, which means being able to prevent and avoid unintentional harm caused by AI systems. Each of these three components is necessary but, if taken in isolation, not sufficient for the achievement of trustworthy AI. Therefore the three factors should work in a complementary way, mutually harmonised and with some overlap in their operation.

This is the perspective assumed by the authors while producing the present deliverable.

3. Ethical framework for using AI in aviation

3.1. A brief introduction to the role of AI ethics in the EU

As well documented by the many studies commissioned by EU Institutions, AI systems have **disruptive intrinsic features** that challenge the current legal state of the art. AI-powered tools indeed may present levels of complexities and autonomous behaviours that are not fully predictable by a human, especially when based on non-deterministic software. Moreover, AI behaviour can continuously adapt according to the surrounding environment and machine performance.

In particular, the **scalable and increasing level of autonomy of AI** represents the most disruptive feature of this technology compared with previous deterministic software. The latter in fact, contrary to AI, always produces the very same output when given the same input no matter how many times it is run, while the output of AI depends on the environment and on the 'experience' of the system.

The increased autonomy of AI systems leads to potential concerns for safety, security and interaction with human operators. On the one hand, the main causes of safety risks generated by complex software or algorithms are qualitatively different from risks caused by physical products. On the other hand, under the current legal framework, safety and liability requirements are calibrated according to ex-ante conformity assessment procedures which are mainly conceptualised for products that are 'predictable' in time after deployment.

This consolidated regulatory approach, however, does not contain specific provisions for products that are possibly subject to evolution during their lifecycle. This is a common feature of several AI systems that are subject to considerable change after their first placement on the market [56, p. 14]. This is the reason why the failure or abuse of autonomous systems potentially have cascading effects that eventually may further impact several fundamental rights and values. Indeed, the use of AI may violate

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

human dignity, personal autonomy and individual liability when discretion exercised by a machine reduces the role of human actors and decisions to the secondary agents of a technology-led interaction [56, p. 17].

In other words, these specific characteristics of AI systems challenge the EU legal framework inspired by the **principle of technological neutrality (or agnosticism)**[2] since they are qualitatively different from previous technological advancements. This is the reason why existing legislation can be difficult to apply and to be adapted to AI solutions. Furthermore, as many other countries, the EU still does not have a specific AI regulatory framework [57].

Notwithstanding this gap, **AI systems do not operate in a lawless world** [92, p. 6]. The analysis of the rules applicable to these technologies thus needs to consider the different normative sources available, including legal provisions, consensus-based voluntary standards and ethical references. Approaching the regulatory issues related to the development, deployment and use of these technologies, the involved stakeholders should be compliant with the already existing applicable legislation. They have to proactively interpret the prerogatives and responsibilities provided by the regulatory literature, taking into account the specific features of the AI-powered solutions and the material consequences that may arise from their use in operations.

In this transition period towards a stable AI legal framework, **ethics principles can promote a consistent and values-oriented interpretation of existing legislation**. Of course, ethical normativity does not have a binding or compulsory force of law. **Since any new provisions would most probably be based on the same ethical principles, technological and procedural design that will take into account these principles from the early stage of development and deployment implicitly embrace a future-proof compliance strategy** [92, pp. 9 ff.]

In conclusion the remainder of this document is based on two preliminary assumptions:

a) Even today AI systems do not operate in a lawless world, since existing provisions do apply;
b) The ethics principles valid today will continue to be valid in the foreseeable future.

Consistently with the method suggested by the EU Institutions [62], **the regulatory assessment conducted by HAIKU will follow this proactive approach**, facilitating a clear and (possibly) future-

[2] Technological neutrality is usually intended as a principle aimed to take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology. This is also intended as the freedom of individuals and organizations to choose the most appropriate and suitable technology for their needs. Products, services or regulatory frameworks taking into account the principle of technology neutrality neither impose nor discriminate in favour of the use of a particular type of technology. More details are available at [36][10] rec. 18 and [11][85].

As later explained , this principle in aviation law is known as technological agnosticism. This intends the regulatory approach that has a neutral (or agnostic) understanding of the technological factors. In other words, the regulatory act shall define the performance requirements with no constraints about the technologies that should be used to achieve the objectives prescribed by law. For the disambiguation of these two concepts, please, see the definitions provided in Annex B -Annex B.

proof interpretation and application of legal and ethics requirements for AI systems. In particular, the legal analysis of the regulatory provisions applicable to these technologies will take into account the different normative sources available, including legal and ethical references [47, p. 3] [52, p. 2].

Looking at the specificities of this project and its purposes, one needs first to consider the obligations and duties stated by EU, national and international law, within a comprehensive framework. Additionally, horizontally applicable general legislation should be contextualised and interpreted in relation to domain-specific rules and standards for the use of AI in aviation. As a consequence, this document also considers the recent EC legislative proposals [56][62][64], oriented to innovate the current SoA, through the establishment of a solid EU legal and regulatory framework according to the guidelines provided by the EU Commission and European Parliament [55][52][63][66].

It is noteworthy that the acts composing the new general AI legislation proposed by the EC would not be directly applicable to aviation. However, these general requirements will inform and orient the interpretation of the sector legislation for all the open issues concerning the application of AI in aviation.

As a final note, the authors of this document are well aware of the different binding force of the selected references.

3.2. EU AI general ethical framework

3.2.1. The normative value of AI ethics

As previously mentioned, the EU embraces a three-pronged approach to a Trustworthy AI, aimed to foster the ethical, lawful and robust development of this family of technologies.

According to this understanding, ethics represents a prominent aspect of the EU approach to AI. Ethics guidelines – as well as the related principles and requirements – are a core pillar for developing a human-centred understanding of AI. These may contribute to shape «not only technology's inherent properties, but also the qualities of the socio-technical systems involving AI applications» [91, p. 5].

The Consortium assumes that ethics should have a integrative and adaptive normative value. On the one hand, looking at legal principles, at least in the EU, we can assume the minimal starting point for any future strategy of compliance will rely on the core values of the European fundamental rights tradition (following the European Convention of Human Rights (ECHR) and The Charter of Fundamental Rights of the European Union). On the one hand, from a strictly legal standpoint, well-established compliance requirements explicitly prescribe what is normative binding, at least looking at the past of the technologies at issue. While technology gradually evolves, ethics shall fill the gaps between general legal principles and specific compliance standards suggesting what may happen in terms of shaping and guiding the development of AI regulation.

In this regard, ethical guidelines – especially if officially endorsed by official accredited institutions, may

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

help all AI stakeholders involved in designing, developing, deploying, implementing, using or being affected by AI to adopt a proactive approach.

3.2.2. The High-Level Experts Group on AI

In its Communication of 25 April 2018 and 7 December 2018 [48], 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.

3.2.3. AI Ethics Principles

In its Ethics Guidelines, the HLEG AI identifies the AI ethics principles mirroring and relying on the main fundamental rights families. Its scrutiny, in particular, focused on (1) the respect for human dignity, (2) freedom of the individual, (3) respect for democracy, justice and the rule of law and (4) equality, non-discrimination and solidarity (including the rights of persons at risk of exclusion) and (5) citizens’ rights [91, p. 10].

On these premises, the Guidelines outlined the following four fundamental principles: (1) respect for human autonomy, (2) prevention of harm, (3) fairness and (4) explicability [more details: Annex C].

Many of these principles are to a large extent already reflected in existing legal requirements for which mandatory compliance is required. However, in this transition time, these principles should inspire the interpretation of the existing laws and policies Moreover, these imperatives «can inspire new and specific regulatory instruments, can help interpreting fundamental rights [N.o.A. related issues] as our socio-technical environment evolves over time, and can guide the rationale for AI systems’ development, deployment and use – adapting dynamically as society itself evolves» [91, p. 11].

3.2.4. AI Ethical requirements

To transpose these principles into concrete features and directly applicable rules, the HLEG AI also suggested a series of general requirements aimed at outlining the minimal compliance level of AI systems with the mentioned ethical expectations.

Basically, the HLEG AI as well as the EC opted for a systematic understanding of the different ethical and socio-technical issues, including both individual and societal aspects [more details available in Annex D, while ALTAI references in the related tables]. Briefly, the list includes:

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

- **human agency and oversight,** including fundamental rights, human agency and human oversight [Table D. 1];
- **technical robustness and safety**, including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility [Table D. 2];
- **privacy and data governance**, including respect for privacy, quality and integrity of data, and access to data [Table D. 3];
- **transparency**, including traceability, explainability and communication [Table D. 4];
- **diversity, non-discrimination and fairness**, including the avoidance of unfair bias, accessibility and universal design, and stakeholder participation [Table D. 5];
- **societal and environmental wellbeing**, including sustainability and environmental friendliness, social impact, society and democracy [Table D. 6];
- **accountability**, including auditability, minimisation and reporting of negative impact, trade-offs and redress [Table D. 7].

The respect of these requirements has to be continuously evaluated and addressed during the AI systems' life cycle.

For the purposes of the HAIKU project, these requirements have to be taken in to consideration over the whole lifecycle of the digital assistance tools, since the early stage of the design. From a practical perspective, the following questions may help Use Cases leaders and stakeholders to identify and address the ethical consequences of their technical and organisational choices.

3.2.5. The HLEG Assessment List for Trustworthy AI (ALTAI)

Based on the feedback received, the AI HLEG presented the final Assessment List for Trustworthy AI (ALTAI) in July 2020. ALTAI is a practical tool that translates the Ethics Guidelines into an accessible and dynamic (self-assessment) checklist. The checklist can be used by developers and deployers of AI who want to implement the key requirements in practice. The HAIKU project will use ALTAI in a customised version, calibrated on the needs of civil aviation AI applications [Annex D].

3.3. EASA Guidelines for AI in civil aviation

3.3.1. From the HLEG Ethics Framework to EASA Level 1 Guidelines

Automated technologies are a major opportunity for the aviation industry but come also with a significant number of challenges with respect to trustworthiness, safety and security. EU/EASA have produced several technology-agnostic and performance-based rules and AMC/GM, which are also applicable to AI. None of them however, is yet sufficiently detailed for concrete guidance on AI applications in aviation.

Therefore, in addition, EASA released in 2020 [11] a roadmap and the first set (Level 1) of usable guidelines to guide aviation stakeholders in solving some of the main challenges linked to this disruptive technology.

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

These guidelines apply to any system developed using ML techniques or incorporating ML algorithms, and are intended for use in safety-related applications or for applications related to environmental protection covered by the Basic Regulation 2018/1139 [9].

Specifically the guidelines are divided in the following categories [13]:

a) Trustworthiness analysis, including human oversight;
b) Learning assurance;
c) AI explainability;
d) AI safety risk assessment; and
e) Organisations.

3.3.2. Trustworthiness

EASA states that as the first step the involved aviation organisation should identify the operational environment in which the AI-based (sub)system will be used. In light of this, the objectives of the trustworthiness analyses refer to the identification of the high-level function(s)/task(s) to be performed by the (sub)system either in interaction with the human or in autonomy.

To support compliance with the objectives of the AI trustworthiness guidelines, a detailed ConOps detailing precisely how the system will be operated is expected to be developed by the organisation, focusing on the definition of the Operational Design Domain (ODD) and on the capture of specific operational limitations and assumptions.

In particular, the guidelines recommend to the aviation organisations to perform an ethics-based trustworthiness assessment for any AI-based (sub)system developed addressing the questions from the EU Commission Assessment List for Trustworthy AI (ALTAI)[93].

In the safety and security assessment aspects of the trustworthiness analysis, the following objectives are considered in the guideline. The suggested approach, in this regard, can be summarized as follow:

- define the metrics to evaluate the AI/ML component performance and reliability.
- estimate the generalisation gap. The output of this objective may then be fed into the system safety assessment.
- carry out a safety support assessment for any change in the functional (sub)system embedding a component developed using AI/ML techniques or incorporating AI/ML algorithms.

The present EASA guidelines build on the ethics assessment on the HLEG.

Furthermore, the applicant should demonstrate to the competent authority to comply with national and EU data protection GDPR and assess the environmental impact of the AI-based (sub)system.

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

3.3.3. Human oversight

As anticipated, the EC High-Level Expert Group (HLEG) on AI, released in 2019 a set of Ethics Guidelines [93] for Trustworthy AII. The HLEG further 'operationalised' the guidelines by means of a set of seven gears and sub-gears which included 'human agency' and 'oversight'. The term 'human agency' refers to the decision authority which is delegated to the human (e.g. pilot or ATCO) supported by AI applications.

A taxonomy of the automation levels and of the human role is contained in the EASA guidance for Level 1 machine learning applications [13] and JARUS taxonomy on the matter, is reproduced in Table C. 1 and Table C. 2.

EASA AI Roadmap AI Level	Function allocated to the system to contribute to the high-level task	Role of Human
Level 1A Human augmentation	Automation support to information acquisition Automation support to information analysis	Human in Command (HIC): all decisions are taken by the human
Level 1B Human assistance	Automation support to decision-making	HIC
Level 2 Human-AI collaboration	Overseen and overridable automatic decision-making Overseen and overridable automatic action implementation	Human-in-the-Loop (HITL) Human may override any automatic action
Level 3A More autonomous AI	Overridable automatic decision-making Overridable automatic action implementation	HITL
Level 3B Fully autonomous AI	Non-overridable automatic decision-making Non-overridable automatic action implementation	Human-on-the-Loop (HOTL).

Table 1 -EASA, Levels of Automation/Autonomy

The boundary between level 2 and level 3A lies in the level of oversight that is performed by the human end user on the operations of the AI-based system. A strong prerequisite for level 2 is the ability for the human end user to possibly intervene in every decision-making and/or action implementation of the AI-based system.

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

Conversely, in level 3A applications, the ability of the end user to override the authority of the AI-based system is limited to cases where it is necessary to ensure safety of the operations (e.g. an operator supervising a fleet of UAS, terminating the operation of one given UAS upon alerting).

The HLEG produced an Assessment List for Trustworthy Artificial Intelligence (ALTAI) [93] including a set of questions to self-assess necessary oversight measures through governance mechanisms. This set of questions has been expanded and adapted to aviation in Annex 5 of the EASA guidelines [13].

These questions should be answered either by the organisation (e.g. aircraft operator, aerodrome operator, ANSP, etc.) or by the human using the AI application during operations (e.g. pilot, ATCO, etc.). Furthermore, these questions should be answered by the developers of HAIKU use cases or, after the project conclusions, by the organisation intending to introduce AI applications into its operations. In fact, the legal actor overseeing the AI-based system could vary during the life cycle (e.g. designer, operator or service provider, human end user).

3.3.4. Learning assurance

The learning assurance has the main aim of providing guarantees that the AI training performed on sampled data sets can be generalised and maintain adequate performance when fed with yet unseen operational data.

The objective is to gain confidence at a sufficient level that a ML application supports the intended functionality, thus opening the ‘AI black box’ as much as practicable. In this light, the first objective is to describe the proposed learning assurance process.

Secondly, the applicant should describe the system and subsystem architecture, to serve as reference for related safety (support) assessment and learning assurance objectives.

Finally, each of the captured requirements should be validated, evaluating the performance and robustness of the trained model based on the test data set and of course the process of model verification should be documented, including the final results.

EASA hence recommends a new concept of ‘learning assurance’ to provide novel Means of Compliance. The objective is to gain confidence at an appropriate level that an ML application supports the intended functionality, thus opening the ‘AI black box’ as much as practicable.

> **Learning assurance**: All of those planned and systematic actions used to substantiate, at an adequate level of confidence, that errors in a data-driven learning process have been identified and corrected such that the system satisfies the applicable requirements at a specified level of performance, and provides sufficient generalisation and robustness guarantees.

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

To illustrate the process, EASA proposes to modify the typical development assurance V-cycle to incorporate the ML concept. This would result in a new learning assurance process steps, which can be represented in a W-shaped process outline:

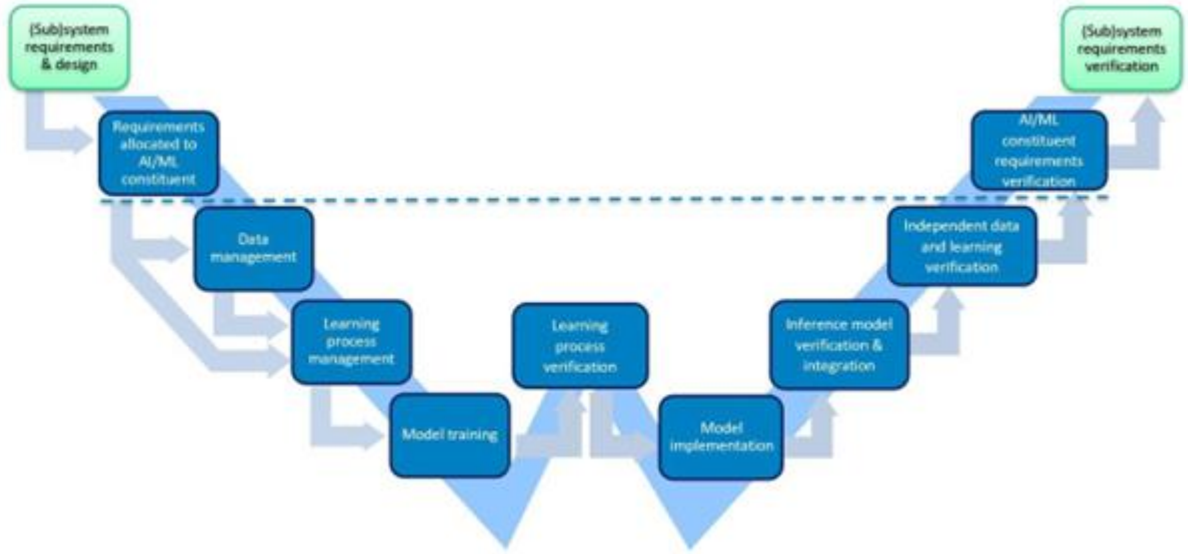
(Sub)system requirements & design
Requirements allocated to AI/ML constituent
Data management
Learning process management
Model training
Learning process verification
Model implementation
Inference model verification & integration
Independent data and learning verification
AI/ML constituent requirements verification
(Sub)system requirements verification

Figure 1– EASA, Guidelines for AI in Civil Aviation, Learning Assurance

Basically, the safety and security assessments would still be carried out based on existing rules (e.g., CS 25.1309 for applications on large aeroplanes), from which the Design Assurance Level (DAL) would emerge. On the right branch of the diagram the verification would still be based mainly on AMC 20-115D [8] for aviation products and equipment (and hence on EUROCAE ED12C [20]).

But at the bottom of the model, new MoC needs to be developed, in fact for verification of the learning process.

3.3.5. AI Explainability

Increasing the levels of automation of the AI-based systems may result in a reduction of operator awareness of the logic leading to the automated decisions or actions. Trust is considered to be essential and critical to the general acceptability of AI-based systems. Therefore, in the context of operations, in order to maintain the trust and ensure an adequate efficiency of the interaction, there will be a need for the AI-based systems to artificially provide explanations with regard to their decisions and actions. In this perspective, the guidelines specify 1) to identify the list of humans that are intended to interact with the AI-based (sub)system, at any stage of its life cycle, together with their roles, their responsibilities and their expected expertise; 2) to identify which task(s) the humans are intended to perform in interaction with the AI-based (sub)system, as well as the task allocation pattern; 3) to specify the set of necessary explanations to be provided to the human and 4) to ensure the validity of the specified explanation, based on actual measurements (e.g., monitoring) or on a quantification of the level of uncertainty.

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

3.3.6. Safety risk assessment

For some AI/ML applications, it could be impractical to fully cover all the objectives defined in the explainability and learning assurance building blocks of the EASA guidelines. Some objectives, therefore, would result in a residual safety risk that may be accommodated by implementing some mitigations of the safety risk, possibly through procedures. In this regard, the guidelines suggest determining whether the coverage of the objectives associated with the explainability and learning assurance building blocks is sufficient or if an additional dedicated layer of protection, called hereafter Safety Risk Mitigation (SRM), would be necessary to mitigate the residual safety risks to an acceptable level and to establish SRM means, taking into account that safety risks may emerge also from security threats.

3.3.7. Organisations

Finally, all involved aviation organisations might need to introduce adaptations in order to ensure the adequate capability to meet the objectives defined within the AI trustworthiness building blocks and to maintain the compliance of the organisation with the rules on safety, security, privacy and liability summarised in this document.

For this, the organisation should review its processes and adapt them to the introduction of AI technology. Secondly, the organisation should implement a data-driven 'AI continuous safety assessment system' based on operational data and in-service events.

3.3.8. Concluding remarks

In conclusion, the EASA guidelines cover five building blocks: trustworthiness analysis, learning assurance, explainability, safety risk mitigation and organisations. These guidelines present a first set of objectives for Level 1 Artificial Intelligence ('assistance to human'), to anticipate future EASA guidance and requirements for safety-related machine learning (ML) applications. The guidelines aim at guiding applicants when introducing AI/ML technologies into systems intended for use in safety-related or environment-related applications in all domains covered by the EASA Basic Regulation (Regulation (EU) 2018/1139 [83]). At the moment, the guidelines cover only an initial set of AI/ML techniques and will be enriched with more and more advanced techniques, as the EASA AI Roadmap is implemented.

For the HAIKU project this leads to:

a) identify the DAL for each application developed by the use case, based on a safety assessment;

b) use as a benchmark for the software documents to be collected AMC 20-115D [8] and related EUROCAE ED-12C [20]; and

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

c) in the second iteration of this document, develop proposals for future EASA/EUROCAE MoC enabling involved aviation organisations to reach HAIKU's target TRL, and later TRL 8 or 9, after and beyond the HAIKU Project.

Take away message

Ethics can provide a helpful contribution to the development of AI systems, especially if considered since the early stages of the design process. Ethics principles represent and codify the social expectations related to the good use of AI, in a general and long term perspective. Therefore, the use of the ethics principles and requirements defined by the HLEG can assure a future proof compliance with the current and future legislative and regulatory framework. In particular, the use of ALTAI, as customised for the HAIKU purposes, can lead to a more aware design of the use cases and the related validation scenarios.

4. EU legal framework for the use of AI

4.1.The current state-of-the-art on the EU AI regulation

Although law and regulation are the essence of one of the three funding pillars of EU strategy for a Trustworthy AI, at present the EU does not have a specific set of rules for AI yet. The absence of clear and specific rules at the EU level has induced many Member States to act on their own initiatives, approaching case by case the most relevant issues that emerged within their national jurisdictions. This approach results in a fragmented and uncertain legal framework that may create obstacles to investments and increase the costs of business related to AI. Unharmonized levels of protection of fundamental rights and uncertainty about legal remedies and compensations in case of harm may fuel mistrust and discourage people's acceptance of these technologies.

4.2. The legal basis for EU Legislation on AI

In light of the above, the EC has launched prominent initiatives to address the legal uncertainty related to the unclear regulation of AI. The whole package of measures relies on the Article 114 of the Treaty on Functioning of the EU (hereinafter: TFEU) as «measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market» (Article 114(1) TFEU). Consistently with the intents expressed by the White paper on Artificial Intelligence, the EU follows specific objectives in regulating AI [55, p. 3][63, p. 2]:

- ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values;
- ensure legal certainty to facilitate investment and innovation in AI;

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

- enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems;
- facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

4.3. The EU AI Legislative Initiative and the proposals under discussion

Pursuing these objectives, the EC has presented three new legislative proposals as pillars of the new normative architecture, namely:

- the Artificial Intelligence Act (hereinafter also: AI Act), a proposal for a Regulation laying down harmonised rules on artificial intelligence and amending certain union legislative acts (COM(2021) 206 final) [55];
- the Artificial Intelligence Liability Directive (hereinafter also: AI Liability Dir.), a proposal for a directive adapting non-contractual civil liability rules to artificial intelligence (COM (2022) 496 final) [63]
- the renewal of the Product Liability Directive (hereinafter also: PLD.R), thereby still a proposal for a directive on liability for defective products (COM(2022) 495 final) [61].

The titles of these three documents emphasise how, in the understanding of the EU legislators, safety and liability in AI regulation are the two sides of the same coin. They apply at different moments but reinforce each other. While rules to ensure safety and protect fundamental rights will reduce risks, they do not eliminate those risks entirely. Where such risks materialise, damages may still occur, and liability rules provide clear apportionment standards and ensure compensation [53][93][10]. The principles and rules established by these documents for the regulation of AI, of course, are not binding yet, since all three proposals are at an intermediate stage of the law-making process. Nonetheless, even though specific legal requirements are still subject to possible fluctuations, the core milestones outlined by these proposals may facilitate a proactive approach to address the legal issues concerning innovative solutions powered by AI.

This is the reason why the Consortium, in accordance with the approach suggested by the EU and HLEG AI, decided to take into careful consideration the insights provided by these normative resources. In particular, the rules provided by the three proposals here will be used to promote a future-proof design of AI systems and practices, anticipating and addressing possible future safety and liability issues from the early stage of the design. Moreover, the concepts and definitions outlined within this early AI-specific legal framework will then be used to address potential interpretative issues in aviation law, facilitating proactive compliance with sectoral safety standards [for more details, see: Annex 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

It is important to stress that this approach will not detract from traditional interpretative criteria. Where available, special law repeals general laws.

The following paragraphs will highlight the principles and rules taken into account to establish the legal framework adopted for the purposes of the HAIKU project.

4.4.EC proposal for an AI Regulation (AI Act)

4.4.1. The legal definition of AI and the new rules for high-risk AI systems

The first relevant contribution provided by the AI Act concerns the introduction of a legal definition of AI for the purposes of EU law. In light of this, even though different (and more comprehensive and/or specific) definitions of AI are available [58], only the legal one will be considered to define the material scope of the AI Act and the technologies affected by its principles and rules.

According to Article 3(1) of the proposal,

> «‘**artificial intelligence systems’ (AI systems)** means software that is developed with one or more of the techniques and approaches listed in Annex I [e.g., machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines,(symbolic) reasoning and expert systems; statistical approaches, Bayesian estimation, search and optimization methods] and can, for any given set of human-defined objectives, generate outputs such as contents, predictions, recommendations, or decisions influencing the environments they interact with».

According to a risk-based approach to technological innovation, the proposal introduces the explicit prohibition of certain artificial intelligence practices where these may raise unacceptable risks [55, p. 43, Article 5]. For AI systems that may create a high risk to the health and safety of fundamental rights of natural persons, the classification is based on the intended purpose and functions performed by these components, also according to a contextual understanding of them and their use, and not only on technological features [55, p. 13].

For the purposes of HAIKU, it is essential to bear in mind that AI systems identified as high-risk may regard AI technology used in (1) critical infrastructures (e.g. transport), that could put the life and health of citizens at risk and (2) safety components of products (e.g. AI application in robot-assistant and digital assistant).

Moreover, high-risk AI systems can be classified in two main categories, namely:

- AI systems intended to be used as a safety component of products subject to a third-party ex-ante conformity assessment [55, p. 45, Article 6(1)], or

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

- Stand-alone AI systems with mainly fundamental rights implications since their risks have already experienced or are likely to materialise in the near future (these are explicitly listed in Annex III) [55, p. 45, Article 6(2)].

Considering the fast-evolving nature of these technologies, the AI Act already includes a flexibility clause that will allow the Commission to update and/or expand the list of high-risk AI systems used over time in certain predetermined domains [55, p. 45-46, Article 7].

Against this background, high-risk AI systems may be permitted within the EU market if they are compliant (at least) with the mandatory safety and security horizontal requirements and obligations provided by the AI Act (Title III, Chapter 2). They have to satisfy technical and non-technical requirements over the whole lifecycle. This means that once they overcome the ex-ante conformity assessment needed for placing on the market and putting into service, these technologies may be further subjected to ex-post control check mechanisms on a routine basis. In particular, a new check is needed if substantial changes happened after the first ex-ante conformity assessment.

Notwithstanding the material scope of the AI Act probably will not include aviation and ATM [55, p. 24, recital 29], the rules provided within its framework aim to suggest a general working method to proactively approach the design and development of these technologies since the early stage of development. They provide a general-purpose methodology over this time of transition.

4.4.2. Highlights on relevant definitions

Once defined which systems can fall within the scope of the AI Act, the following step concerns the identification of actors subjected to the obligations and requirements provided by this document. In this regard, the proposal opts for a horizontal approach now including all the participants across the AI value chain. A complete list of these players is available in Article 3 [55, p. 39]. However, for the purposes of the HAIKU project, the attention should primarily focus on the following notions.

Reference	Definition	For the purposes of HAIKU
Article 3(2)	**Provider** as «a natural or legal person, public authority, agency or other body that **develops an AI system** or that **has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark**, whether for payment or free of charge»	It is advisable that the owners and tech providers of the Use Cases previously assess if they can be qualified as a provider in accordance with the AI Act definition.
Article 3(4)	**Users**	It is advisable that the owners and tech providers of the Use Cases previously

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 «**any natural or legal person, public authority, agency or other body using an AI system under its authority**, except where the AI system is used in the course of a personal non-professional activity»	assess if they can be qualified as a user in accordance with the AI Act definition. If not, it is also advisable to previously identify who might be the potential users

Table 2 -AI Act – Relevant Definitions

More details about the position of 'authorised representative', 'importer', 'distributor', and 'operator' are available in Annex B. Please, note that for the purposes of the AI Act, the term 'operator' has a generic meaning, i.e. «the provider, the user, the authorised representative, the importer and the distributor» [Article 3(8)]. It shall not be intended as a synonym of "operator" as this concept is used in other domains.

4.4.3. Development requirements

As anticipated, the AI Act aims at introducing specific requirements for the design, development, deployment and marketing of AI systems. As noted, the pillars of this new normative architecture include practices that are already part of the state of the art for many diligent operators working in this sector [55, p. 13]. Nonetheless, the main goal of the proposed regulation is to tailor these requirements to the specific features of AI. In this regard, compliance requirements focus on six main critical nodes, which will be presented in the following paragraphs.

- **Risk management**

According to a risk-based approach, the first requirement prescribed concerns the functions and features of the risk management systems [55, Article 9(1)]. As already mentioned, this system should consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating. Risk assessment methodologies shall rely on generally acknowledged state-of-the-art, giving consideration to the technical knowledge, experience, education, and training to be expected by the user and the environment in which the system is intended to be used. In light of this, risk mitigation measures should ensure the elimination or reduction of risks as far as possible through adequate design and development; the implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated; and, where appropriate, training for users. Specific and overall residual risks have to be assessed acceptable, in accordance with their intended purpose or under conditions of reasonably foreseeable misuse. Those residual risks shall be communicated to the user. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and are in compliance with the risk-management requirements.

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

A supporting table for the analysis of these relevant development requirements for the purposes of HAIKU is available in Table E. 1

- **Data governance**

Models that need to be trained deserve particular attention, especially for the aspects related to the quality of training, validation and testing data sets [definitions available in Annex B]. In this regard, the design, development and deployment of high-risk AI systems have to be informed by appropriate data governance practices, covering all the many steps required for the establishment and use of databases from collection to preparation processing operations until assumption formulation and quality assessments. Training, validation and testing data sets shall be relevant, representative, free of errors and complete and, where required by the intended purpose or use of the AI system, they have to be assessed in light of the characteristics or elements that are particular to the specific geographical, behavioural or functional setting [Article 10]. Where training and biases monitoring, detection and correction may require the processing of special categories of personal data, providers have to enforce appropriate cyber-security and privacy-preserving measures according to the current EU data protection legislation [79][80][83].

A supporting table for the analysis of these relevant development requirements for the purposes of HAIKU is available in Table E. 2.

- **Transparency duties**

Tentatively transposing the ethical requirements concerning explainability and transparency, the regulation proposal further devotes particular attention to documental, record-keeping and informative duties, intended as functional to the effective exercise of accessibility, interpretability and liability prerogatives [63, p. 12 and Article 4(2)]. In this regard, high-risk AI systems not only have to be accompanied by the technical documentation drawn up before these are put on the market or service [55, Article 11]. These technologies also need to have specific by-design capabilities enabling the automatic recording of the events (logs) occurring while the system is operating. Moreover, logging capabilities have to enable monitoring over standard operations as well as over those that may lead to substantial modifications of the purpose of the systems, facilitating post-market monitoring mechanisms. Adequate levels of traceability must be ensured over the whole systems lifecycle, proportionated to the intended purpose and use of these latter and their risk exposure to the safety and fundamental rights of the people potentially affected [55, Article 12]. Eventually, the design must be sufficiently transparent to enable users to interpret the system's output and use it appropriately and needs to be accompanied by concise, complete, correct, comprehensible and clear information and instructions for the use. Additional information should be provided to facilitate human oversight, including technical measures to facilitate the interpretation of the outputs [55, Article 13].

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

A supporting table for the analysis of these relevant development requirements for the purposes of HAIKU is available in Table E. 3.

- **Human oversight**

The AI Act also introduces specific requirements concerning the design and development of human-machine interface tools, in order to allow an effective oversight by natural persons over the functioning of the AI systems. In particular, the role of human agents firstly has a pre-emptive and remedial nature over the functioning of these latter, preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse. From a pragmatic standpoint, the proposed regulation would introduce as mandatory measures and requirements aimed at ensuring the individuals to:

- fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible;
- remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (‘automation bias’), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;
- be able to correctly interpret the high-risk AI system’s output, taking into account in particular the characteristics of the system and the interpretation tools and methods available;
- be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system;
- be able to intervene in the operation of the high-risk AI system or interrupt the system through a “stop” button or a similar procedure [55, Article 14(4)].

According to the technological neutrality and proportionality principles, it is reasonable to assume that these requirements should be assessed on a contextual basis, taking into account the technological state of the art and the specific needs of the users involved.

A supporting table for the analysis of these relevant development requirements for the purposes of HAIKU is available in Table E. 4.

- **Technological robustness**

The requirements concerning technological robustness mainly focus on accuracy, robustness and cybersecurity. The position of these needs should not be misunderstood: security is intended as an essential (and implicit) feature of high-risk AI systems. Therefore, technological robustness – broadly intended – has to be tailored to the intended purpose of each system, ensuring accurate results and performance throughout its lifecycle [55 Article 15(1)]. In this regard, according to the expected

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

lifetime of the systems, necessary maintenance and care measures shall be ensured, as well as the release of the related software updates. Assuming the system will continue to learn after being placed on the part or put into service, these should have capabilities to ensure the due management of possible future biased output, thanks to the development of 'feedback loops'. More generally, high-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular, if due to their interaction with natural persons or other systems. Systems should also be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities, ensuring the prevention, control and mitigation of attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws. Even in this case, according to the technological neutrality and proportionality principles, it is reasonable to assume that these requirements should be assessed on a contextual basis, taking into account the technological state of the arts and the specific needs of the users involved.

A supporting table for the analysis of these relevant development requirements for the purposes of HAIKU is available in Table E. 5.

- **Quality management and conformity**

Beyond the requirements related to the design and development of high-risk AI systems, the proposed regulation also introduces specific obligations for providers, proactively addressing quality management and conformity assessments. In this regard, providers have to ensure systematic and orderly documentation of several sensitive aspects of AI systems' usage and functioning. In particular, they have to provide written policies, procedures and instructions, concerning their strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system and all techniques, procedures and systematic actions to be used for to ensure the compliance with the design, development, data quality and feedback loops requirements mentioned above [55].

A supporting table for the analysis of these relevant development requirements for the purposes of HAIKU is available in Table E. 6.

Take-away message

The AI Act proposal aims at introducing new and specific development requirements for a trustworthy AI. Even though its provisions are not definitive yet, they may provide useful insights about the future EU AI regulatory framework. In particular, for the purposes of HAIKU, these norms can help the interpretation and the compliance assessment of existent aviation law requirements, checking if the current state of the art is aligned with these possible future amendments.

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

4.5.EC proposal for an AI Liability Directive

4.5.1. The core: ease the burden of proof for victims of damages caused by AI

The second pillar of the EU AI legal framework is the AI Liability directive [63].AI specific issues regarding liability are linked to certain characteristics of AI systems, *e.g.,* the opacity/lack of transparency and explainability of some models, the margin of risks associated to autonomous behaviours, the complexity of the socio-technical systems surrounding the production and use of these technologies and, in some cases, the continuous adaptation and the lack of predictability of self-learning algorithms[3] [64, Annex 5]. These features generally make the application of existing liability rules uncertain and more difficult. Indeed, the victim and possible liable person wanting to check liability risks, as well as judges having to decide about liability claims, have to rely on cases and norms they need to interpret general rules which were not designed with AI in mind [64, p. 2].

Moreover, measures concerning private law (of which non contractual liability rules are part) are characterized by long-standing national legal traditions. This is the reason why liability frameworks at national level present significant divergences, and this makes Member States – and even more non-EU partners – reluctant to pursue coordinated reforms in this field [59, pp. 9 ff.].

Against this background, the new rules introduced by the AI Liability directive are intended to refresh the existing burden-of-proof measures to address the AI-specific problems. They build on the substantive conditions of liability currently existing in national rules, such as causality or faults, but focus on target proof-related measures, ensuring that victims have the same level of protection as in cases not involving AI systems. In particular, the proposal opts for a stage-based approach and strengthens the use of disclosure and rebuttable presumption. This would make it easier to integrate the harmonised AI-specific adaptations of liability rules into the different national legal frameworks without friction [64, p. 33]. More details about this twofold strategy and the related implications for the HAIKU project will be available in the following paragraphs.

The Directive aims at easing the burden of proof easing for claimants avoiding exposing providers, operators and users of AI systems to higher liability risks [64, p. 6]. On the other hand, the new rules also aim to provide a unitary framework able to embrace the existent unilateral legislative measures adopted by the MSs for addressing AI liability issues, so avoiding further legal fragmentations [64, p. 19].

[3] AI systems not having such characteristics can be dealt with under the existing liability rules, similarly to other types of software [8, p. 2].

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

4.5.2. Highlights on relevant definitions

Complementing the AI Act, from a legal standpoint, the AI Liability directive follows the same definitions introduced by this latter. On the other hand, from a legal standpoint, this new piece of legislation introduces three relevant notions, namely: damage, claimant and duty of care [Annex B].

For the purposes of the HAIKU project, the just mentioned definitions and the underlying legislative choices may have relevant consequences, as explained in the following paragraphs.

First, considering the **implicit notion of damage**, the AI liability directives should only cover «damage caused by an output of an AI system or the failure of such a system to produce an output where such an output should have been produced».

As better specified in the sections dedicated to aviation law [ref. AMC CS 25-1309] the notions of 'failures' and 'failure conditions' have a domain-based meaning. Nonetheless, the two concepts basically focus on components and/or parts or elements of them, thus giving more prominence to the technological factor than to the human ones. However, considering the use of AI (especially when used for supporting decision-making), to mark a clear distinction between these two may be not so easy, since the interaction might be based on a factual collaboration between human operators and AI. This is the reason why the implicit notion of damage suggested by the AI Liability Dir. (as well as the conditions that could cause it and the causal link between the damage and the injury) may raise some concerns. As specified by the Recital 15 [63, p. 18], under this new legal regime «*there is no need to cover liability claims when the damage is caused by a human assessment followed by a human act or omission, while the AI system only provided information or advice which was taken into account by the relevant human actor*». ***This choice consequently questions the plain application of these new rules to human-AI teaming scenarios having collaborative features***. Indeed – as this recital continues – the EU legislator, at least for the moment, assumes that: «in the latter case, it is possible to trace back the damage to a human act or omission, as the AI system output is not interposed between the human act or omission and the damage, and thereby establishing causality is not more difficult than in situations where an AI system is not involved».

Secondly, recalling the provided notion of '**claimant'**, it is noteworthy that the legislator provides that claims for damages can be brought not by the injured person only, but also by persons that have succeeded in or have been subrogated into the injured person's rights, or by someone acting on behalf of one or more injured parties. In this regard, subrogation and representation allow individuals to obtain a compensation for damages by or thanks to third parties, such as insurance companies or consumer organisations. These provisions aim to give more possibilities to persons injured by an AI system to have their claims assessed by a court, even in cases where individual actions may seem too costly or too cumbersome to bring, or where joint actions may entail a benefit scale [63, p. 12].

Considering the use of AI systems postulated by the HAIKU project and the related use cases, these provisions suggest a careful and proactive approach. In safety-critical domains, like aviation, negative

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

events usually may have a plural offensive nature i.e., it has an intrinsic attitude to offend/damage more people at once. **Since liability risks and compensation are consequently rated, subrogation and group representation for damages caused by the use of AI systems may increase the economic exposure of the organisations involved in the deployment of these technologies**.

Eventually, the explicit reference to the **duty of care** has to be read as a general call to consider the impacts of technological innovation related to AI and the potential damages for the interests of the subjects involved according to a holistic and comprehensive understanding. In this regard, consistently with the aviation proactive approach to safety and security, consideration and impact assessment on the design and implementation of new AI based solutions should be always addressed according to the principles of precaution and prevention.

4.5.3. Material scope and interplay with EU Aviation Law

Defining the material scope of the AI Liability directive, article 1 does not apply to criminal liability (63, article 1(2)) and shall not affect rules of Union law regulating conditions of liability in the field of transport (63, article 1(3)(a)). Moreover, MSs «may adopt or maintain national rules that are more favourable for claimants to substantiate a non-contractual civil law claim for damages caused by an AI system, provided such rules are compatible with Union law» (article 1(4)).

These limitations may also involve the liability regime for damages caused by the misfunctioning of AI systems in the aviation domain. Therefore, waiting for sectoral legislative review, in the transition period the new norms introduced by the proposed directive should be appreciated and used for their guidance interpretative value.

According to the principle as per special law repeals general laws, for air transport law the EU institutions already provided the following clarifications, with particular attention to the perspective application to UAS [64, Annex 6, pp. 132 ff.].

Reference	Interplay with the AI Liability proposal	Consequences for EU Aviation Law
Reg. (EC) 785/2004 on insurance requirements for air carriers and aircraft operators	The Regulation does not harmonise issues of civil liability or the burden of proof.	When applicable, the rules proposed by the AI liability directive can be used for alleviating the burden of proof for the victims. The mandatory insurance requirements for those types of AI systems would not specifically include AI-enabled

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

		products of category falling under Reg. (EC) 786/2004
Reg. (EC) 2027/97 on air carrier liability in the event of accidents	The Regulation is still applicable for the part concerning damages to passengers' baggage and delay.	The policy measures envisaged under the AI liability initiative do not overlap with Regulation (EC) No 2027/97. The Regulation does not address liability for damage caused by UASs to third parties or the liability of parties other than the air carrier for damage caused by UAS, such as aircraft operators not licensed as air transport undertakings or service providers of air traffic management. In addition, it does not cover alleviations of the burden of proof to the benefit of the claimant seeking compensation for damage caused by an UAS. The future proposal on liability for AI could apply to autonomous AI-enabled UASs and air traffic management systems
Montreal Convention for the Unification of Certain Rules for International Carriage by Air	It is doubtful whether the Montreal Convention covers the liability of UAS operators for damage caused to third parties on the ground. The Montreal Convention does not cover liability towards third parties, e.g. liability vis-à-vis a passer-by who is injured by an	Separate application of the two liability regime until the EU Commission would provide harmonised rules on strict liability of users/operators of certain Ai-enabled technologies. When applicable, the rules proposed by the AI liability

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

	autonomous delivery drone during a landing manoeuvre, due to an erroneous output of the drones' AI-enabled perception system. Neither does it cover liability of other entities than the air carrier, such as aircraft operators not licensed as air transport undertakings, or air traffic management service providers. In addition, the Convention does not regulate alleviations of the claimant's burden of proof regarding substantive liability conditions that could be obscured by the use of AI.	directive can be used for alleviating the burden of proof for the victims.
Implementing Regulation (EU) 2021/664 on a regulatory framework for the U-space	The policy measures envisaged under the AI liability initiative do not overlap with Implementing Regulation (EU) 2021/664. That Implementing Regulation does not address liability for damage caused by UASs to third parties or the liability of parties other than the air carrier for damage caused by UAS, such as aircraft operators not licensed as air transport undertakings or service providers of air traffic management. In addition, it does not cover alleviations of the burden of proof to the benefit of the	Separate application of the two liability regime until the EU Commission would provide further clarifications and/or guidance. When applicable, the rules proposed by the AI liability directive can be used for alleviating the burden of proof for the victims.

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

	claimant seeking compensation for damage caused by an UAS.	
Implementing regulation (EU) 2017/373 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions (Annex III, ATM/ANS. OR.020 Liability and Insurance cover)	The preferred policy options envisaged under the AI liability initiative do not overlap with Implementing Regulation (EU) 2017/373. That Implementing Regulation does not cover alleviations of the burden of proof to the benefit of the claimant seeking compensation for damage caused by an UAS.	When applicable, the rules proposed by the AI liability directive can be used for alleviating the burden of proof for the victims.
1952 Rome Convention on Damages Caused by Foreign Aircraft to Third Parties on the Surface	It is doubtful whether the Convention covers the liability of UAS operators for damage caused to third parties on the ground. The 1952 Rome Convention, ratified by only four Member States, addresses this kind of damage, but it is uncertain whether that Convention might be interpreted as covering UASs. Furthermore, the 1952 Rome Convention does not cover liability for collisions between aircraft in the air nor alleviations of the claimant's burden of proof regarding substantive liability conditions that could be obscured by the use of AI.	Separate application of the two liability regime until the EU Commission would provide further clarifications and/or guidance. When applicable, the rules proposed by the AI liability directive can be used for alleviating the burden of proof for the victims.

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

	Lastly, the Convention only covers international flights, unless the signatory state explicitly declares that it also covers domestic flights in that state. Hardly any unmanned aircraft fly internationally today.	

Table 3 - AI Liability Dir., Interplay with Aviation Law

4.5.4. Disclosure duties and rebuttable presumptions

Specifically considering the new rules proposed by the proposal, the directive aims at introducing two main solutions, namely a duty of disclosure of evidence correlated to a rebuttable presumption[4] of non-compliance [63, article 3] and a rebuttable presumption of a causal link in the case of fault [63, article 4].

Generally, disclosure duties aim at making available and accessible the information that users and providers of high-risk AI have to record or document pursuant to the AI Act. This solution could help the victim to make a successful liability claim, providing evidence for demonstrating fault or proving the liable persons did not comply with their obligations under the AI Act. The requests should be supported by facts and evidence sufficient to establish the plausibility of the claims. The competent national courts thus can order such disclosure and, if needed, provide adequate safeguards to ensure proportional protection of the interest of all the parties involved, preventing blanket requests.

These duties are coordinated with a rebuttable presumption of non-compliance. This procedural tool allows to assume non-compliance from the non-collaborative behaviour of the subject burden of the disclosure duties. The defendant, however, has the right to rebut the presumption.

In case fault consists in the lack of compliance with a duty of care under Union or national law (*e.g.* aviation law), a rebuttable presumption of a causal link allows the claimant to assume the correlation between that non-compliance and the output produced by the AI system. On the one hand, the claimant has to prove the fault of the defendant according to the applicable EU and national rules. On the other hand, the court can presume the fault on the basis of non-compliance with a court order for

[4] Rebuttable presumption is a tool already existing in many legal frameworks and basically helps the victims to overcome proof-related difficulties. It is intended as an assumption made by a court or the legislator that is taken to be true unless someone proves otherwise. For instance, If the victim meets a reduced burden of proof, e.g. by demonstrating the plausibility or likelihood of certain facts, it is presumed that those facts occurred. In order to avoid having to pay compensation, it is then for the liable party to demonstrate that these facts did in reality not occur or that other facts, for which the liable party is not responsible, occurred. This tool leaves the basic distribution of the burden of proof intact, but makes it easier for the victim to discharge that burden. [64, p. 33]

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

disclosure of preservation of evidence. Moreover, the court can establish the conditions for the applicability of the presumption of causality whereby once judges had determined the excessive difficulties for the claimant to prove the causal link.

The analysis of these relevant requirements for the purposes of HAIKU is available in Table E. 7.

Take-away message

The AI Liability Directive proposal aims to clarify the future legal regime on the allocation of the burden of proof for damages arising from the failure of AI systems. As explained by the table of the interplay between this new proposal and aviation law liability regime, the new norms can help the interpretation and the compliance assessment of existing aviation law requirements. In particular, these new references may help to establish a valid compliance strategy, also taking into account the potential impacts of ex-post disclosure duties and the liability risks related to rebuttable presumption of non-compliance.

4.6.EC proposal for the revision of the Product Liability Directive

4.6.1. Costumer Products Liability as a general and residual discipline

Looking at the prospective EU legal framework for AI, the third pillar of this architecture is the Product Liability Directive (PDL)[33]. The rules introduced by this latter was approved in 1985 and defined an harmonised discipline for the protection of EU consumers. Overtime the regime introduced by the PLD in 1985 has been periodically reviewed and amended, especially to adapt the contents of the norms to the scientific and technological advances that have occurred.

As explained by the Commission, «product safety and product liability are complementary mechanisms for achieving a functioning single market for goods that ensure high levels of safety» [61, p. 3]. This is the reason why the PLD is generally intended as one of the cornerstones of EU law. This set of rules, since the beginning of the EU harmonisation process, established specific guarantees to foster and facilitate consumers’ trust in the internal market benefits.

Anticipating the consideration above-exposed about the complementary nature of safety and liability legislation concerning AI, this directive couples with sectoral product safety legislation (*e.g.,* on machinery [38], pharmaceutical products [35][37], toys [39], radio equipment [42]) and, more generally, with the general regime established by the General Product Safety Directive (GPSD) [34].

Differently from other statutes, the PLD covers extra-contractual liability of the producers for injuries/damage caused by a lack of safety. The addressees of its protection are consumers intended as natural persons only, excluding professional users and usages for commercial purposes [61, article 1]. The right to compensation is subject to a limitation period of 3 years running from the day the person injured becomes aware of damage, defectiveness and the identity of the liable economic

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

operator [33, article 14, and 61, article 1]. As observed for the AI Liability Directive, the PLD assumes the right to compensation can be exercised by the victim, by the succeeding or subrogating person or by person acting on behalf of one or more injured persons, according to EU or national law.

4.6.2. PLD AI-oriented proposal for revision and its contribution to HAIKU

In 2018[46], the periodic evaluation carried out as part of the Commission's regulatory fitness and performance (REFIT) programme, concluded that the PLD had several shortcomings. In particular, from the observations collected in the report emerged that it is legally unclear how to apply the PLD's decades-old definitions and concepts to products in the modern digital economy and circular economy [61, p. 1]. And this is more than evident in all those cases where the interpreter needs to take into account the developments related to new technologies, including artificial intelligence (AI)[54].

In light of the above, the PDL proposal for revision [61] can be a useful resource for defining the HAIKU project legal framework. The proposed amendments not only address concerns common to all the actors now involved in the development and deployment of AI in different sectors. The new discipline may also provide clarifications and insights about the concepts and definitions that, on a long term perspective, may have a general guidance value.

A supporting table for the analysis of the relevant provisions of this proposal for the purposes of HAIKU is available in Table E. 8.

4.6.3. The notion of defectiveness and the exemptions from liability

Generally, a product can be considered defective when it does not provide the level of safety expected by the public at large and intended users in particular. To assess defectiveness manufacturers, as well as certification authorities and courts, have to take into account all factors and circumstances of design, implementation, development and deployment of the product at stake.

The PDL and related law cases, both at national and EU level, over time provide relevant insights to identify the criteria and factors that should be taken into account for the purposes of these conformity/defectiveness assessments.

Take-away message

Product Liability regime is basically dedicated to assure compensation to consumers that suffered damage caused by defective products. As a residual regime, it is applicable when no more specific rules are available. The PLD, especially in light of its prospective amendments, may provide useful interpretative insights and design suggestions for the purposes of HAIKU. In particular, the defectiveness indexes elaborated by law cases on its norms, can help to pre-empt and better address failures or misuses of AI systems, as well as to improve their technological 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

5. EU aviation legal framework for AI

The reader here will find an overview of the applicable legal requirements to AI in aviation, according to the current sectoral legal framework. More information about the different areas covered by the following sections is available in Annex G -

5.1. ICAO provisions

The International Civil Aviation Organisation (ICAO) is aware that with the advent of big data and ever increasing computer power, use of **AI** has risen significantly over the last years [95]. According to ICAO, applications related mainly to the development of **deep learning models** for **detection** and **classification** of **images, text and voice**, were the most common in aviation until the end of 2022. In other words, non-safety-critical applications.

As of the end of December 2022, no deliverables on the matter have been published by ICAO on AI. However, ICAO has laudably promoted research on aviation applications of AI and participated in the Focus Group (FG) on the subject led by the International Telecommunication Union (ITU). Only deliverables by EASA and EUROCONTROL were listed on the ICAO web page on the day of the visit. This could indicate that presently Europe is in the lead for the applications of AI in aviation.

Since ICAO provisions on AI might emerge in the future, it is important to strive for maintaining the EU leadership, to be in the position of influencing possible future ICAO publications.

On the other hand, at the end of 2022 no obstacles emerge from ICAO provisions for implementation of AI in aviation. In the absence of specific Standards and Recommended Practices (SARPs), those of general nature contained in Annex 19 to the Chicago Convention would still apply [96]. Consequently, States must oversee AI application in civil aviation, while all Service Providers (e.g. aircraft operators, aerodrome operators, Air Navigation Service Providers (ANSPs), etc.) shall extend the scope of respective Safety Management Systems (SMS) to any AI application used in operations.

5.2. ITU deliverables

The Focus Group on Aviation Applications of Cloud Computing for Flight Data Monitoring (FG AC) was established by the ITU-T Telecommunication Standardisation Advisory Group (TSAG) in June 2014 in response to a special meeting on Global Flight Tracking of Aircraft organised by the ICAO and an Expert Dialogue on Real-time Monitoring of Flight Data, facilitated by ITU.

The objective of FG AC was to explore how Information and Communication Technologies (ICTs), including cloud computing and big data analytics, could support aviation applications, such as real-time monitoring of flight data, and to identify the requirements for related ICT/telecommunication standards.

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

TSAG endorsed the following four Deliverables produced by the FG AG in 2016 [107]:

a) Deliverable 1 - Existing and Emerging Technologies of Cloud Computing and Data Analytics;
b) Deliverable 2/3 - Use Cases and Requirements;
c) Deliverable 4 - Avionics and Aviation Communications Systems; and
d) Deliverable 5 - Key findings, recommendations for next steps and future work.

AI was considered in particular for its machine learning (ML) potential.

Deliverable 5 states that a cloud service provider can provide reliable, secure and affordable infrastructure in which to host the applications needed to support Flight Data Monitoring (FDM) and other types of data analytics. A cloud Service Provider (SP) may provide additional data analytics tools and services to drive additional benefit from the data and information generated by standard FDM techniques and other data sources such as weather, Aircraft Communications Addressing and Reporting System (ACARS), Electronic Flight Bags (EFBs), etc. The use of the cloud as a repository for sensitive data and information requires an assurance of security and privacy such as ISO/IEC 27001 and ISO/IEC 27000 family to protect the applicable airline as the Cloud Service Customer (CSC) [104][106].

5.3. European Regulations applicable to AI in aviation

5.3.1. Legal basis

Until 1986 the EU was unable to establish a comprehensive regulatory framework for civil aviation, because decisions on the matter were subject to unanimous vote in the Council and hence even tiny minorities were able to block, to defend their national protectionism.

This unfortunate situation was changed in 1987, when the so-called ‘Act Unique’ originated by President Jacques Delors became applicable [66]. Since then, a majority vote applied in the Council on transport matters, including civil aviation and related regulations started to emerge for several facets of aviation, from commercial competition, liability, international affairs and so on, including safety, Human Factors (HF) and security.

No specific and detailed legally-binding rules on application of AI in civil aviation exist today. However, regulations having a wider scope would still apply to civil aviation.

This paragraph hence summarises the main legally-binding provisions on general aspects of safety, HF and security which are equally applicable to AI.

Today, point 2 of Article 100 of the Treaty on the Functioning of the EU (TFEU) gives competency to the co-legislators for sea and air transport:

> The European Parliament (EP) and the Council, acting in accordance with the ordinary legislative procedure, may lay down appropriate provisions for sea and air transport. They

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

> shall act after consulting the Economic and Social Committee and the Committee of the Regions.

This means that EP and Council may adopt, through majority voting, any act deemed necessary for civil aviation, including on safety, HF and security aspects of AI applications in aviation.

The figure presents a systematic overview of the main areas covered by this analysis. The most relevant parts will be addressed in the remaining part deliverable. The others instead, will be available in the dedicated annexes.

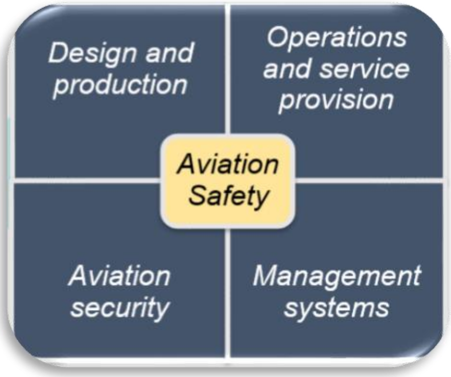

Figure 2 - Map of EU Aviation Law domains covered by the SOAR

5.3.2. AI in Articles of EASA Basic Regulation on aviation safety

The European Union Aviation Safety Agency (EASA) was established in 2002 through the so-called first 'Basic Regulation'. Therein the mandate of EASA was limited to airworthiness of aviation products (e.g. aircraft, engines, propellers) and environmental impact of aircraft. Airborne software was included, however without any competence for cyber-security and without any mention of AI. The competences for airworthiness included also related organisations and personnel.

The mandate of EASA was extended in 2008 to Aircraft Operations, Flight Crew Licencing (FCL) and Third Country Operators (TCO), once more including related software, organisations and personnel, but neither mention of cyber-security nor of AI.

This approach was confirmed by subsequent Regulation 2009/1108 which extended the mandate of EASA to ATM and ANS, amending 216/2008.

Regulation 216/2008 was repealed in 2018 by the so-called New Basic Regulation (NBR) 2018/1139, which further extended the mandate of EASA to ground handling, cyber-security and civil drones of any mass.

Neither explicit mention of AI nor of ML is contained in the Articles of this NBR. Software is mentioned in few definitions related to ATM/ANS, aerodromes and Unmanned Aircraft Systems (UAS), stating that software is indeed an integral element of any constituent or equipment and therefore, in the scope of several provisions of NBR, even if not explicitly mentioned.

In this perspective, the Articles of the NBR most relevant for their applicability to AI are available in Table F. 1 in Annex F.

5.3.3. Essential Requirements on aviation safety

The EASA NBR, similarly to several other acts adopted by the EU Legislator, is based on the so-called 'New Approach' for regulation of safety, conceived in the early eighties and laid down in a Council Resolution of 1985 [5].

This 'New Approach' is based on four fundamental principles:

1. Legislative harmonisation is limited to the adoption, by means of Directives or Regulations, of the **Essential Safety Requirements** (ER) with which products put on the market must conform, and which will therefore enjoy free movement throughout the territory of the EU;
2. The task of drawing up the technical specifications needed for the production and placing on the market of products conforming to the Essential Requirements established by the Legislator, while taking into account the current stage of technology, is entrusted to **Standard Development Organisations** (SDOs; e.g. CEN);
3. These technical specifications are not mandatory and maintain their status of **voluntary standards**;
4. But at the same time authorities are obliged to recognise that products, services, organisations and personnel in conformity with harmonised standards are **presumed to conform to the ERs** established by the Legislator.

Although initially conceived only for industrial products, the Legislator applied the spirit of the 'new approach' to all facets of aviation safety: products and systems, aerodromes, operations and services, involved organisations and personnel. Therefore, current EASA NBR 2018/1139 is complemented by several Annexes, eight of which containing ERs .

The ERs most relevant for their applicability to AI are listed in Table F. 2. However, the following paragraphs provide some brief summaries of the main requirements to take into consideration for the different areas covered by this SOAR. More details available in Annex F.

Take-away message on aviation safety

In conclusion, ERs listed in Annexes II to IX of NBR 2918/1139, although neither sufficiently detailed for concrete application nor explicitly mentioning AI, establish provisions applicable also to AI with regard to:

- **Safety of design, production and maintenance to ensure suitability for intended use of any safety-related system;**
- **Suitability for use of non-installed equipment;**
- **Security, including training in this domain and cyber-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

- **Instructions delivered by the manufacturer when the system is introduced into service and subsequently, whenever necessary, throughout the life-cycle of the system;**
- **Clear and explainable instructions and procedures for staff tasked to use systems.**

The Articles of NBR 2018/1139 and related ERs are further detailed in several legally-binding Commission Regulations (so called 'hard rules'), supported by EASA so-called 'soft rules', EUROCONTROL publications and consensus-based industry standards, as presented in the following paragraphs.

Take-away message on design and production

In conclusion, although technology agnostic, EC Regulation 748/2012 [40] mandates some processes to validate and verify AI airborne applications. Furthermore, provisions exist therein for cyber-security, including during the production phase.

Take-away message on operations and service provision

In summary, the most relevant responsibilities assigned by regulations to operators and SPs concern:

- **Risk assessment is required for any newly introduced AI application;**
- **Safety-critical AI applications shall be subject to approval by the competent authority;**
  - **for lower risk AI applications the LoI of the authority could be reduced;**
  - **during the initial period after introduction of new AI applications, receiving feedback from involved personnel would be important, not only for data collection and analysis, but also to improve the HMI and to feed EBT; and**
  - **AI shall be administered, throughout its life cycle, including control of data sources.**

Take-away message on aviation security

In conclusion, following amendment 16 to ICAO Annex 17, EC Regulation 2019/1583 [50] and EASA Opinion 03/2021 [13] introduced a performance-based (i.e. not prescriptive on technical details) and risk-based regulatory framework for aviation ICT systems, which is becoming applicable also to AI functions and whose key requirement would be an ISMS, possibly part of an Integrated Management System, as explained in the paragraph below. This would continue, even when the NIS2 Directive (on 18 October 2024) and the provisions on ISMS (expected in 2025/Q4) will become applicable.

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

5.3.4. Commission Regulations on management systems

A key requirement for ‘organisations’ is to be equipped with a Safety Management System (SMS).

One way of describing the SMS is through the Tomasello’s ‘pyramid’ [120]:

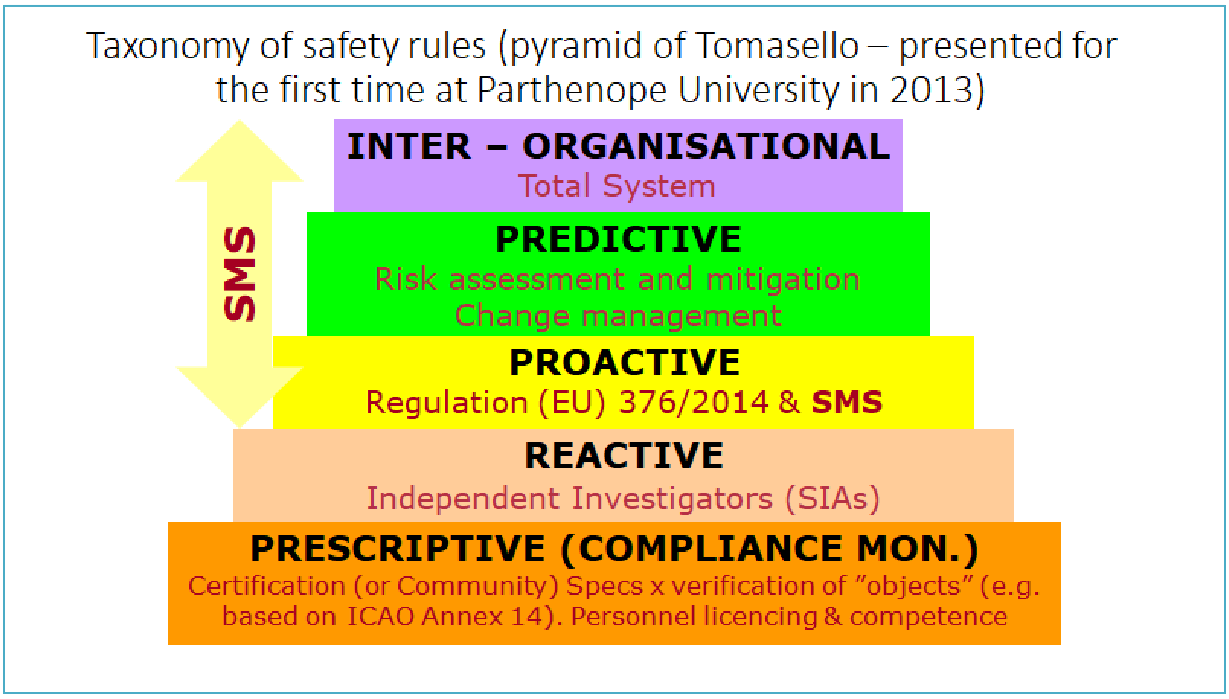
Taxonomy of safety rules (pyramid of Tomasello – presented for the first time at Parthenope University in 2013)
SMS
INTER – ORGANISATIONAL
Total System
PREDICTIVE
Risk assessment and mitigation
Change management
PROACTIVE
Regulation (EU) 376/2014 & SMS
REACTIVE
Independent Investigators (SIAs)
PRESCRIPTIVE (COMPLIANCE MON.)
Certification (or Community) Specs x verification of ”objects” (e.g. based on ICAO Annex 14). Personnel licencing & competence

Figure 3 - Taxonomy of Safety rules (Tomasello's Pyramid)

In that vision an organisation builds safety in layers and each layer, for its implementation, requires the existence of the lower layers.

The bottom layer is ‘prescriptive’ safety management, which means ensuring compliance with the applicable legally-binding rules (e.g. those summarised in the paragraphs above). This is covered by the Commission Regulations on operators and SPs summarised in the previous paragraphs, which all demand the establishment of a ‘Compliance Monitoring’ function.

The second layer from the bottom is ‘reactive’ safety, constituted by independent investigations conducted by Safety Investigation Authorities (SIAs) established in the EU through Regulation 996/2010 [76]. In the context of reactive safety, in case of accident or serious incident the operator or SP is required to report to the competent SIA and thereafter to remain available to provide any additional information which the SIA may require.

However, following the studies of Herbert Willian Heinrich [90], SMS in all industry segments including aviation, requires to collect and analyse reports even on minor safety occurrences, since these could be precursor of a fatal accident in the future. This approach is the ‘proactive’ approach in the third layer of the pyramid. This layer is one of the prime responsibilities of the operator or service provider,

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

based on the collection and analysis of safety reports inside the organisation. However, ‘proactive’ safety shall also be implemented at national and EU level, as mandated through Regulation 376/2014 [77].

In the context of ‘proactive’ safety, even in relation to AI applications, the basic responsibilities of the designer, operator or SPs are:

a) to establish and maintain a proactive safety management inside the organisation;
b) to provide mandatory reports to the competent authority based on mentioned Regulation 376/2014 [77]; and
c) creating a climate of ‘just culture’ in which personnel is encouraged to provide voluntary occurrence reports, since from their analysis systematic safety concerns may emerge (e.g. on the explainability of the AI applications).

However, both ‘reactive’ and ‘proactive’ safety intervene only ‘after’ something occurred. In case of changes and in particular when introducing new technologies, such as AI, the fourth layer of the pyramid (i.e. ‘predictive’) becomes paramount.

For this the existing EU regulations on certified operators and certified SPs typically require the organisation to submit a procedure to the approval of the competent authority, detailing:

a) methods to identify hazards, assess the risk and evaluate the effect of mitigations, usually based on the mentioned ICAO SMM; and
b) classification of changes in ‘minor’ and ‘major’, remaining the latter subject to prior approval by the competent authority before implementation.

Most probably introducing new AI applications for safety-related functions would be a major change.

However, AI most often requires exchange of data, or at least more of one organisation would be involved in the risk assessment and mitigations. Hence the upper and last layer of the pyramid (i.e. inter organisational) becomes relevant and requires joint involvement of at least two organisations.

In conclusion, for a novel and very innovative technology like AI, the fourth (predictive) and the upper (inter organisational) layers of the pyramid become the most important. They apply under current EU/EASA rules for all organisations subject to certification. In this context a SLA between the designer and the operator or SPs may be advisable to define the relationship and possibly to refer to applicable industry standards.

Handling huge quantities of data, may also imply responsibilities for privacy and data protection, based on EU Regulation 2016/679 [79].

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

Take-away message

In conclusion, both aerodrome operators and providers of AMS, when using software applications based on AI, should verify the output of such applications and consider the relevant AMC .

5.3.5. EUROCONTROL guidance on AI

In 2019 EUROCONTROL, together with EC, set up the European Aviation/ATM AI High Level Group (EAAI HLG) composed of key representatives from all aviation sectors: airlines, airports, ANSPs, manufacturers, EU bodies, military and staff associations.

In the subsequent year EUROCONTROL released the Fly AI Report [32] to help demystify and accelerate the uptake of AI in aviation/ATM. The report emphasised that European AI developments must be safe, secure, human-centric, ethical and trustworthy and support the core values of the EU.

In particular, Section 3 of the report proposes several actions that could be taken to accelerate the development of AI in European aviation/ATM, which include [32]:

a) A federated data foundation and AI-infrastructure;
b) Development of AI validation methods and tools, subsequently consolidated into guidelines (e.g. AMC, GM) supported by industry standards;
c) Operational deployment starting from cybersecurity applications and from non-safety critical applications;
d) Performance-based approach to reduce time-to-market;
e) Development of AI culture, through training and change management.

Although the Fly AI report does neither express EC, EUROCONTROL, EDA nor NATO official view and although EUROCONTROL is not empowered to adopt any hard or soft rules, nevertheless the report represents an authoritative opinion of several segments of the aviation industry.

Nothing in that report contrasts the conclusions reached in the previous paragraphs.

6. Provisions of other aviation authorities in the world

The reader here will find an overview on the regulatory initiatives undertaken by other aviation authorities in the world on AI and on application of AI in aviation. More information about the different areas covered by the following sections is available in Annex G -

6.1. JARUS

6.1.1. What is JARUS?

The Joint Authorities for Rulemaking on Unmanned Systems (JARUS) are a group of experts gathering aviation regulatory expertise from all around the world.

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 2023 JARUS counted 63 member countries from the five continents and as well EASA and EUROCONTROL.

The purpose of JARUS, as stated in the Terms of Reference (ToR) [109], is “to recommend a single set of technical, safety and operational requirements for all aspects linked to the safe operation of UAS.

The JARUS recommended requirements and guidance material aim to facilitate aviation authorities to develop their own regulations, simultaneously avoiding duplicate efforts and fostering global harmonisation.

For instance the three risk-based categories of UAS operations and the Specific Operation Risk Assessment (SORA) developed by JARUS have been embedded into EC Regulation 2019/947[50] and also in Colombia, Georgia and Qatar and in progress in the Regional Safety Oversight Organisation (RSOO) Agencia Centroamericana para la Seguridad Aeronáutica (ACSA).

6.1.2. JARUS automation and autonomy for UAS

The scope of JARUS is limited to UAS and the environment in which they operate (e.g. ATM, UTM, UAM). This includes automation and autonomy, but not specifically AI or ML.

However, AI/ML and UAS have a point of contact in the taxonomy of the JARUS draft document on Automation and Autonomy for UAS [110].

Although automation and autonomy are relevant for aviation, they are also relevant for several other industry segments, especially those which are looking with interest at AI/ML.

Among other industry segments, the most relevant may be automotive, which is also heavily investing in automation. JARUS therefore has taken as main reference the Joint ISO/SAE standard J3016[120] which provides the most widely used taxonomy of automation levels in the transport sector. More details are reproduced in Annex C.

In summary JARUS proposes a classification scheme centred on the role of the human in performing operational functions. It also introduces the Operational Design Domain (ODD) concept as a mechanism to scope autonomous functions to help manage a complex multi-dimensional operational environment, as defined in mentioned J3016 [120].

In its taxonomy, JARUS includes a Level 0, which is not mentioned in the EASA AI guidelines, but which is identical to SAE J3016 Level 0 [120].

And the JARUS proposals go up to Level 5 (Full autonomy) which corresponds to Level 5 in SAE and to Level 3B in EASA.

One can therefore notice that the taxonomy of automation/autonomy levels is not fully harmonised across different regulatory authorities and SDOs. Further details are provided in Annex D.

Furthermore, JARUS adds one more ambitious level to the SAE taxonomy (for the moment however, not labelling it level 6), This is ambitious Level is named ‘Trusted Autonomy’ which presupposes building mutual trust between the machine and the human to achieve a highly autonomous system which can optimally interact with the human to deliver the highest possible levels of mission safety, efficiency and effectiveness. This Trusted Autonomy Level perfectly matches the concept of AI Trustworthiness in the EASA guidelines, but it is not yet present in the SAE taxonomy.

Finally, JARUS announces the intention to consider levels of automation of the airspace environment in a future JARUS document, which, if not properly managed could lead to further jeopardising harmonisation.

A single taxonomy of automation/automation systems across all transport sectors would be highly desirable. Luckily, as presented by Beatrice Pesquet-Popescu [113], standardisation activities on the matter are being progressed jointly by EUROCAE WG 114 abd SAE G34. The community should encourage such efforts, with the inclusion of Level 1A (ref. EASA) and Level 6 on Trustworthy AI.

6.2. FAA

Disruptive innovation is a term introduced by Clayton Christensen in 1997 [3] as opposed to sustainable innovation. In contemporary aviation several improvements (e.g. more efficient engines, new materials) are sustainable innovations, since they do not radically change the market. Disruptive innovation instead creates new markets, new habits and eventually leads to obsolete technologies to fade out. For instance, in the XIX century the train was a disruptive innovation, which led mankind abandoning horse-driven coaches for long range travel. In the XX century, among the disruptive innovations one could mention the personal computer and the parallel decline of the mainframes or the smart mobile telephone supplanting telephones enabling only voice conversations.

Nowadays, scholars [111] consider UAS to be a disruptive innovation. But also AI/ML can be considered disruptive innovation.

When confronted with disruptive innovations, the US Federal Aviation Administration (FAA) normally follows the cultural tradition of the British ‘common law’, which is ‘bottom up’. It consists in dealing with situations case-by-case and adopting rules only after a few years, when a tradition emerges.

In fact, while EU has regulated drone operations since 2019, the FAA regulates them in 2023 still mainly through ‘exemptions’[5]. Similarly, while EASA has already published guidelines to develop and implement AI applications in aviation, the FAA is very active only to promote R&D[6], which would contribute to building a tradition.

[5] https://www.faa.gov/uas/advanced_operations/certification/section_44807

[6] https://www.faa.gov/aircraft/air_cert/step/disciplines/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

The only place in FAA regulatory material available in 2023/Q1 [87] is the list of issues for certification of small aeroplane which refers to FAA Advisory Circular (AC) 20-115D, almost identical to EASA AMC 20-115D, when the designer intends to implement AI-based applications. The EASA guidelines also suggest using 115D [8], but consider this alone not sufficient for building trust in AI.

Take-away message

In conclusion US/FAA are lagging behind EU/EASA for regulation of emerging disruptive innovations, like AI/ML, for cultural reasons (i.e. FAA follows the bottom-up approach of the British common law, while the EU/EASA approach is top-down, based on the Illuminist tradition.

For HAIKU this means that, from the regulatory perspective, it is not necessary to look at the USA, while the Project should strive to contribute to maintaining the EU leadership in this domain.

7. 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. More information about the different areas covered by the following sections is available in Annex G -

7.1. Standards and tools for Software (SW) development

EASA AMC 20-115D, using the performance-based approach, recognises the following standards published by the European Organisation for Civil Aviation Equipment (EUROCAE) or by the U.S. Radio Technical Commission for Aeronautics (RTCA) as MoC for SW development:

a) EUROCAE ED-12C [20]and RTCA DO-178C on Software Considerations in Airborne Systems; and related supplementary standards listed here
b) EUROCAE ED-215 [21]and RTCA DO-330 [115]on Software Tool Qualification;
c) EUROCAE ED-216 [22]and RTCA DO-333 [116]on Formal Methods for SW development;
d) EUROCAE ED-217 [23]and RTCA DO-332 [117]on Object- Oriented Technology and Related Techniques; and
e) EUROCAE ED-218 [24]and RTCA DO-331 [118]on Model-Based Development and Verification of 13 December 2011.

The cornerstone of ED-12C [20] 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 failure condition(s). In turn the DAL establishes the rigour necessary to demonstrate compliance with the standard.

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

ED-12C [20] and equivalent DO-178C recognise five levels of SW DAL, available in Table G. 1.

Take-away message

In conclusion, EASA does not prescribe any specific standard for SWAL/DAL in case of ATM/ANS systems, conversely recommending ED-12C [20] for airborne software and for SW at aerodromes. It is hence proposed to use ED-12C [20] throughout the HAIKU use cases, regardless of whether they focus on airborne or ground-based AI SW.

7.2. Standards for cyber-security

As explained, most probably all aviation organisations will be mandated, by 2025/Q4 to implement an ISMS.

At the level of 'soft rules' these provisions are complemented by EASA AMC-42 [12].

For the purposes of HAIKU, EASA AMC 20-42 recognises as MoC the EUROCAE and RTCA standards are available in Table G. 2.

Take-away message

In conclusion, bearing in mind that ISMS would be required only from beginning of 2026 and in any case at TRL 8 or 9, it is recommended that:

a) **HAIKU use cases using inter alia aeronautical information consider ED-201A[30];**
b) **HAIKU use cases developing AI airborne applications consider ED-203A[27];**
c) **HAIKU use cases developing AI applications for ATM/UTM consider ED-205A[31]; and**
d) **EASA should amend the AMC/GM related to cyber security aspects for ATM/ANS, mentioning ISO/IEC 27005 and EUROCAE ED-201A, 205A and 206[30][31][32].**

7.3. Standards on taxonomy of automation/autonomy

The most relevant international standard for the taxonomy of automation/autonomy is Joint ISO/SAE standard J3016[120], already mentioned, since taken as a starting point for the JARUS activities on the matter.

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 [28], 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

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

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, as presented in Annex D, in 2023 no consolidated and globally harmonised taxonomy of autonomy/automation, encompassing as well AI/ML exists.

On this topic, EUROCAE WG 114 is developing a new EUROCAE Report (ER-xxx, DP003) on the taxonomy of AI in aeronautical safety-related systems.

This WG, established through the ToR approved by the EUROCAE Council in 2019 [28], is working jointly with SAE G-34, which offers the opportunity to align the taxonomy across the entire transport sector.

It is recommended that EASA suggests to EUROCAE WG 114 to develop a comprehensive taxonomy, including all the rows in the Table in Annex D to this document.

8. From theory to practice: preliminary checklists for HAIKU

Aware of the intrinsic complexities emerged in the SOAR, the Consortium elaborated a dedicated methodology for the assessment of the ethical and legal requirements of the use cases covered by HAIKU. This is a three-prong approach:

1. First of all, the partners involved will be supported n the correct identification of their duties of observing compliance with the applicable EU requirements, thanks to the use of explicit open questions and suggestions
2. In light of the findings obtained, the actors will be immediately aware of the possible consequences of individuals and organizations, and on the related apportionment of responsibilities.
3. Eventually, all the actors involved will have a prompt insight on the consequences of their actions, taking into account if their effects might be limited to the duration of HAIKU or also later, in the following developing stages.

The table below shows an example of this methodology once applied. In this case, we take into consideration a critical ethical requirement for the solutions developed within HAIKU, namely the human oversight.

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

Q	Text	Who should answer		When?	
		Organisation	Human end user	During HAIKU	After HAIKU
a	Is the AI-based system designed to interact, guide or take decisions by end users that affect humans or society?	YES	NO	YES	YES
a sub 1	Could the AI-based system generate confusion for end users and/or subjects on whether a decision, content, advice or outcome is the result of an algorithmic decision?	YES	NO	YES	YES
a sub 2	Are end users and/or other subjects adequately made aware that a decision, content, advice or outcome is the result of an AI-based system?	YES	NO	NO	YES
b	Could the AI-based system generate confusion for end users and/or subjects on whether they are interacting with a human or AI-based system?	YES	NO	YES	YES
b sub 1	Are end users and/or subjects informed that they are interacting with an AI-based system?	YES	NO	NO	YES
c	Could the AI-based system affect human autonomy by generating over-reliance by end users?	YES	NO	YES	YES
c sub 1	Did you put in place procedures to avoid end users over-rely on the AI-based system?	YES	NO	NO	YES
d	Could the AI-based system affect human autonomy by interfering with the end	YES	NO	YES	YES

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

Q	Text	Who should answer		When?	
		Organisation	Human end user	During HAIKU	After HAIKU
	user's decision-making process in any other unintended and undesirable way?				
d sub 1	Did you put in place any procedure to avoid that the AI-based system inadvertently affects human autonomy?	YES	NO	NO	YES
e	Does the AI-based system simulate social interaction with or between end users and/or subjects?	YES	NO	YES	NO
f	Determine whether the AI-based system is overseen by a HIC, HITL or HOTL based on appropriate definitions	YES	NO	YES	YES
g	Have the humans, whether HIC, HITL or HOTL, been given specific training on how to exercise human oversight?	YES	NO	NO	YES
h	Did you establish any detection and response mechanisms for undesirable adverse effects (safety, security, learning assurance, explainability) of the AI-based system for the end user?	YES	NO	NO	YES
i	Did you ensure a 'stop button' or procedure for safety mitigation, to safely abort an operation when needed?	YES	NO	YES	YES
j	Did you take any specific oversight and control measures to reflect the self-learning or autonomous nature of the AI-based system?	YES	NO	YES	YES

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 4 - Human oversight. HAIKU self-assessment list

This is a sample of how we will use the results obtained by the preliminary ethical assessments provided by the ALTAI questionnaire customized for HAIKU [Annex D] as well as the findings obtained by the application of the suggestions reported in the tables concerning the legislative development requirements outlined in the Annex E and F.

The following table provides some helpful insights on the correlation between the theoretical and operational part of the documents.

Theory	Practice
Ethical framework [§ 3]	**Annex D – Checklist based on ALTAI** ➔ Tables from D.1 to D.8
Legal requirements for AI, in general [§ 4]	**Annex E – Development requirements for GAI** ➔ Safety: Tables from E.1 to E.7 ➔ Liability: Table E.7 ➔ Defectiveness: Table E.8 and E.9
Legal requirements for AI, in aviation [§ 5]	**Annex F – Applicable regulatory requirements for AI in aviation** ➔ EASA NBR: Table F.1 ➔ Essential requirements: Table F.2 ➔ AMC/GM: Table F.3 ➔ Operations and service: Table F.4 ➔ Aviation security: Table F.5 ➔ Airdrome: Table F.6
Industry standards for AI in aviation [§ 7]	**Annex G – Applicable industry standards for AI in aviation** ➔ ED-12C / DO-178C: Table G.1 ➔ EASA/EUROCAE: Table G.2 ➔ WG 72 standards: Table G.3

Table 5 – Theory and practice intersections

In the conclusions, the readers will find other operative suggestions to use these tools at the best, taking into consideration all the human, operational, technical and regulatory aspects.

Considering the ongoing debate on the ethics and regulatory issues related to the application of AI in aviation, these findings will be updated in light of the most recent references. In this regard, the pending methodological issues will be further addressed in D7.2 and D7.3.

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

9. Conclusion and recommendations

The legal and regulatory framework here outlined confirms how a proactive and future-proof compliance approach may substantially benefit the development and deployment of AI systems in and for aviation.

No doubt, the current uncertainties about the future AI regulation may raise some concerns about the most appropriate compliance strategy. However, the previous mapping of the current legal and regulatory SOA allows to identify a preliminary set of requirements that could support the design and development process from now on. Approaching potential safety and HF issues at a very early stage of technological and procedural design facilitates the minimization of future technological, economic and liability risks exposure, timely introducing the most appropriate adjustments.

This being said, the complexity of the legal framework now into force is undeniable, and this is further complicated by the uncertainties about the poor stable references specifically forwarded AI. This is the reason why, to facilitate the access to rich contents of this document and support the use of these final recommendations, this section is structured around four main questions.

1. How to tackle the current legal and regulatory uncertainties about AI in aviation?

On a global scale, the EU is playing a leading role for the development of a trustworthy AI, promoting a solid and long-term regulatory strategy to align this technological revolution with the expectations of the society and its different stakeholders. Moreover, as this deliverable highlighted, the legal and regulatory comparison with the USA demonstrates and confirms this primacy, especially in aviation law.

In this regard, from a general perspective, it is essential to remark that **the EU AI strategy relies on the principle of technological neutrality, and a risk-based attitude that informs all the proposals of the AI Legislative Initiative** (the AI Act, directly, and the AI Liability Dir., indirectly).

This understanding presents (and somehow inherits) robust similarities with the precautionary/preventive approach inspires legislators and operators in safety-critical environments. **Looking at the EU aviation law foundations, technological agnosticism and performance-based compliance thus shall continue to be the cornerstones of safety-by-design, as well as of the following safety assessment methodologies.**

In this regard, it is noteworthy that, at the end of 2022, no obstacles emerge from ICAO provisions for implementation of AI in aviation. On the other hand, US/FAA are lagging behind EU/EASA for regulation of emerging disruptive innovations, like AI/ML. For HAIKU this means that, from the regulatory perspective, it is not necessary to look at the USA, while the Project should strive to contribute to maintaining the EU leadership in this domain.

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

2. How to use these funding principles in practice, for the HAIKU use-cases design?

The final version of this deliverable, towards the end of the HAIKU project, will refer to the future consolidation of the AI Legislative Initiative and the consequent update and renewal of sectoral regulation. Meanwhile, as emerged by the analysis carried out in this document, it is essential to identify which are the research/operative areas more exposed to safety, HF and liability issues related to the use of AI within the project.

Once identified the most exposed areas, the owners of the use cases, as well as the other partners involved in the use cases design and validation activities, will have to adopt a two-stage approach. First, they shall look at norms currently prescribed by aviation law now into force. Then, they shall assess if those mandatory requirements also satisfy the expectations and compliance duties outlined by the articles of the AI specific proposals (*i.e.,* the AI Act, the AI Liability directive and the PDL.R).

According to the total system approach, the first step of this progressive analysis concerns the operational environment of the single use case. Indeed, once scoped the material context of the operations, the identification of the most impacted research areas – and, consequently, the relevant reference requirements for the operators (natural persons) and organisations involved (legal persons) – will be easier.

Operations Environment	Natural persons	Legal persons
Cockpit ATM Tower / Centre Airdrome Airport	Pilot Flight Crew ATCO Ground handlers	Air Carriers / Airlines ANSP Airport management body Ground handling companies

Table 6 -Operations Environment and Actors Mapping

Against this background and in light of the norms now into force, the list of the more sensitive research and operation areas, basically includes the areas listed immediately below. As explained, at a preliminary reading, the respective requirements can be applicable to AI systems too, notwithstanding the wording of correlate regulation does not explicitly mention these technologies. To facilitate the access to the specific guidelines provided by the deliverable, the different sets of applicable requirements are systematically reported in the reference table available in Annex F.

Norms by area	Norms by act	Requirements (tables)

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

Aviation safety	– EASA NBR – EASA ERs – Regulation on management systems – EASA soft rules on system safety assessment	Table F. 1 - AI in Articles of EASA Basic Regulation on aviation safety Table F. 2 - Essential Requirements on aviation safety applicable to AI
Design and production	– Regulations on design and production	Table F. 3 - EC Regulations on design and production . AMC/GM applicable to AI
Operations and service provision	– Regulations on operations and service provisions	Table F. 4 - EC Regulations on operations and service provision. Rules applicable to AI
Aviation security	– Regulations on aviation security – EASA soft rules for aerodromes	Table F. 5 - EU Regulations on aviation security. Paragraphs applicable to AI Table F. 6 - EASA soft rules on aerodromes applicable to AI
Cyber-security	– EASA NBR – ITU deliverables – Regulation on management systems – EASA soft rules on software – EASA soft rules on cyber-security	Table F. 5 - EU Regulations on aviation security. Paragraphs applicable to AI

Table 7 -- Norms and Requirements Mapping

Once this first assessment about mandatory requirements is concluded, the owners of the use cases, as well as the partners involved in the cases design and validation, will have a preliminary picture of the level of compliance of the related scenarios and useful indicators to improve it in future.

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. How to assure organisations and operators involved in HAIKU from AI-related safety and liability risks?

Eventually come the issues specifically related to the material implementation of AI systems in aviation, and the possible consequences of these organisational choices on the safety and liabilities risks of the actors involved (natural and legal persons).

Implicitly, here we are before a grey area, where the regulation, as well as the respective requirements, are not stable yet. Nonetheless, opting for the proactive approach that traditionally informs aviation law, it is advisable to carry out a last cross-check between mandatory and the AI non-specific requirements provided by aviation law and the new requirements suggested by the ongoing-discussed proposals generated by the HLEG AI Ethics Guidelines and the EU AI Legislative Initiative.

In this regard, it is advisable to firstly address the potential issues arising from the level of automation and the role of the human agents. Once considered this aspect, the attention should then converge on the operative questions to assess the specific ethics and legal risks. Further references are available in annex F.

It is essential to highlight that operators and organisations should run a comprehensive risk assessment for any newly introduced AI application, taking into consideration technical, organisational, and human factors into a unitary framework of analysis.

4. How can regulatory authorities support the compliant development of a trustworthy AI?

In this regard, the role of competent regulatory and certification authorities will be crucial, especially in the cases involving the use of high-risk safety critical AI applications. EASA and JARUS already announced the intention to update existent requirements to consider high levels of automation of the airspace environment in the future – and this with the primary aim to properly manage this transition avoiding further jeopardising harmonisation.

However, the pending normative uncertainties need to be addressed and mitigated also in the transitional period. Particular attention should be paid to SMEs involved in the design and development of innovative AI solutions. These entities should receive adequate and proactive advisory support – both from the technical and legal standpoints - during the initial period after introduction of new AI applications, receiving feedback from the authorities as well as from involved personnel. This collaboration should then continue throughout the entire life cycle of the AI systems, at least until the stabilisation of the current normative framework.

Annex A - List of acronyms

Table A. 1 - List of Acronyms

Acronym	Term
AC	Advisory Circular
ACARS	Aircraft Communications Addressing and Reporting System
ACSA	Agencia Centroamericana para la Seguridad Aeronáutica
ADR	Aerodrome
ADS	Automatic Dependent Surveillance (Aviation)
ADS	Automated Driving System (Automotive)
AeMC	Aero-Medical Centres (AeMC)
AI	Artificial Intelligence
AIS	Aeronautical Information Service (or System)
ALTAI	Assessment List for Trustworthy Artificial Intelligence
AltMOC	Alternative Means of Compliance
AMC	Acceptable Means of Compliance
AMMD	Airport Moving Map Display
AMS	Apron Management Service
ANS	Air Navigation Services
ANSI	American National Standard Institute
ANSP	Air Navigation Service Provider
AOC	Aircraft Operator Certificate
AOC	Aeronautical Operational Control
ASTM	American Society for Testing and Materials
ATC	Air Traffic Control

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

ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
ATO	Approved Training Organisation
CAMO	Continuing Airworthiness Management Organisation
CAT	Commercial Air Transport
CDI	Compliance Demonstration Items
CIS	Common Information Service
CS	Certification Specifications
CSC	Cloud Service Customer
CEN	Comitè Europeènne de Normalisation
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CMO	Compliance Monitoring Officer
CS	Certification Specifications
CS-ADR-DSN	Certification Specifications on Aerodrome Design
CU	Command Unit to pilot a UAS
DAH	Design Approval Holder
DAL	Design Assurance Level
DDT	Dynamic Driving Task
DOA	Design Organisation Approval
DPO	Data Protection Officer
DSN	Design
EAAI HLG	European Aviation/ATM AI High Level Group
EAR	Easy Access Rules
EASA	European Union Aviation Safety Agency

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

EBT	Evidence-Based Training
EC	European Commission
ECCSA	European Centre for Cybersecurity in Aviation
ECHR	European Convention of Human Rights
ED	Executive Director
EFB	Electronic Flight Bag
ENISA	EU Network and Information Systems Agency
EP	European Parliament
EPAS	European Plan for Aviation Safety
EPRS	European Parliament Research Service
ER	Essential Requirement
ETSO	European Technical Standard Order
EU	European Union
EUCFR	EU Charter of Fundamental Rights
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FCL	Flight Crew Licencing
FDM	Flight Data Monitoring
FG	Focus Group
FG AC	Focus Group on Aviation Applications of Cloud Computing for Flight Data Monitoring
FIS	Flight Information Service
FSTD	Flight Simulation Training Device
GDPR	General Data Protection Regulation (reg. EU 2016/679)
GM	Guidance Material

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

HF	Human Factors
HIC	Human-In-Command
HITL	Human-In-The-Loop
HLEG	High Level Expert Group (on AI)
HMI	Human-Machine Interface
HOS	Health and Occupational Safety
HOTL	Human-On-The-Loop
HW	Hardware
ICA	Instructions for Continuing Airworthiness
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission.
IMS	Integrated Management System
ISMS	Information Security Management Systems
ISO	International Standard Organisation
ITU	International Telecommunications Union
IUEI	Intentional Unauthorised Electronic Interaction
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
LoI	Level of Involvement
MOA	Maintenance Organisation Approval
MoC	Means of Compliance
MOPS	Minimum Operational Performance Standard
ML	Machine Learning
MS	Member States

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

MTBF	Mean Time Between Failures
MTOM	Maximum Take-Off Mass
NAS	National Airspace. System
NB	Notified Body
NBR	New Basic Regulation
NIS	Network and Information Systems
ODD	Operational Design Domain
ODP	Open Distributed Processing
OEDR	Object and Event Detection and Response
OJ	Official Journal
PBR	Performance-Based Regulation
PISRA	Product Information Security Risk Assessment
PLD	Product Liability Directive (5/374/EEC, consolidated version)
PLD.R	Proposal for a Dir. on liability for defective products (COM/2022/495 final)
POA	Production Organisation Approval
QE	Qualified Entity
QMS	Quality Management System
RBR	Risk-Based Regulation
RSOO	Regional Safety Oversight Organisation
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SAFO	Safety Officer
SARPs	Standards and Recommended Practices
SC	Special Committee (or Sub-Committee)

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

SDO	Standard Development Organisation
SECO	Security Officer
SHELL	Software, Hardware, Environment, Liveware, Liveware
SIA	Safety Investigation Authorities
SLA	Service Level Agreement
SME	Small or Medium-sized Enterprise
SMM	Safety Management Manual
SMS	Safety Management System
SOAR	State of the Art Review
SORA	Specific Operation Risk Assessment
SP	Service Provider
SW	Software
SWAL	Software Assurance Level
TCO	Third Country Operator
TEU	Treaty of the European Union
TFEU	Treaty on the Functioning of the EU
ToR	Terms of Reference
TSAG	Telecommunication Standardisation Advisory Group
UAM	Urban Air Mobility
UAS	Unmanned Aircraft Systems
UML	Unified Modelling Language
UTM	UAS Traffic Management

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

Annex B - Definitions

Table B. 1 - Definitions

Term	Definition	Source	Reference
[Non-personal] data	data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679 (see: personal data)	Reg. EU 2018/1807	Article 3(1)
Artificial intelligence systems	software that is developed with one or more of the techniques and approaches listed in Annex I [e.g., machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines,(symbolic) reasoning and expert systems; statistical approaches, Bayesian estimation, search and optimization methods] and can, for given set of human-defined objectives, generate outputs such as contents, predictions, recommendations, or decisions influencing the environments they interact with	AI Act (COM/2021/206 final)	Article 3(1)
Automation	The use of machines or computers instead of people to perform a task (Adapted from ASTM TR-1 EB).	Adapted from ASTM TR-1 EB	
Autonomous aircraft	An unmanned aircraft that does not allow pilot intervention in the management of the flight	ICAO Circ 328 AN/190	
Autonomous systems	Have the ability and authority of decision making, problem-solving, and/or self-governance under possibly bounded, variable, or abnormal conditions (Deterministic or Non-	JARUS, 2022	

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

	deterministic; Adapted from National Research Council of Canada).		
Aviate	The tasks required to be performed to manage the flight dynamics of an aircraft safely	Adapted from ASTM TR-1 EB	
Biometric categorisation system	an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data	AI Act (COM/2021/206 final)	Article 3(35)
Biometric data	personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data	AI Act (COM/2021/206 final) Reg. EU 2016/79	Article 3(33) Article 4(14)
CE marking of conformity (CE marking)	a marking by which a provider indicates that an AI system is in conformity with the requirements set out in Title III, Chapter 2 [Requirement for high-risk AI systems] of [the AI Act] and other applicable Union legislation harmonising the conditions for the marketing of products ('Union harmonisation legislation') providing for its affixing	AI Act (COM/2021/206 final)	Article 3(24)
Claim for damages	a non-contractual fault-based civil law claim for compensation of the damage caused by an output of an AI system or the failure of such a system to produce an output where such an output should have been produced	AI Liability (COM/2022/496 final)	Article 2(5)
Claimant	a person bringing a claim for damages that: (a) has been injured by an output of an AI system or by the failure of such a system to produce an output where such an output should have been produced; (b) has succeeded to or has been subrogated to the right of an injured person by virtue of law or contract; or (c) is acting on behalf of one or more injured	AI Liability (COM/2022/496 final)	Article 2(6)

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

	persons, in accordance with Union or national law		
Common specifications	a document, other than a standard, containing technical solutions providing a means to, comply with certain requirements and obligations established under [the AI Act]	AI Act (COM/2021/206 final)	Article 3(28)
Communicate	The tasks required to integrate an aircraft into airspace with other airspace users safely.	JARUS, 2022	
Component	any item, whether tangible or intangible, or any related service, that is integrated into, or inter-connected with, a product by the manufacturer of that product or within that manufacturer's control	PLD.R (COM/2022/495 final	Article 4(3)
Conformity assessment	the process of verifying whether the requirements set out in Title III, Chapter 2 [Requirement for high-risk AI systems] of [the AI Act] relating to an AI system have been fulfilled	AI Act (COM/2021/206 final)	Article 3(20)
Conformity assessment body	a body that performs third-party conformity assessment activities, including testing, certification and inspection	AI Act (COM/2021/206 final)	Article 3(21)
Damage	material losses resulting from: death or personal injury, including medically recognised harm to psychological health; (b) harm to, or destruction of, any property, except: (i) the defective product itself; (ii) a product damaged by a defective component of that product; (iii) property used exclusively for professional purposes;	PLD.R (COM/2022/495 final	Article 4(6)
Data	data as defined in Article 2, point (1), of Regulation (EU) 2022/868 of the European Parliament and of the Council *i.e. «any digital representation of acts, facts or information and any compilation of such acts,*	PLD.R (COM/2022/495 final	Article 4(6)

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

	facts or information, including in the form of sound, visual or audiovisual recording» [Reg. EU 2022/868 (DGA)]		
Defendant	the person against whom a claim for damages is brough	AI Liability (COM/2022/496 final)	Article 2(8)
Degraded mode	Refers to a system that has lost a functional capability, but may continue to operate safely under defined limitations	JARUS, 2022	
Duty of care	a required standard of conduct, set by national or Union law, in order to avoid damage to legal interests recognised at national or Union law level, including life, physical integrity, property and the protection of fundamental rights	AI Liability (COM/2022/496 final)	Article 2(8)
Emotion recognition system	an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data	AI Act (COM/2021/206 final)	Article 3(34)
Harmonised standard	a European standard as defined in Article 2(1)(c) of Regulation (EU) No 1025/2012 *i.e., «* ‘standard’ means a technical specification, adopted by a recognised standardisation body, for repeated or continuous application, with which compliance is not compulsory, and which is one of the following: ‘international standard’ means a standard adopted by an international standardisation body; ‘European standard’ means a standard adopted by a European standardisation organisation; ‘harmonised standard’ means a European standard adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation;	AI Act (COM/2021/206 final)	Article 3(27)

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

	'national standard' means a standard adopted by a national standardisation body»		
Human-in-the-Loop	A system control method where a human directly provides inputs and evaluates outputs to manage system parameters	Adapted from ASTM TR-1 EB	
Human-machine symbiosis	The highest level of integration that can be achieved between the human and the system with the goal of seamlessly sharing airspace & operational information and intention	adapted from Symbiotic Systems Whitepaper, JARUS, 2022	
Human-off-the-Loop	A method of system control in which no human is monitoring the system control. A machine provides inputs and evaluates outputs to manage system parameters	Adapted from ASTM TR-1 EB "Human-out-of-the-Loop"	
Human-on-the-Loop	A method of system control in which a human monitors a machine that provides inputs and evaluates outputs to manage system parameters. The human may take over the control at any point (come into the loop)	Adapted from ASTM TR-1 EB	
Input data	data provided to or directly acquired by an AI system on the basis of which the system produces an output	AI Act (COM/2021/206 final)	Article 3(32)
Instructions for use	the information provided by the provider to inform the user of in particular an AI system's intended purpose and proper use, inclusive of the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used	AI Act (COM/2021/206 final)	Article 3(15)
Intended purpose	the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales	AI Act (COM/2021/206 final)	Article 3(12)

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

	materials and statements, as well as in the technical documentation		
Manufacturer	any natural or legal person who develops, manufactures or produces a product or has a product designed or manufactured, or who markets that product under its name or trademark or who develops, manufactures or produces a product for its own use	PLD.R (COM/2022/495 final	Article 4(11)
Manufacturer's control	the manufacturer of a product authorises a) the integration, inter-connection or supply by a third party of a component including software updates or upgrades, or b) the modification of the product	PLD.R (COM/2022/495 final	Article 4(5)
Navigate	The tasks required to be performed to safely aviate an aircraft from one point of reference to another	Adapted from ASTM TR-1 EB	
Object and Event Detection and Response OEDR	The subtasks of the dynamic flight task that include monitoring the flying environment (detecting, recognizing, and classifying objects and events and preparing to respond as needed) and executing an appropriate response to such objects and events	Adapted from SAE J3016	
Operational design domains (odd)	Operating conditions under which a given autonomous flight system or feature thereof is specifically designed to function, including environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of specific operational characteristics (Adapted from SAE J3016). When defining an ODD the function of the feature or system in normal, contingency, and emergency operations should be considered	JARUS, 2022	
Operator	the provider, the user, the authorised representative, the importer and the distributor	AI Act (COM/2021/206 final)	Article 3(8)

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

Performance of an AI system	the ability of an AI system to achieve its intended purpose	AI Act (COM/2021/206 final)	Article 3(18)
Personal data	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	Reg. EU 2016/679 (GDPR)	Article 4(1)
Phase of Flight	For this document, phase of flight refers to a period within a flight including ground operations. In the case of a human-occupied aircraft, a flight begins when any person boards the aircraft with the intention of flight and continues until all such persons have disembarked. In the case of an unoccupied aircraft, a flight begins when the aircraft is ready to move with the purpose of flight and continues until it comes to rest at the end of the flight and the primary propulsion system is shut down	From CAST Common Taxonomy, JARUS, 2022	
Potential claimant	a natural or legal person who is considering but has not yet brought a claim for damages	AI Liability (COM/2022/496 final)	Article 2(7)
Product	all movables, even if integrated into another movable or into an immovable. 'Product' includes electricity, digital manufacturing files and software	PLD.R (COM/2022/495 final	Article 4(1)
Professional user	a natural or legal person, including a public authority or a body governed by public law, using or requesting a data processing service for purposes related to its trade, business, craft, profession or task	Reg. EU 2018/1807	Article 3(8)

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

Provider	a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge	AI Act (COM/2021/206 final)	Article 3(2)
Putting into service	the supply of an AI system for first use directly to the user or for own use on the Union market for its intended purpose	AI Act (COM/2021/206 final)	Article 3(11)
Putting into service	the first use of a product in the Union in the course of a commercial activity, whether in return for payment or free of charge, in circumstances in which the product has not been placed on the market prior to its first use	PLD.R (COM/2022/495 final	Article 4(10)
Reasonably foreseeable misuse	the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems	AI Act (COM/2021/206 final)	Article 3(13)
Related service	a digital service that is integrated into, or inter-connected with, a product in such a way that its absence would prevent the product from performing one or more of its functions	PLD.R (COM/2022/495 final	Article 4(4)
Safety component of a product or system	a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property	AI Act (COM/2021/206 final)	Article 3(14)
Serious incident	any incident that directly or indirectly leads, might have led or might lead to any of the following: (a) the death of a person or serious damage to a person's health, to property or the environment, (b) a serious and irreversible	AI Act (COM/2021/206 final)	Article 3(44)

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

	disruption of the management and operation of critical infrastructure.		
Substantial modification	a change to the AI system following its placing on the market or putting into service which affects the compliance of the AI system with the requirements set out in Title III, Chapter 2 [Requirement for high-risk AI systems] of [the AI Act] or results in a modification to the intended purpose for which the AI system has been assessed	AI Act (COM/2021/206 final)	Article 3(23)
Testing data	data used for providing an independent evaluation of the trained and validated AI system in order to confirm the expected performance of that system before its placing on the market or putting into service	AI Act (COM/2021/206 final)	Article 3(31)
Training data	data used for training an AI system through fitting its learnable parameters, including the weights of a neural network	AI Act (COM/2021/206 final)	Article 3(29)
User	any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity	AI Act (COM/2021/206 final)	Article 3(4)
Validation data	data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process, among other things, in order to prevent overfitting; whereas the validation dataset can be a separate dataset or part of the training dataset, either as a fixed or variable split	AI Act (COM/2021/206 final)	Article 3(30)

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

Annex C - Levels of Automation/Autonomy/Human Oversight

Several taxonomies of the automation levels and of the related human role are available, among which those published in the EASA guidance for Level 1 machine learning applications, joint SAE/ISO J3016 [120]and that under development in the JARUS methodology for evaluation of autonomy.

The EASA, ISO/SAE and JARUS taxonomies are compared in the table below:

Table C. 1 - Levels of automation/autonomy. Comparative taxonomy

EASA Level	JARUS Level	SAE	Nickname	Description	Role of human
No equivalent	0	0	Manual Operation (No driving automation)	JARUS: No automation SAE: The performance by the driver of the entire Dynamic Driving Task (DDT), even when enhanced by active safety systems	Crew responsible for all functions including controlling the aircraft, evaluating and responding to aircraft and airspace environments, communicating with external systems, and managing the aircraft when failures present themselves
1A	No equivalent	No equivalent	Human augmentation	Automation support to information acquisition Automation support to information analysis	Human in Command (HIC): all decisions are taken by the human
1B	1	1	Human assistance (Assisted Operation)	EASA: Automation support to decision-making JARUS: Systems supporting crew in performing the specified function. SAE: Sustained and ODD-specific execution by a driving automation system of either the lateral or the longitudinal vehicle motion control subtask of the DDT (but not	HIC/HITL

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

EASA Level	JARUS Level	SAE	Nickname	Description	Role of human
				both simultaneously) with the expectation that the driver performs the remainder of the DDT	
2	2	2	Human-AI collaboration (Task Reduction) (Partial driving automation)	EASA: Overseen and overridable automatic decision-making Overseen and overridable automatic action implementation JARUS: System may take over a specific task or function to help crew focus on more mission critical tasks. SAE: Sustained and ODD-specific execution by a driving automation system of both the lateral and longitudinal vehicle motion control subtasks of the DDT with expectation that the driver completes the OEDR subtask and supervises the driving automation system.	Human-in-the-Loop (HITL) Human may override any automatic action
3A	3	3	More autonomous AI (Supervised Automation)(Conditional Driving Automation = Fallback ready user)	EASA: Overridable automatic decision-making Overridable automatic action implementation JARUS: System handles aircraft functions and also monitors and responds to changes in	HITL

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

EASA Level	JARUS Level	SAE	Nickname	Description	Role of human
				the environment. Crew moves from actively managing the function to monitoring the safety and effectiveness of the operational outcomes. SAE: The sustained and ODD-specific performance by an ADS of the entire DDT with the expectation that the DDT fallback- ready user is receptive to ADS-issued requests to intervene, as well as to DDT performance-relevant system failures in other vehicle systems, and will respond appropriately.	
No equivalent	4	4	High Automation	JARUS: Crew may trust one or more flight systems to perform their function because technology has demonstrated ability to perform entire tasks or functions effectively and have a robust capability to respond to their environment autonomously (i.e. without human supervision).	Human-on-the-Loop (HOTL)

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

EASA Level	JARUS Level	SAE	Nickname	Description	Role of human
				SAE: Sustained and ODD-specific performance by an ADS of the entire DDT and DDT fallback without any expectation that a user will need to intervene.	
3B	5	5	Fully autonomous AI (Full driving automation)	EASA: Non-overridable automatic decision-making, JARUS: At the far end of the spectrum is a fully autonomous function. SAE: Sustained and unconditional (i.e., not ODD-specific) performance by an ADS of the entire DDT and DDT fallback without any expectation that a user will need to intervene	Human-on-the-Loop (HOTL) JARUS: At this level of automation there is neither human involvement in the function, and likely nor human awareness of dynamic operational parameters
No Equivalent	No numerical level specified	No equivalent	Trusted Autonomy	Deployment of trusted autonomous systems results from the optimised balance of human and machine tasks with a focus on integrity metrics defined to support safe and efficient airspace operations.	As autonomy increases, the human needs to build trust in the machine and the machine needs to build trust in the human

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

EASA Level	JARUS Level	SAE	Nickname	Description	Role of human
				Trusted autonomy can be considered a pathway to progressively remove the inherent limitations of full autonomy as known in 2023	

There could be scope for harmonisation of the above taxonomy on the global scale and even beyond 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

Annex D - Ethics Principles and Requirements for the ALTAI

As explained, this deliverable relies and referred to the most relevant and well-established principles and requirements, as detailed by HLEG in its guidance materials.

The paragraphs that follow provide a more in-depth analysis of these principles and requirements. More punctual information about the impact of these within the HAIKU project is available at §§.

1. Ethics Principles

As firs, there is the principle of **respect for human autonomy**. According to the European fundamental rights tradition, this is directed towards ensuring respect for the freedom and autonomy of human beings. In this regard, humans interacting with AI systems must be able to keep full and effective self-determination over themselves, profitably and freely taking part in the life of their communities. This is why AI-powered solutions should not unjustifiably subordinate, coerce, deceive, manipulate, condition or herd humans. Instead, since the early stage of their design, they should be oriented to augment, complement and empower human cognitive, social and cultural skills, following human-centric understanding of these technologies over their whole lifecycle.

Secondly, there is the principle of **prevention of harm**; a milestone of applied ethics (especially of bioethics). As any other technology, procedure or practice, AI systems should neither cause nor exacerbate harm or otherwise adversely affect human beings. This is consistent and extent in this domain the traditional protection of human dignity as well as mental and physical integrity. AI systems, as well as the environments in which they operate must be safe and secure, ensuring technically robust solutions and preventive and precautionary measures to avoid or impede they are open to malicious use. Particular attention should be addressed to vulnerable persons and asymmetric relationships. On the one hand, vulnerable people and groups should receive greater attention and be included in the development, deployment and use of AI systems. On the other hand, AI strategies specifically addressed to contexts characterized by asymmetries of power or information, such as between employers and employees, businesses and consumers or governments and citizens should take into account the disparate and adverse impacts potentially related to technological innovation. Not least, preventing harm also entails consideration of the natural environment and all living beings.

Analogous attentions should be paid to the principle of **fairness**, intended in its substantive and procedural dimension. From one side, from a substantial standpoint, fair AI system should aim at ensuring equal and just distribution of both benefits and costs, and ensuring that individuals and groups are free from unfair bias, discrimination and stigmatisation. Moreover, the use of AI systems should never lead to people being deceived or unjustifiably impaired in their freedom of choice. Additionally, fairness implies that AI practitioners should respect the principle of proportionality between means and ends, and consider carefully how to balance competing interests and objectives.

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

On the other, considering the procedural dimension, fairness entails the ability to contest and seek effective redress against decisions made by AI systems and by the humans operating them.

Eventually (but not less relevant) comes the principle of **explicability**, implicitly connected with fairness expectations and claims. This is one of the more crucial and debate desideratum for building and maintaining users' trust in AI systems. This principle basically aims to promote and ensure that processes, capabilities and purpose of AI systems can be openly communicated, and so far the decisions – to the extent possible – can be explainable to those directly and indirectly affected. In this regard, it has to be highlighted that an explanation as to why a model has generated a particular output or decision (and what combination of input factors contributed to that) is not always possible. These cases are referred to as 'black box' algorithms and require special attention. In those circumstances, other explicability measures (e.g. traceability, auditability and transparent communication on system capabilities) may be required, provided that the system as a whole respects fundamental rights. The degree to which explicability is needed may highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate. Nonetheless, the essential content of this principle implicitly represents a functional enabler of the other principles, establishing the essential conditions for their realization ex ante and ex post.

2. Ethics requirements

Human agency and oversight, as a requirement, aims to orient the development of AI to the respect of fundamental rights, hampering human agency and oversight in HMIs. Users should be empowered by the use of AI, avoiding any potential negative consequence. Automation therefore should be coupled with appropriate guarantees by design and by default enabling reasonable self-assessment procedures. In addition, governance mechanisms should always ensure effective protection of human autonomy and self-determination, prioritizing human-centred approaches (e.g., human-in-the-loop (HITL), human-on-the-loop (HOTL), or human-in-command (HIC)).

Technical robustness and safety, instead, refers to all the precautions and remedies aimed at preventing harms related to technical and environmental issues in HMI. In this regard, the scope of this requirement encompasses all the strategies and initiatives addressed to mitigate the vulnerabilities and contrast the attacks of potential adversaries. This set of measures should consider attacks targeting data, models and infrastructures, minimizing risks related to data poisoning and model leaking. AI systems should have safeguards that enable a fallback plan in case of problems. The level of safety measures required depends on the magnitude of the risk posed by an AI system, which in turn depends on the system's capabilities. Accuracy, reliability and reproducibility of the results obtained by an AI systems are essential premises to ensure and promote a reliable development, deployment and use of these technologies.

Privacy and data governance requirements cover all the ethical and legal issues related to the protection of fundamental rights, firstly considering those directly affected by a massive processing 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

data and information. Privacy, in this connection, should be intended as a comprehensive set of interests ranging from the respect of human dignity and respect of private life to informational self-determination. Guarantees and remedies aimed at insuring the quality and integrity of data, as well as access to dataset are implicit and substantive corollaries of these assumptions.

Transparency, as a principle, encompasses several relevant element of AI, including data, systems and business models. In this connection, as a requirement, transparency includes all the measures and remedies aimed at ensure the ability to explain both the technical processes of an AI system and the related human decisions, both from a technical and organisational perspective. Implicitly, this presume the data sets and the processes yield the AI system’s decision should be documented to the best possible standard to allow for traceability and an increase in transparency. Human should also be always aware of interacting with a machine, facilitating communication of the AI system's level of accuracy, as well as its limitations.

Diversity, non-discrimination and fairness, jointly considered, ensure the enablement inclusion and diversity throughout the entire AI system’s life cycle. In this regard, to avoid unfair biases or unintended (in)direct prejudice and discrimination, data sets used by AI systems (both for training and operation) should be free by inadvertent historic bias, incompleteness and bad governance models. To develop AI systems that are trustworthy, it is advisable to consult stakeholders who may directly or indirectly be affected by the system. Moreover, systems should be user-centric and designed in a way that allows interested people to use AI products or services, regardless of their age, gender, abilities or characteristics.

Societal and environmental wellbeing, as a requirement, in line with the principles of fairness and prevention of harms, fosters a broader approach to AI impact assessment, encompassing also the societal and contextual concerns connected to the technological innovation. In this connection, AI should be sustainable and environmentally friendly, helping tackling some of the most pressing societal concerns. Moreover, the spread of these systems should not negatively alter the conception of social agency, or impact our social relationships and attachment. The effects of these systems must therefore be carefully monitored and considered. This impact should also be assessed from a societal perspective, taking into account its effect on institutions, democracy and society at large.

Accountability implicitly refers to all the requirements aimed at ensuring auditability, minimisation and reporting of negative impact, trade-offs and redress. Basically, it necessitates that mechanisms be put in place to ensure responsibility and accountability for AI systems and their outcomes, both before and after their development, deployment and use. If auditability entails the enablement of the assessment of algorithms, data and design processes, mitigation and reporting strategies include both the ability to report on actions or decisions that contribute to a certain system outcome, and to respond to the consequences of such an outcomes. Moreover, when unjust adverse impact occurs, accessible mechanisms should be foreseen that ensure adequate redress.

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. The value of EU AI Ethics Principles in a global landscape

Obviously, different contexts and AI systems may require specific adjustments and adaptations, according to the specific ethical issues and needs of the related scenarios [91, p. 6]. Aviation, in particular, requires a more specific and context-based approach. This sector, indeed, relies not only on EU based legislation, but on international law and treaties with specific scope and sectoral approach.

In this regard, over the last few years, we have witnessed a recent blooming of a number of ethical guidelines and charters, often inspired by different philosophical and sociological bases. As observed, this is gradually frustrating the practical utility of these document, frequently leading to overlapping or contrast among the many principles there established [110].

For this reason, the HAIKU Consortium opted for this minimalist and EU-based approach, relying on generalist eminent documents. However, taking into consideration the international and non-EU limited nature of aviation, the Consortium also takes into consideration the need to reconcile its approach with the global AI ethical discourse. In this regard, thanks to a solid and accredited comparative literature review [88], the project ethics framework tentatively refers to 5 common principles of AI ethics:

a. **Benefiance**, indented as promoting well-being, preserving dignity, and sustaining the planet
b. **Nonmalificiance**, as preventing and mitigating harms to privacy, security and fundamental rights and interests
c. **Autonomy**, as the power of decision-making and self-determination
d. **Justice**, as promoting prosperity, preserving solidarity and avoiding unfairness
e. **Explicability**, as essential enabler of the other principles through intelligibility and accountability

Being in line with this basic taxonomy, the HAIKU ethics framework can dialogue not only with the principles recognized and established within the EU for the AI ethics, but also other international specific and non-specific references that could support the development of these technologies on a global scale [88, p. 10].

4. ALTAI Checklist for the purposes of HAIKU

Table D. 1 – Human agency and oversight

Requirement #1 HUMAN AGENCY AND OVERSIGHT
HUMAN AGENCY AND AUTONOMY

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

No.	Question	YES	NO	Why?
1	Is the AI system designed to interact, guide or take decisions by human end-users that affect humans or society?			
1.1	Could the AI system generate confusion for some or all end-users or subjects on whether a decision, content, advice or outcome is the result of an algorithmic decision?			
2	Could the AI system generate confusion for some or all end-users or subjects on whether they are interacting with a human or AI system?			
3	Could the AI system affect human autonomy by generating over-reliance by end-users?			
4	Could the AI system affect human autonomy by interfering with the end-user's decision-making process in any other unintended and undesirable way?			
4.1	Did you put in place any procedure to avoid that the AI system inadvertently affects human autonomy?			
HUMAN OVERSIGHT				
No.	**Question**	**YES**	**NO**	**Why?**
1	Have the humans (human-in-the-loop, human-on-the-loop, human-in-command) been given specific training on how to exercise oversight?			
2	Did you establish any detection and response mechanisms for undesirable adverse effects of the AI system for the end-user or subject?			
3	Did you ensure a 'stop button' or procedure to safely abort an operation when needed?			

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	Did you take any specific oversight and control measures to reflect the self-learning or autonomous nature of the AI system?			

Table D. 2 - Technical robustness and safety

Requirement #2 TECHNICAL ROBUSTNESS AND SAFETY				
RESILIENCE TO ATTACK AND SECURITY				
No.	**Question**	**YES**	**NO**	**Why?**
1	Could the AI system have adversarial, critical or damaging effects (e.g. to human or societal safety) in case of risks or threats such as design or technical faults, defects, outages, attacks, misuse, inappropriate or malicious use?			
2	Is the AI system certified for cybersecurity (e.g. the certification scheme created by the Cybersecurity Act in Europe)19 or is it compliant with specific security standards?			
3.1	Did you assess potential forms of attacks to which the AI system could be vulnerable?			
3.2	Did you consider different types of vulnerabilities and potential entry points for attacks such as:			
3.2.1	Data poisoning (i.e. manipulation of training data);			
3.2.2	Model evasion (i.e. classifying the data according to the attacker's will);			
3.2.3	Model inversion (i.e. infer the model parameters)			
4	Did you put measures in place to ensure the integrity, robustness and overall security of the AI system against potential attacks over its lifecycle?			
GENERAL SAFETY				

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

No.	Question	YES	NO	Why?
1	Did you define risks, risk metrics and risk levels of the AI system in each specific use case?			
1.1.	Did you put in place a process to continuously measure and assess risks?			
2	Did you identify the possible threats to the AI system (design faults, technical faults, environmental threats) and the possible consequences?			
2.1	Did you assess the risk of possible malicious use, misuse or inappropriate use of the AI system?			
2.2	Did you define safety criticality levels (e.g. related to human integrity) of the possible consequences of faults or misuse of the AI system?			
3	Did you assess the dependency of a critical AI system's decisions on its stable and reliable behaviour?			
3.1	Did you align the reliability/testing requirements to the appropriate levels of stability and reliability?			
4	Did you plan fault tolerance via, e.g. a duplicated system or another parallel system (AI-based or 'conventional')?			
ACCURACY				
No.	**Question**	**YES**	**NO**	**Why?**
1	Could a low level of accuracy of the AI system result in critical, adversarial or damaging consequences?			
2	Did you put in place measures to ensure that the data (including training data) used to develop the AI system is up-to-date, of high quality, complete and representative of the environment the system will be deployed in?			

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	Did you put in place a series of steps to monitor, and document the AI system's accuracy?			
4	Did you consider whether the AI system's operation can invalidate the data or assumptions it was trained on, and how this might lead to adversarial effects?			
5	Did you put processes in place to ensure that the level of accuracy of the AI system to be expected by end-users and/or subjects is properly communicated?			
RELIABILITY, FALL-BACK PLANS AND REPRODUCIBILITY				
No.	**Question**	**YES**	**NO**	**Why?**
1	Could the AI system cause critical, adversarial, or damaging consequences (e.g. pertaining to human safety) in case of low reliability and/or reproducibility?			
1.1	Did you put in place a well-defined process to monitor if the AI system is meeting the intended goals?			
1.2	Did you test whether specific contexts or conditions need to be taken into account to ensure reproducibility?			
2	Did you put in place verification and validation methods and documentation (e.g. logging) to evaluate and ensure different aspects of the AI system's reliability and reproducibility?			
2.1	Did you clearly document and operationalise processes for the testing and verification of the reliability and reproducibility of the AI system?			
3	Did you define tested failsafe fallback plans to address AI system errors of whatever origin and put governance procedures in place to trigger them?			

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	Did you put in place a proper procedure for handling the cases where the AI system yields results with a low confidence score?			
5	Is your AI system using (online) continual learning?			
5.1	Did you consider potential negative consequences from the AI system learning novel or unusual methods to score well on its objective function?			

Table D. 4 - Privacy and Data Governance

Requirement #3 PRIVACY & DATA GOVERNANCE				
DATA GOVERNANCE				
No.	Question	YES	NO	Why?
1	Did you consider the impact of the AI system on the right to privacy, the right to physical, mental and/or moral integrity and the right to data protection?			
2	Depending on the use case, did you establish mechanisms that allow flagging issues related to privacy concerning the AI system?			
3	Did you consider the privacy and data protection implications of the AI system's non-personal training-data or other processed non-personal data?			
4	Did you align the AI system with relevant standards (e.g. ISO, IEEE) or widely adopted protocols for (daily) data management and governance?			

Table D. 5 - Transparency

Requirement #4 TRANSPARENCY				
EXPLAINABILITY				
No.	Question	YES	NO	Why?

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	Did you explain the decision(s) of the AI system to the users?			
2	Do you continuously survey the users if they understand the decision(s) of the AI system?			
COMMUNICATION				
No.	**Question**	**YES**	**NO**	**Why?**
3	In cases of interactive AI systems (e.g., chatbots, digital assistant), do you communicate to users that they are interacting with an AI system instead of a human?			

Table D. 6 - Diversity, non-discrimination and fairness

Requirement #5 DIVERSITY, NON-DISCRIMINATION AND FAIRNESS				
AVOIDANCE OF UNFAIR BIAS				
No.	**Question**	**YES**	**NO**	**Why?**
1	Did you establish a strategy or a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data as well as for the algorithm design?			
2	Did you consider diversity and representativeness of end-users and/or subjects in the data?			
2.1	Did you test for specific target groups or problematic use cases?			
2.2	Did you research and use publicly available technical tools, that are state-of-the-art, to improve your understanding of the data, model and performance?			
2.3	Did you assess and put in place processes to test and monitor for potential biases during the entire lifecycle of the AI system (e.g. biases due to possible limitations stemming			

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

	from the composition of the used data sets (lack of diversity, non-representativeness)?			
2.4	Where relevant, did you consider diversity and representativeness of end-users and or subjects in the data?			
4	Did you ensure a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system?			
4.1	Did you establish clear steps and ways of communicating on how and to whom such issues can be raised?			
4.2	Did you identify the subjects that could potentially be (in)directly affected by the AI system, in addition to the (end-)users and/or subjects?			
5	Is your definition of fairness commonly used and implemented in any phase of the process of setting up the AI system?			
5.1	Did you consider other definitions of fairness before choosing this one?			
5.3	Did you ensure a quantitative analysis or metrics to measure and test the applied definition of fairness?			
5.4	Did you establish mechanisms to ensure fairness in your AI system?			
ACCESSIBILITY AND UNIVERSAL DESIGN				
No.	**Question**	**YES**	**NO**	**Why?**
3	Did you ensure that Universal Design principles are taken into account during every step of the planning and development process, if applicable?			
4	Did you take the impact of the AI system on the potential end-users and/or subjects into account?			

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

4.1	Did you assess whether the team involved in building the AI system engaged with the possible target end-users and/or subjects?			
	Did you assess whether there could be groups who might be disproportionately affected by the outcomes of the AI system?			
STAKEHOLDERS PARTICIPATION				
No.	**Question**	**YES**	**NO**	**Why?**
1	Did you consider a mechanism to include the participation of the widest range of possible stakeholders in the AI system's design and development?			

Table D. 7 - Social and environmental well-being

Requirement #6 SOCIAL AND ENVIRONMENTAL WELL-BEING				
ENVIRONMENTAL WELL-BEING				
No.	**Question**	**YES**	**NO**	**Why?**
1	Are there potential negative impacts of the AI system on the environment?			
2	Where possible, did you establish mechanisms to evaluate the environmental impact of the AI system's development, deployment and/or use (for example, the amount of energy used and carbon emissions)?			
IMPACT ON WORK AND SKILLS				
No.	**Question**	**YES**	**NO**	**Why?**
1	Does the AI system impact human work and work arrangements?			
2	Did you pave the way for the introduction of the AI system in your organisation by informing and consulting with impacted workers and their representatives (trade			

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

	unions, (European) work councils) in advance?			
3	Did you adopt measures to ensure that the impacts of the AI system on human work are well understood?			
4	Could the AI system create the risk of de-skilling of the workforce?			
5	Does the system promote or require new (digital) skills?			

Table D. 8 - Accountability

Requirement #7 ACCOUNTABILITY				
AUDITABILITY				
No.	**Question**	**YES**	**NO**	**Why?**
1	Did you establish mechanisms that facilitate the AI system's auditability (e.g. traceability of the development process, the sourcing of training data and the logging of the AI system's processes, outcomes, positive and negative impact)?			
2	Did you ensure that the AI system can be audited by independent third parties?			
RISK MANAGEMENT				
No.	**Question**	**YES**	**NO**	**Why?**
1	Did you foresee any kind of external guidance or third-party auditing processes to oversee ethical concerns and accountability measures?			
1.1	Does the involvement of these third parties go beyond the development phase?			

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

Annex E - Tables on EU AI Legislative Initiative Requirements

1. AI Act Relevant Developments Requirements for the purposes of HAIKU

The following tables can be used by HAIKU partners for a preliminary self-assessment of the use cases design. The same criteria will be further used carrying on the tasks T7.2, T7.3 and T7.4.

Table E. 1 - AI Act relevant development requirements (Risk management)

RISK MANAGEMENT		
Reference	**Requirement**	**For the purposes of HAIKU**
Article 8	**Compliance** «(1) High-risk system shall comply with the requirements established […] (2) The intended purpose of the high-risk Ai system and risk management system […] shall be taken into account when ensuring compliance with those requirements»	To have a clearer idea of the specific compliance burdens on the shoulder of the actors involved in each use case, it is advisable to preventively: ● **Classify the AI system at issue according to the criteria provided by the AI Act** ● If qualified as 'high-risk', assess how this qualification may inform the specific regime (if any) prescribed by the sector-based regulation
Article 9 (1) and (2)	**Risk management system** «(1) a risk management system shall be established, implemented, documented and maintained in relator o high-risk AI systems. (2) The management system shall consist of a continuous iterative process run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic updating comprising the following steps: a. identification and analysis of the known and foreseeable risks associated with each high-risk AI system; b. estimation and evaluation of the risks that may emerge when the	If the AI system at issue is qualified as a high-risk one, it is advisable that the owner of each use case shall: ● **assess if ordinary sector-based regulation already prescribes the establishment/implementation of a risk management system** ○ if NO, establish/implement (or consider how to establish/implement) a risk management system as described by the AI Act (at least a preliminary assessment) ○ if YES, assess if the existent risk management system satisfies the requirements prescribed by the AI ACT (at

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

	high-risk AI system is used in accordance with its intended purpose and under conditions of reasonably foreseeable misuse; c. evaluation of other possibly arising risks based on the analysis of data gathered from the post-market monitoring system […]; d. adoption of suitable risk management measures »	least a preliminary assessment) ● **implement (or consider how to implement) a risk assessment strategy comprising the steps described by the AI ACT**
Article 9 (3) and (4)	**Risk management measures** «(4, II) In identifying the most appropriate risk management measures, the following shall be ensured: a. elimination or reduction of risks as far as possible through adequate design and development; b. where appropriate, implementation of adequate mitigation and control measures in relation to risks that cannot be eliminated; c. provision of adequate information [to users[7]], in particular as regards the risks referred [to the emerging from consistent usages with the intended purposes[8]], and, where appropriate, training to users. In eliminating or reducing risks related to the **use of the high-risk AI system**, due consideration shall be given to the **technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used**».	Once assess the material risks related to the use of the high-risk AI system at issue, it is advisable that the owner of each use case shall: ● **assess how the technological design and development (or its adjustment) can eliminate or reduce the risk** ● **assess how the residual risks may impact on the task-responsibility and liability risks exposure of the actors involved (acceptability)** ● assess the effectiveness of the already implemented risk-mitigation and risk-control measures and if others are needed ● assess the technical knowledge, experience, education, training to be expected by the user and the environment in which the system is intended to be used and provide more training where appropriate ● **provide to the perspective users adequate information about**

[7] AI Act [55], article 13

[8] AI Act [55], article 9(2)(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

	«(4, I) The risk management measures […[9]] shall be such that **any residual risk associated with each hazard as well as the overall residual risk of the high-risk AI systems is judged acceptable**, provided that the high-risk AI system is used **in accordance with its intended purpose or under conditions of reasonably foreseeable misuse**. Those **residual risks shall be communicated to the user**.» «(3) The risk management measures […[10]] shall give due **consideration to the effects and possible interactions resulting from the combined application of the requirements [for high-risk systems[11]].** They shall take into account the **generally acknowledged state of the art, including as reflected in relevant harmonised standards or common specifications**»	**inherent and residual risks related to the use of the systems consistent with the intended purposes and under conditions of reasonably and foreseeable misuse**
Article 9 (5),(6) and (7)	**Testing procedures** «(5) High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter. (6) Testing procedures shall be suitable to achieve the intended purpose of the	Once assess the material risks related to the use of the high-risk AI system at issue and the related mitigations, it is advisable that the owner of each use case shall: ● test if the system performs consistently for its intended purposes, and if the already implemented mitigations can be improved

[9] AI Act [55], article 9(2)(d)

[10] AI Act [55], article 9(2)(d)

[11] AI Act [55], Chapter 2.

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 system and do not need to go beyond what is necessary to achieve that purpose. (7) The testing of the high-risk AI systems shall be performed, as appropriate, at any point in time throughout the development process, and, in any event, prior to the placing on the market or the putting into service. Testing shall be made against preliminarily defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.»	

Table E. 2 - AI Act relevant development requirements (Data Governance)

DATA GOVERNANCE		
Reference	**Requirement**	**For the purposes of HAIKU**
Article 10(2)	**Data governance and management practices** «Training, validation and testing data sets shall be subject to appropriate data governance and management practices. Those practices shall concern in particular, a. the relevant design choices; b. data collection; c. relevant data preparation processing operations, such as annotation, labelling, cleaning, enrichment and aggregation; d. the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; e. a prior assessment of the availability, quantity and suitability of the data sets that are needed;	See § 5

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

	f. examination in view of possible biases; **g.** the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed»	
Article 10(3) and (4)	**Data sets** «(3) Training, validation and testing data sets shall be relevant, representative, free of errors and complete. They shall have the appropriate statistical properties, including, where applicable, as regards the persons or groups of persons on which the high-risk AI system is intended to be used. These characteristics of the data sets may be met at the level of individual data sets or a combination thereof. (4) Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used.»	See § 5

Table E. 3 -AI Act relevant development requirements (Transparency)

TRANSPARENCY DUTIES		
Reference	**Requirement**	**For the purposes of HAIKU**
Article 12	**Record-keeping and logging capabilities** «(1) High-risk AI systems **shall be designed and developed with capabilities enabling the automatic recording of events ('logs')** while the high-risk AI systems is operating. Those	Once assess the material risks related to the use of the high-risk AI system at issue and the related mitigations, it is advisable that the owner of each use case shall: ● **assess if ordinary sector-based regulation already prescribes the**

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

	logging capabilities shall conform to recognised standards or common specifications. (2) The logging capabilities shall **ensure a level of traceability of the AI system's functioning throughout its lifecycle that is appropriate to the intended purpose of the system**. (3) In particular, logging capabilities shall enable the **monitoring of the operation of the high-risk AI system with respect to the occurrence of situations that may result in the AI system presenting a risk** [at national level][12] **or lead to a substantial modification**, and facilitate the post-market monitoring [...[13]]»	**specific logging capabilities by design** ○ if NO, introduce the specific logging capabilities by design as described by the AI Act (at least an elementary version for validation purposes) ○ if YES, assess if the existent logging capabilities by design satisfies the requirements prescribed by the AI ACT (at least an elementary version for validation purposes) ● **assess if the existent/introduced logging system enables the operations monitoring requirements concerning AI system may present a risk at national level or lead to a substantial modification of the AI system at issue**
Article 13(2) and (3)	**Transparency and provision of information to users** «(2) High-risk AI systems **shall be accompanied by instructions for use** in an appropriate digital format or otherwise that include **concise, complete, correct and clear information that is relevant, accessible and comprehensible to users**.	Once assess the material risks related to the use of the high-risk AI system at issue and the related mitigations, it is advisable that the owner of each use case shall: ● **assess if ordinary sector-based regulation already prescribes the specific information duties and the specific contents of the information policy**

[12] AI Act [55], Article 65(1): «AI systems presenting a risk shall be understood as a product presenting a risk defined in Article 3, point 19 of Regulation (EU) 2019/1020 insofar as risks to the health or safety or to the protection of fundamental rights of persons are concerned». See: Reg. (EU) 2019/1020, Article 3(19): «'product presenting a risk' means a product having the potential to affect adversely health and safety of persons in general, health and safety in the workplace, protection of consumers, the environment, public security and other public interests, protected by the applicable Union harmonisation legislation, to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned, including the duration of use and, where applicable, its putting into service, installation and maintenance requirements»

[13] AI Act [55], Article 61.

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) The information referred […[14]] shall specify: (b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including: (i) its intended purpose; (ii) the level of accuracy, robustness and cybersecurity […[15]]against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity; (iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights; (iv) its performance as regards the persons or groups of persons on which the system is intended to be used; (v) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the AI system. (c) the changes to the high-risk AI system and its performance which have been pre-determined by the	○ if NO, the owner should draft an information policy containing the contents specified by the AI Act (at least an elementary version for validation purposes) ○ if YES, assess if the existent information policy satisfies the requirements prescribed by the AI ACT (at least an elementary version for validation purposes) ● **assess if the existent/introduced information policy is able to address the potential issues concerning future changes of the high-risk Ai system pre-determined by the owner/provider**, and if this information allow the users to profitably manage the connected residual risks (if any)

[14] AI Act [55], Article 13(2).

[15] AI Art [55], Article 15.

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

	provider at the moment of the initial conformity assessment, if any»	

Table E. 4 -AI Act relevant development requirements (Human oversight)

HUMAN OVERSIGHT		
Reference	**Requirements**	**For the purposes of HAIKU**
Article 14(2)	**Human oversight** «Human oversight shall aim at preventing or minimising the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular when such risks persist notwithstanding the application of other requirements set out in [the AI Act[16]] »	It is advisable that the owner of each use case shall ensure appropriate technical and organizational measures to ensure human oversight, from the early stages of the projecting process (HAIKU activities included).
Article 13(1)	**Transparency and interpretability by design** «(1) High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users **to interpret the system's output and use it appropriately**. An appropriate type and **degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider** […[17]]»	It is advisable that the owner of each use case shall: ● test how the design of the procedures and the interfaces allows an easy interpretation of the results obtained (also counterfactual verifications) ● address the potential interpretability issues from the early stages of the projecting process (HAIKU activities included).
Article 13(3)(d)	**Transparency and human oversight**	

[16] AI Act [55], Chapter 2.

[17] AI ACT [55], Chapter 3

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 information provided to the users shall specify:] «the human oversight measures [...[18]], including the technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users»	
Article 14(1) And (3)	**Interfaces and human oversight** «(1) High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use» «(3) Human oversight shall be ensured through either one or all of the following measures: (a) identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service»	It is advisable that the owner of each use case shall (see above): ● test how the design of the procedures and the interfaces allows an easy interpretation of the results obtained (also counterfactual verifications) ● address the potential interpretability issues from the early stages of the projecting process (HAIKU activities included).
Article 14(4)	**Human oversight in practice** «The measures referred to in paragraph 3 shall enable the individuals to whom human oversight is assigned to do the following, as appropriate to the circumstances: (a) fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be	It is advisable that the owner of each use case shall: ● establish assessment methodologies inspired by the principles set by the AI Act

[18] AI Act [55], Article 14

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

	detected and addressed as soon as possible; (b) remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system ('automation bias'), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons; (c) be able to correctly interpret the high-risk AI system's output, taking into account in particular the characteristics of the system and the interpretation tools and methods available; (d) be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system; (e) be able to intervene on the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure»	

Table E. 5 - AI Act relevant development requirements (Technological robustness)

TECHNOLOGICAL ROBUSTNESS		
Reference	**Requirement**	**For the purposes of HAIKU**
Article 15(1) and (2)	**Accuracy** «(1) High-risk AI systems shall be designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle. (2) **The levels of accuracy and the relevant accuracy metrics of high-risk**	Once assess the technological risks related to the use of the high-risk AI system at issue, it is advisable that the owner of each use case shall: ● **comply with the accuracy requirements for software and automated systems prescribed by ordinary sector-based regulation** ● **assess if the existent/introduced information policy is able to address the potential issues concerning intrinsic accuracy**

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 systems shall be declared in the accompanying instructions of use.»	**limitations of the technology at stake** ● **suggest to intermediate and final users the best training strategies for safely addressing the intrinsic accuracy limitations of the technology at stake over operations (**at least an elementary version for validation purposes) See: Accuracy requirements specified by aviation law and regulation.
Article 15(3)	**Robustness** «High-risk AI systems shall be resilient as regards errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems. The robustness of high-risk AI systems may be achieved through technical redundancy solutions, which may include backup or fail-safe plans. High-risk AI systems that continue to learn after being placed on the market or put into service shall be developed in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations ('feedback loops') are duly addressed with appropriate mitigation measures.»	Once assess the technological risks related to the use of the high-risk AI system at issue, it is advisable that the owner of each use case shall: ● **comply with the robustness requirements for software and automated systems prescribed by ordinary sector-based regulation** ● **assess if the existent/introduced mitigation measures are able to address the potential issues related to self-learning AI systems and the required feedback loop over time** See: Robustness requirements specified by aviation law and regulation.
Article 15(4)	**Cybersecurity** «High-risk AI systems shall be resilient as regards attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities.	Once assess the technological risks related to the use of the high-risk AI system at issue, it is advisable that the owner of each use case shall: ● **comply with the robustness requirements for software and**

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 technical solutions aimed at ensuring the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks. The technical solutions to address AI-specific vulnerabilities shall include, where appropriate, measures to prevent and control for attacks trying to manipulate the training dataset ('data poisoning'), inputs designed to cause the model to make a mistake ('adversarial examples'), or model flaws»	**automated systems prescribed by ordinary sector-based regulation** ● **assess if the existent/introduced cybersecurity measures are able to address the potential risks of data poisoning, adversarial attacks and model flaws, considering the intended purposes of the systems at stake** See: Cybersecurity requirements specified by aviation law and regulation.

Table E. 6 -AI Act relevant development requirements (Quality management and conformity)

QUALITY MANAGEMENT & CONFORMITY		
Reference	**Requirement**	**For the purposes of HAIKU**
Article 16	**Obligations of providers of high-risk AI systems** Providers of high-risk AI systems shall: (a) ensure that their high-risk AI systems are compliant with the requirements set [for these kind of technologies by the AI Act[19]]; (b) have a quality management system [...[20]]; (c) draw-up the technical documentation of the high-risk AI system; (d) when under their control, keep the logs automatically generated by their high-risk AI systems; (e) ensure that the high-risk AI system undergoes the relevant conformity assessment procedure, prior to its	Once assess the risks related to the use of the high-risk AI system at issue and the related mitigations, it is advisable that the owner of each use case shall: ● **assess and comply with the quality management requirements for software and automated systems prescribed by ordinary sector-based regulation** ● **assess if the existent satisfies the general requirements prescribed by the AI Act**

[19] AI Act [55], Chapter 2.

[20] AI Act [55], Article 17.

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

	placing on the market or putting into service; […[21]]	
Article 17 (1) and (2)	**Quality management system** «(1) Providers of high-risk AI systems shall put a quality management system in place that ensures compliance with this Regulation. That system shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions, and shall include at least the following aspects: (a) a strategy for regulatory compliance, including compliance with conformity assessment procedures and procedures for the management of modifications to the high-risk AI system; (b) techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system; (c) techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the high-risk AI system; (d) examination, test and validation procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out; (e) technical specifications, including standards, to be applied and, where the relevant harmonised standards are not applied in full, the means to be used to ensure that the high-risk	Once assess the risks related to the use of the high-risk AI system at issue and the related mitigations, it is advisable that the owner of each use case shall: ● **assess and comply with the quality management requirements for software and automated systems prescribed by ordinary sector-based regulation** ● **assess if the existent satisfies the general requirements prescribed by the AI Act** In this regard, the guidelines and take-away messages provided by this deliverable may be a helpful tool to set a preliminary version of the quality management system for validation purposes (especially for points (a), (b) and (c) if addressed in form of a checklist) However, **the efforts shall be proportional to the sizes of providers' organisations (taking into account the stage of the design/development process)**

[21] The following requirements refer to development and deployment progresses not included in the research scope of the HAIKU project.

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 system complies with the requirements set out [by the AI Act[22]]; (f) systems and procedures for data management, including data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purposes of the placing on the market or putting into service of high-risk AI systems; (g) the risk management system […[23]]; the setting-up, implementation and maintenance of a post-market monitoring system […[24]]; (h) procedures related to the reporting of serious incidents and of malfunctioning […[25]]; (i) the handling of communication with national competent authorities, competent authorities, including sectoral ones, providing or supporting the access to data, notified bodies, other operators, customers or other interested parties; (j) systems and procedures for record keeping of all relevant documentation and information; (k) resource management, including security of supply related measures; (l) an accountability framework setting out the responsibilities of the management and other staff with	

[22] AI Act [55], Chapter 2.

[23] AI Act [55], Article 9.

[24] AI Act [55], Article 61.

[25] AI Act [55], Article 62.

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

	regard to all aspects listed in this paragraph. (2) **The implementation of aspects referred to in paragraph 1 shall be proportionate to the size of the provider's organisation**.	
Article 20(1)	**Automatically generated logs** «(1) Providers of high-risk AI systems shall keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control by virtue of a contractual arrangement with the user or otherwise by law. The logs shall be kept for a period that is appropriate in the light of the intended purpose of high-risk AI system and applicable legal obligations under Union or national law.»	Once assess the risks related to the use of the high-risk AI system at issue and the related mitigations, it is advisable that the owner of each use case shall: ● **assess and comply with automatic logging capabilities required for software and automated systems prescribed by ordinary sector-based regulation** ● **assess if the existent satisfies the general requirements prescribed by the AI Act** See above: Record-keeping and logging capabilities (article 12)

2. AI Liability Dir. Relevant Compliance Requirements for the purposes of HAIKU

The following tables can be used by HAIKU partners for a preliminary self-assessment of the use cases design. The same criteria will be further used carrying on the tasks T7.2, T7.3 and T7.4.

Table E. 7 -AI Liability Dir. relevant compliance requirements

DISCLOSURE DUTIES & REBUTABLE PRESUMPTION		
Reference	**Requirement**	**For the purposes of HAIKU**
Article 3(1)	The court is empowered to order the provider or user the disclosure of relevant evidence at its disposal about a specific high-risk AI system that is suspected of having caused damages.	The provider or user should establish its compliance strategy in order to be able of providing this evidence. Technical and organizational design and implementation should be carried on consistently with AI Act and documented/recorded as required by law.

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

Article 3(3)	The court is empowered to order the provider or user specific measures to preserve the evidence mentioned [above]	The provider or user should establish its compliance strategy in order to be able of comply with this order. Technical and organizational design and implementation should be carried having in mind the possibility.
Article 3(4) first and third parts	The court shall limit the disclosure of evidence to that which is necessary and proportionate to support a potential claim for damage and is empowered to take specific measure necessary to preserve confidentiality when that evidence is used or referred to in legal proceedings	The provider or user should establish its information classification matrix. Technical and organizational design and implementation should be carried having in mind the possibility.
Article 4 (1)(a)	The claimant has to demonstrate and the court shall presume from lack of disclosure the fault of the defendant consisting in the non-compliance with a duty of care laid down in Union or national law directly intended to protect against the damages occurred	The provider or user should document technical and organizational choices and their impact on the evolution of processes and procedures. The provider or user should establish its information classification matrix consistently with the different interests related to this documental production.
Article 4(1)(c)	The claimant has to demonstrate that the output by the Ai system or the failure of the AI system t produce an output gave rise to the damage	The provider or user should document technical and organizational choices and their impact on the evolution of processes and procedures.
Article 4(2)	In the case of a claim of damages against a provider of a high-risk Ai system subject to the requirements laid down in chapter 2 and 3 of the AI Act or a person subject to the provider's obligation as provided by the AI Act, presumption of non-compliance are rated according to the requirements laid down by those norms	The provider or user should document technical and organizational choices and their impact on the evolution of processes and procedures.

3. PLD.R. Relevant Provisions for the purposes of HAIKU

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 following tables can be used by HAIKU partners for a preliminary self-assessment of the use cases design. The same criteria will be further used carrying on the tasks T7.2, T7.3 and T7.4.

Table E. 8 - PLD.R. relevant provisions

Reference	Requirement	For the purposes of HAIKU
Article 3 (1 and 6) Article 6 Article 9	AI systems and AI-enabled goods are “products” and therefore an eventual damage compensation may be available without the injured person having to prove the manufacturer’s fault, just like for any other product	If not differently regulated by other specific regimes, damages related to use of AI systems and AI-enabled goods may be compensated with an easier burden of proof for the victims (defectiveness, damage and causal link)
Article 3(5) Article 3(2-4)	not only hardware manufacturers but also software providers and providers of digital services that affect how the product can be held liable	All the actors involved in the development and deployment value chain can be liable for the damages related to the use of the products or the functioning of its components.
Article 3 (5) Article 7 (1 and 4) Article 6 (1) (c)	manufacturers can be held liable for changes they make to products they have already placed on the market, including when these changes are triggered by software updates or machine learning and factors such as the interconnectedness or self-learning functions of products have been added to the non- exhaustive list of factors to be taken into account by courts when assessing defectiveness	Intrinsic dynamic features of an AI systems or an AI-enabled good can be included to factors list to assess defectiveness. The different actors involved in design, development and deployment process should document technical and organizational choices and their impact on the evolution of processes and procedures.

The table below lists the most relevant and long-term consolidated criteria and highlights the consequences for the stakeholders involved in the HAIKU project. In addition, the table also takes into consideration the possible exceptions from liability considering the conditions actually enforced by the PDL and new ones suggested by the proposal for revision.

Table E. 9 - PLD.R, Defectiveness indexes and exceptions

Reference	Defectiveness index	Exemption
PLD.R [61], article 6 (1)(g)	Level of compliance with regulatory established safety requirements	The defectiveness is due to compliance of the product with mandatory regulations issued by public authorities

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

PLD [33] + law cases	Design reasonable safety	The product was designed according to the available state of the art
PLD [33] + law cases	Design/product correspondence	
PLD [33] + law cases	Quality materials used to manufacture the product	
PLD [33] + law cases PLD.R [61], article 6 (1)(a)	Presentation of the product	The product was not officially placed on the market or put in into service The defectiveness did not exist when the product was placed on the market or put in into service
PLD.R [61], article 6 (1)(c)	Presentation (and control) of any ability of the product to continue to lean after the development	The objective state of scientific and technical knowledge at the time when the product was placed on the market, put into service The product still was under the control of the manufacturer (not applicable to software updates or upgrades, and the following lack of software updates or upgrades necessary to maintain safety)
PLD.R [61], article 6 (1)(a)	Instructions for installation, use and maintenance	The product was autonomously modified by the owner after the purchase
PLD.R [61], article 6 (1)(f)	Information about product safety requirements, including safety-relevant cybersecurity requirements	
PLD [33] + law cases	Instructions on the safe use of the product	
PLD [33] + law cases	Information on the proper use of the product	
PLD [33] + law cases PLD.R [61], article 6 (1)(b)	Information about the foreseeable risks of not following instructions	

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

PLD [33] + law cases	Warnings about the dangers inherent in a product	
PLD.R [61], article 6 (1)(d)	Effect on the product of other products that can reasonably be expected to be used together with the product	The defectiveness of the product is attributable to the design of a component or of functional corollary product/service

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

Annex F - Detailed analysis of EU Aviation Law Requirements for AI and operative tables

1. Insights about the evolution of safety in aviation and its contribution for the use of AI

When the Convention on International Civil Aviation was signed in Chicago on 7 December 1944 [94], the community believed that only the aircraft and the pilot were relevant for safety. In fact, among several possible topics, the Convention only covers certificate of airworthiness (Art. 31 therein) and pilot licences (Art. 32).

Consequently, during the first decades of existence of ICAO attention was devoted to aircraft design, production and maintenance and to human errors, considering each human in isolation and only interfaced with the aircraft and with the environment.

The turning point was on 27 March 1977 when two ‘jumbo jets’ B-747 collided on the runway of Los Rodeos aerodrome in Tenerife Island. The official investigation concluded that it was not sufficient to consider the human in isolation, but interfaced with other humans (e.g. in the cockpit), interfaced with other teams (e.g. pilots and ATCOs) and also interfaced with the organisation to which the human belonged.

This, in 1989, became the official ICAO philosophy through the so-called SHELL model, introduced by Circular 216 [96]. Since then ICAO has put growing attention on ‘organisations’ starting with the Aircraft Operator Certificate (AOC) introduced in Annex 6 to the Chicago Convention in 1990 [98].

This is even more true in the EU, where Basic Regulation 2018/1139 [46] and related Commission Regulations require certification, or at least declaration, for several organisations involved in aviation operations.

All the items listed above compose what ICAO calls the ‘total system’ in the following graph, extracted from the ICAO Safety Management Manual [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

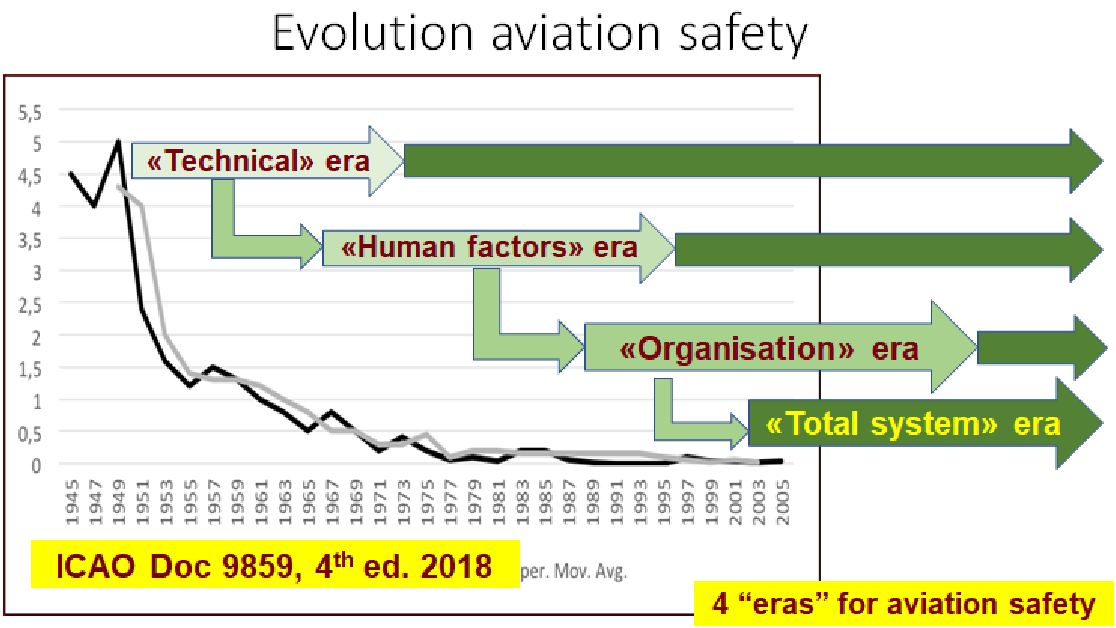

Figure F. 1 - Evolution of aviation safety

2. Hard and soft rules in aviation law

In the jargon of experts on European civil aviation safety rules, there is a distinction between so-called 'hard rules' and 'soft rules'. The former are legally-binding for someone. The latter do not have force of law, although their application may de-facto be required by someone.

This regulatory structure can be depicted in the form of a pyramid:

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

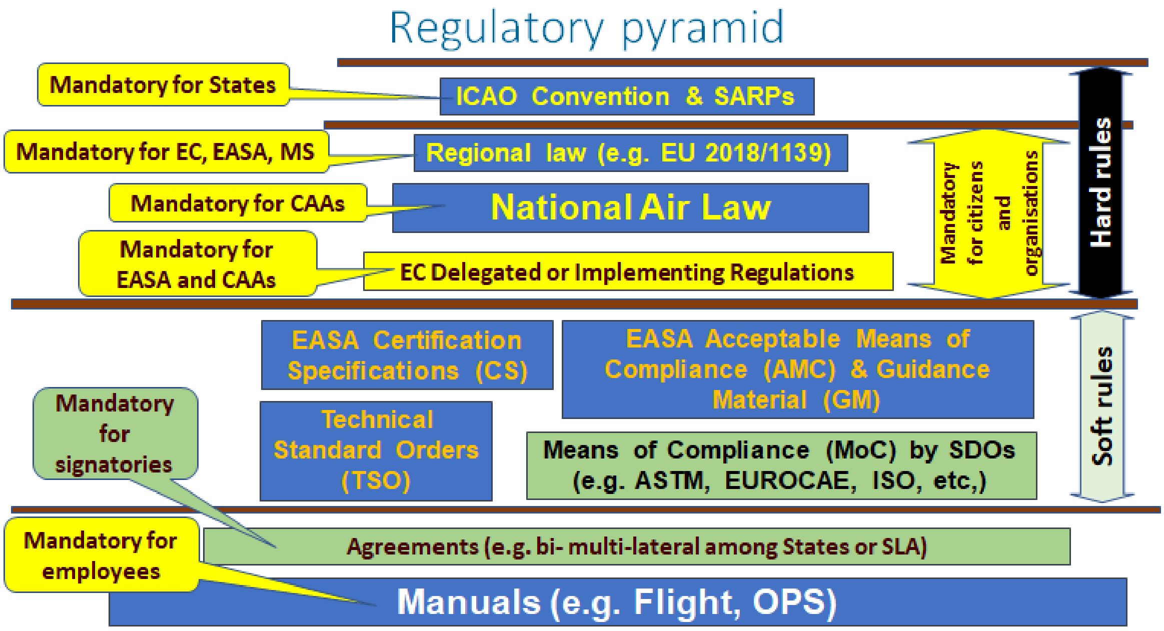
Regulatory pyramid
Mandatory for States
ICAO Convention & SARPs
Mandatory for EC, EASA, MS
Regional law (e.g. EU 2018/1139)
Mandatory for CAAs
National Air Law
Mandatory for EASA and CAAs
EC Delegated or Implementing Regulations
Mandatory for citizens and organisations
Hard rules
EASA Certification Specifications (CS)
EASA Acceptable Means of Compliance (AMC) & Guidance Material (GM)
Mandatory for signatories
Technical Standard Orders (TSO)
Means of Compliance (MoC) by SDOs (e.g. ASTM, EUROCAE, ISO, etc,)
Soft rules
Mandatory for employees
Agreements (e.g. bi- multi-lateral among States or SLA)
Manuals (e.g. Flight, OPS)

Figure F. 2 - Aviation Law Regulatory Pyramid

At the top we have the Chicago Convention and the related standards in its Annexes, which however, based on Articles 1 and 2 of the Convention are mandatory for ICAO Contracting States, but neither for organisations nor for citizens if not transposed.

Below we have the rules with force of law in EU, which comprise:

a) basic EU acts adopted by EP and Council which are legally-binding for anyone, including the EC;
b) National Aviation Law which is binding for the competent authority, for organisations and for citizens; and
c) EC Delegated or Implementing Regulations, at the bottom of the hard rules.

The latter are usually technology-agnostic and performance-based. In other words they establish ‘who’ (the legal entity or natural person) shall do ‘what’, but the level of detail is not sufficient for concrete application.

Hence they need to be complemented by so-called soft rules, which are not legally-binding, but their application constitutes presumption of compliance with the hard rules.

The soft rules comprise AMC/GM published by EASA, or equivalent Advisory Circulars (AC) published by the FAA or other aviation authorities around the world. Soft rules also include Certification Specifications (CS) or European Technical Standard Orders (ETSO), still published by 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

An applicant may elect to use AMC, CS or GM published by EASA, but it may also propose to its competent authority an Alternative Means of Compliance (AltMOC). Convincing the authority and EASA would of course be costly and difficult, but from time to time this happens, driven by the evolution of the State-of-the-Art. And it is likely that this will happen when the aviation industry will introduce AI.

In any case, also AMC and CS tend nowadays to be more and more performance-based. So the community needs more detailed guidance (e.g. for minimum functionality, Minimum Operational Performance Standards (MOPS), test methods, calibration of measuring equipment, standard parts, validation of automated testing tools and so on).

Therefore, soft rules also include consensus-based voluntary standards published by SDOs. These standards have the same legal status (i.e. non legally-binding) of soft rules published by EASA. However, they are often referred to as 'Means of Compliance' (MOCs) if listed by EASA in AMC or other soft rules. Otherwise, they may be proposed as AltMOC.

The EASA soft rules most relevant for AI are summarised in the following paragraphs, while some industry standards are discussed in § 7.

EUROCONTROL is neither a regulatory authority nor an SDO. However, that intergovernmental organisation has developed several guidance documents or technical specifications. Its role to contribute to development of rules for the single European sky (SES) is recognised by Art. 8 of Regulation 2004/549 [71]. Therefore, guidance issued by EUROCONTROL will also be considered in this document.

This Annex aims to shed light on the hard and soft rules applicable to AI applications in aviation. The following paragraphs will present in the detail the requirements applicable to AI in the areas covered by the SOAR. Moreover,

3. AI in Articles of EASA Basic Regulation on aviation safety

The tables below reports in the detail the principles and requirements of aviation safe legislation that may be relevant for the purposes of HAIKU. These can be used by HAIKU partners for a preliminary self-assessment of the use cases design. The same criteria will be further used carrying on the tasks T7.2, T7.3 and T7.4.

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 F. 1- AI in Articles of EASA Basic Regulation on aviation safety

Article	Title	Content	Applicability to AI
4(1)(e)	Principles for measures under this Regulation	lay down, where possible, requirements and procedures in a manner which is performance-based and focuses on objectives to be achieved, while allowing different means of achieving compliance with those performance-based objectives	The EU Legislator strongly recommends EC and EASA PBR, even in the case of electrical or mechanical parts or of deterministic software. This would be even more true with AI, for which prescriptive technical rules are most difficult to be developed
6(2)	European Plan for Aviation Safety (EPAS)	EASA, in close collaboration with Member States (MS) and relevant stakeholders, shall document in a dedicated safety risk portfolio the safety risks and monitor the implementation of related mitigation actions by the parties concerned, including, where appropriate, by setting safety performance indicators.	This means that even today, since implementation of AI is already allowed by the EU/EASA performance-based rules, EASA shall monitor emerging risks and, where necessary, propose appropriate mitigations.

4. Essential Requirements on aviation safety applicable to AI

Table F. 2 -Essential Requirements on aviation safety applicable to AI

ER	Subject	Content	Applicability to AI
Annex II 1.3.4	Explainability	Information needed for the safe conduct of the flight and information concerning unsafe conditions must be provided to the crew or maintenance personnel, as appropriate, in a clear, consistent and unambiguous manner. Systems, equipment and controls, including signs and announcements must be designed and located to minimise	This applies also to presentation of outcomes of AI processes to flight crew. Similar ERs exist for aerodromes, ATM/ANS systems and UAS

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

		errors which could contribute to the creation of hazards.	
Annex II 1.3.5	Information security	Design precautions must be taken to minimise the hazards to the aircraft and occupants from reasonably probable threats, including information security threats, both inside and external to the aircraft, including protecting against the possibility of a significant failure in, or disruption of, any non-installed equipment.	AI safety assessment should consider also information security threats, including for exchanges of information with systems external to aircraft. Similar ERs exist for aerodromes, ATM/ANS systems and UAS
Annex II 1.4.1	Non-installed equipment	Non-installed equipment must perform its safety function or function relevant for safety as intended under any foreseeable operating conditions unless that function can also be performed by other means.	Typical non-installed equipment with ICT components include portable Electronic Flight Bag (EFB) used by crews and Command Unit (CU) to govern the flight of a UAS. Safety, HF and security ERs apply also to these equipment
Annex II 1.5.2	Instructions for Continuing Airworthiness (ICA)	Means must be provided to allow inspection, adjustment, lubrication, removal or replacement of parts and non- installed equipment as necessary for continuing airworthiness.	'Adjustment' may include instructions to train AI embedded into aircraft systems.
Annex V 8.2	Instructions in operation manual	The operation must only be undertaken in accordance with an aircraft operator's operations manual. Such manual must contain all necessary instructions, information and procedures for all aircraft operated and for operations personnel to perform their duties	The aircraft operator shall provide in the OPS Manual also instructions for the use of AI. Similar ERs exist for aerodromes, ATM/ANS systems and UAS

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

Annex V 8.4	Security	The aircraft operator must develop and maintain security programmes adapted to the aircraft and the type of operation including particularly: ... (c) training programmes; and (d) protection of electronic and computer systems to prevent intentional and unintentional system interference and corruption.	This ER applies to aircraft operations even when based on AI applications Similar ERs exist for aerodromes, ATM/ANS systems and UAS
Annex VIII 2.3.3	Automation	Automated tools providing information or advice to ATS personnel shall be properly designed, produced and maintained to ensure that they are fit for their intended purpose.	

5. EC Regulations on design and production. AMC/GM applicable to AI

In the EU/EASA regulatory framework, design and production of aircraft, engines, propellers, parts, systems, aerodromes is subject to three different sets of provisions:

1. legally-binding rules on the administrative procedures, adopted as Commission Regulations;
2. legally-binding rules on involved authorities and involved organisations, equally promulgated by the EC; and
3. Certification Specifications (CS), published by EASA, but non legally-binding.

Normally rules in 1) and 2) are ‘technology agnostic’, alias ‘performance-based’, specifying ‘what’ shall be achieved and demonstrated, leaving technical details to the level of non-binding rules published by EASA or to consensus-based standards published by SDOs.

The legally-binding rules in 1) and 2) are often complemented by non-binding Acceptable Means of Compliance (AMC) and Guidance Material (GM) published by EASA.

One of the consequences of this approach is that, while in ICAO technical details for design of aerodromes are published as mandatory standards in Annex 14 of the Chicago Convention[101] , in the EU these details are not legally-binding and hence published in EASA CS for Aerodrome Design [17].

In the domain of initial airworthiness of aviation products, the most relevant legally-binding rules are contained in Commission Regulation 748/2012 which is complemented by several AMC and GM related to the airworthiness certification processes and related organisations [40].

AI is neither mentioned in the rules nor in the AMC/GM. However, software and cyber-security are mentioned in few AMC or GM as extracted in Table F. 3.

Table F. 3 - EC Regulations on design and production . AMC/GM applicable to AI

AMC or GM	Subject	Content	Applicability to AI
AMC 21.A.15(b)(5)	Certification programme	The applicant should propose a breakdown of the certification programme into meaningful groups of compliance demonstration activities and data, referred as “Compliance Demonstration Items” (CDIs), including references to their proposed Means of Compliance (MoC) and related compliance documents.	Most probably functions based on AI would constitute CDI, for which the applicant shall provide demonstration.
AMC 21.A.15(b)(5)	Certification programme	The applicant should provide sufficient detailed information about the novelty, complexity, and criticality aspects of each proposed CDI	Almost surely, AI functions would be novel, complex and possibly critical
AMC 21.A.15(b)(5)	Certification programme	When the compliance demonstration involves analyses or calculations, a description/identification of the tools (e.g. name and version/release of the software programs) and methods used, the associated assumptions, limitations and/or conditions, as well as of the intended use and purpose …	Automated tools might be used for demonstration of safety of AI airborne applications. In this case even the tools must be validated and verified

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

		furthermore, the validation and verification of such tools and methods should be addressed.	
Appendix A to GM 21.A.91	Examples of Major Changes	When software is involved, account should be taken also of the following guidelines: Where a change is made to software produced in accordance with the guidelines of the latest edition of AMC 20-115 the change should be classified as major if either of the following apply, and the failure effect is Catastrophic, Hazardous or Major:	See paragraph below on 'soft rules' for AMC 20-115
Appendix A to GM 21.A.91	Examples of Major Changes	In the context of a product information security risk assessment (PISRA), a change that may introduce the potential for unauthorised electronic access to product systems should be considered to be 'major' if there is a need to mitigate the risks for an identified unsafe condition.	Also security risks stemming from functions based on AI, should be considered in the PISRA
GM1 21.A.130, 21.A.163 and 21.A.165	Cyber-security	Performance of tasks in real time for the issuance of an 'EASA Form 1 …	Security procedures should not only cover the airborne functions, but any ICT device, internal or external to the organisation, used to collect the evidence for the MoCs and to lead to the attestation of conformity (i.e. Form 1).

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. EC Regulations on operations and service provision. Rules applicable to AI

Several EC Regulations apply to aviation operations and related service provision, among which 2012/965 [41] on operations of aircraft (manned and unmanned in the certified category), 2019/947 [49] on UAS operations in the open and specific categories, 2014/139 [43] on aerodrome operations, 2017/373 [45] on provision of Air Navigation Services (ANS) and 2021/664 [57] on the U-space framework.

Neither AI nor ML are mentioned in any of such regulations or associated AMC/GM.

However, in general all of them allocate responsibilities to the operator or service providers for the management of software, related applications and administration including changes, as well as control of the sources of data.

In this document, only requirements from Regulation 2012/965 [41] on aircraft operations are detailed in this paragraph, since its principles are at least partially contained in the other regulations mentioned herein and because:

a) systems used by an aircraft operator may be airborne (e.g. navigation computer) or ground-based (e.g. used by the flight dispatchers for flight planning or Flight Data Monitoring - FDM);
b) flight crew may use in the cockpit so-called portable Electronic Flight Bags (EFB) which are not a piece of certified avionics, but which nevertheless may host several applications, including those which exchange data with ground systems.

An extract of the provisions in 2012/965, most relevant for AI, is presented in Table F. 4.

Table F. 4 - EC Regulations on operations and service provision. Rules applicable to AI

Rule, AMC or GM	Subject	Content	Applicability to AI
ORO.FC.230 (a)	Recurrent training and checking	Each flight crew member shall complete recurrent training and checking relevant to the type or variant, and associated equipment of aircraft on which they operate.	Recurrent training and checking applies also to AI systems used in Commercial Air Transport (CAT). Same applies to all other operator and Service Providers (SP)
ORO.FC.231 (a)(1)	Evidence-Based Training (EBT)	The operator may substitute the requirements of ORO.FC.230 by establishing,	EBT is fed by actual difficulties encountered by the staff during operations, which for innovative

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

		implementing and maintaining a suitable EBT programme approved by the competent authority.	systems like AI, during initial years may be paramount
ORO.FC.232 (b()1)	EBT programme assessment and training topics	The assessment and training topics shall be: (1) derived from safety and operational data that are used to identify the areas for improvement and prioritisation of pilot training to guide in the construction of suitable EBT programmes;	as above
AMC1 ORO.FC.231 (h)(3) - point (b)(5)	EBT	To extend the validity of the line evaluation of competence to 3 years, the CAT operator should have a feedback process for monitoring line operations which: […] (5) identifies design problems in the Human-Machine Interface (HMI)	Feedback from personnel using AI applications is important to improve the HMI and related training
SPA.EFB.100 (a)	Use of Electronic Flight Bags (EFBs)	A CAT operator shall only use a type B EFB application if the operator has been granted an approval by the competent authority for such use.	Type B EFB applications, inter alia include some functions which could be supported by AI: a) aeronautical chart applications and airport surface maps; b) Airport Moving Map Display (AMMD); c) Applications that make use of the aeronautical operational

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

			control (AOC) communications to collect, process and then disseminate operational data; d) Aircraft performance calculation In principle AI applications shall be approved also for other operators of SPs. The Level of Involvement (LoI) of the competent authority would depend on the related safety and security risk.
SPA.EFB.100 (b) (1)	Use of EFB	Operator shall provide evidence that a risk assessment related to the use of the EFB device that hosts the application and to the EFB application and its associated function(s) has been conducted, identifying the associated risks and ensuring that they are appropriately managed and mitigated	Risk assessment is assumed to be required by any operator or SPs introducing AI applications
SPA.EFB.100 (b) (2)	Use of EFB	Operator shall provide evidence that the HMI of the EFB application have been assessed against human factors principles	HMI for any AI application shall be validated
SPA.EFB.100 (b) (3)	Use of EFB	Operator shall provide evidence of establishment of EFB administration system, procedures and training requirements for the	Administration of AI applications is also required, including changes, instructions from manufacturer and control of the data sources.

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

		administration and use of the EFB applications	

7. EU Regulations on aviation security. Paragraphs applicable to AI

After criminal acts committed by terrorists in New York and Washington on 11 September 2001, the EU Institutions took action for a harmonised response by MS to aviation security threats.

Therefore, the Legislator adopted the first Regulation 2320 [70] on the matter in 2002.

This Regulation was subsequently repealed by Regulation 300/2008 [74] laying down common rules and basic standards on aviation security and procedures to monitor the implementation of the common rules and standards. It also facilitated introduction of new technologies, through adoption of specifications for them.

Common basic standards on aviation security in EU comprise:

a) screening of passengers, cabin baggage and hold baggage;
b) airport security (access control, surveillance);
c) aircraft security checks and searches;
d) screening of cargo and mail;
e) screening of airport supplies;
f) staff recruitment and training.

Since 2009 several EC Regulations have supplemented Regulation (E) N° 300/2008 [74] as regards liquids, aerosols and gels, the use of security scanners, the adoption of alternative security measures, controls of air cargo internally as well as internationally and the specifications of national quality control programmes.

Neither in 300/2008 [74] nor in the EC Regulations supplementing it, software, AI or cyber-security were initially mentioned.

The whole set of previous implementing EC regulations was updated and consolidated by Commission implementing Regulation (EC) 2015/1998 [44], still initially without any mention of AI or cyber-security, although use of AI for airport security was not prohibited.

Outside the field of civil aviation, the EU Legislator adopted so-called NIS Directive (EU) 2016/1148 [81] concerning measures for a high common level of security of Network and Information Systems across the Union (NIS Directive) with a view to achieving a high common level of security of NIS within the Union. The NIS Directive was however not addressing specifically aviation.

The situation changed in 2018, when ICAO adopted amendment 16 to Annex 17 [98] of the Convention on International Civil Aviation, which introduced new standards related to preventive cyber-security measures 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

The EC therefore amended Regulation 2015/1998 [44] accordingly to make the new ICAO standards applicable throughout the EU. Amending Regulation 2019/1583 [50] in fact, introduced a new paragraph 1.7 in the Annex to 2015/1998 [44], containing measures for identification and protection of civil aviation critical ICT systems and data from cyber threats. These measures are summarised in Table F. 5.

In addition, a new Directive (NIS2) was published in the Official Journal of the EU on 27 December 2022 [84]. It will become applicable on 18 October 2024 and at that moment the first NIS Directive of 2016 will be repealed.

The new NIS2 Directive of 2022 strengthens the security requirements, mainly for “essential entities” providing ICT services (e.g., telecommunication operators). While, aviation organizations (e.g., air carriers, aerodrome operators and ATC SPs) are considered essential entities, however their prime aim is not to provide ICT services [84].

The NIS2 Directive addresses also the security of supply chains (e.g. providers of network or components of 5G mobile telephony), throughout the life-cycle of a project.

Furthermore, the NIS2 Directive streamlines reporting obligations and introduces more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. However, since better coordination is established between authorities competent for NIS and competent aviation authorities, no duplicated tasks would emerge for aviation stakeholders.

In addition, through Opinion 03/2021 [13], EASA proposed a new EC Regulation for management of information security risks potentially affecting aviation safety. Therein, ‘information security risk’ means the risk to organisational civil aviation operations, assets, individuals, and other organisations due to the potential of an information security event. Information security risks are associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets.

The purpose of this Opinion was to protect aviation from information security risks, and to make it more resilient to information security events and incidents, through provisions for the identification and management of information security risks which could affect ICT systems and data used for civil aviation purposes, detecting information security events, identifying those which are considered information security incidents, and responding to, and recovering from, those information security incidents to a level commensurate with their impact on aviation safety.

It should be noticed that the proposed provisions are ‘horizontal’, i.e. they apply to competent authorities and organisations across all aviation domains: design (DOA) and production (POA) organisations, air operators, maintenance organisations (MOA), continuing airworthiness management organisations (CAMOs), training organisations (ATO), aero-medical centres (AeMC), operators of flight simulation training devices (FSTDs), air traffic management/air navigation 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

(ATM/ANS) providers, U-space service providers and single common information service (CIS) providers, aerodrome operators and apron management service providers.

Of course, in line with the contemporary approach to regulation, the proposed provisions comprised high-level, performance-based requirements, to be supported by AMC, GM and industry standards.

Both the Implementing Regulation and the Delegated Regulation proposed to establish an Information Security Management Systems (ISMS) for organisations and competent authorities.

Once adopted by EC, the Implementing Regulation would apply to MOAs, CAMOs, air operators, ATOs for aircrew and ATCOs, AeMCs, ATM/ANS providers, FIS and U-space SPs.

At the beginning of 2023, the adoption by the EC of the Implementing Regulation establishing ISMS was still pending.

Conversely, the Delegated Act applicable to aerodrome operators, apron management SPs, DOAs and POAs was adopted on 14 July 2022 as EC Regulation 1645 [60].

Regulation 1645 [60] will apply from 16 October 2025 and it is expected that also the Implementing Regulation would apply at the same date. Both Regulations are harmonised with the NIS2 Directive and would apply even when AI applications are implemented by aviation organisations.

Table F. 5 - EU Regulations on aviation security. Paragraphs applicable to AI

Paragraph	Subject	Content	Applicability to AI
1.7.1	Affected stakeholders	Authority shall ensure that airport operators, air carriers and entities as defined in the national civil aviation security programme identify and protect their critical ICT systems and data from cyber-attacks which could affect the security of civil aviation	In the majority of EU MS the national civil aviation security programme also includes ICT systems used by ANSPs, whether or not based on AI.
1.7.2	Security programme	Operators, and SPs in 1.7.1 shall identify in their security programme the critical ICT systems and data to be	The security programme is required also for AI applications and shall include protection from, detection of, response 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

		protected against cyber threats. The security programme shall detail the measures to ensure the protection from, detection of, response to and recovery from cyber-attacks.	and recovery from cyber-attacks.
1.7.3	Risk assessment	The detailed measures to protect such systems and data from unlawful interference shall be identified, developed and implemented in accordance with a risk assessment carried out by the airport operator, air carrier or entity as appropriate.	Risk assessment is required also for cyber threats affecting AI applications
1.7.4	State oversight	Where a specific authority or agency is competent for measures related to cyber threats within a single Member State, this authority or agency may be designated as competent for the coordination and/or monitoring of the cyber-related provisions in this Regulation.	Responsibility of State not immediately of operators or SPs
1.7.5	Verification of compliance	Where operators or SPs are subjected to separate cybersecurity requirements arising from other EU or national legislation, the	States may establish a different regulatory base to verify compliance with cyber security requirements.

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

		appropriate authority may replace compliance with the requirements of this regulation by compliance with the elements contained in the other EU or national legislation. The appropriate authority shall coordinate with any other relevant competent authorities to ensure coordinated or compatible oversight regimes.	

8. EASA soft rules on system safety assessment

Several EASA soft rules provide guidance for safety assessment of products, systems or infrastructures. The most comprehensive is CS 25.1309 [17] applicable to design of turbine powered large fixed-wing aeroplanes (i.e. MTOM higher than 5700 kg), in the context of type certification (i.e. initial airworthiness).

This rule requires that:

a) The aeroplane equipment and systems must be designed and installed so that:
   - i) Those required for type certification or by operating rules, or whose improper functioning would reduce safety, perform as intended under all the aeroplane intended operating and environmental conditions.
   - ii) Other equipment and systems are not a source of danger in themselves and do not adversely affect the proper functioning of those covered by sub-paragraph (a)(i).

b) The aeroplane systems and associated components, considered separately and in relation to other systems, must be designed so that:
   - i) Any catastrophic failure condition is extremely improbable and does not result from a single failure; and
   - ii) Any hazardous failure condition is extremely remote; and
   - iii) Any major failure condition is remote; and
   - iv) Any significant latent failure is eliminated as far as practical, or, if not practical to eliminate, the latency of the significant latent failure is minimised; and
   - v) For each catastrophic failure condition that results from two failures, either one of which is latent for more than one flight, it must be shown that:
     1) it is impractical to provide additional redundancy; and
     2) given that a single latent failure has occurred on a given flight, the failure condition is remote; and

3) the sum of the probabilities of the latent failures which are combined with each evident failure does not exceed 1/1 000.

c) Information concerning unsafe system operating conditions must be provided to the flight crew to enable them to take appropriate corrective action in a timely manner. Installed systems and equipment for use by the flight crew, including flight deck controls and information, must be designed to minimise flight crew errors which could create additional hazards.

Probabilistic tolerable quantitative values are provided in the associated AMC. Similar, but using less stringent quantitative levels, are applicable to other aircraft categories (e.g., normal category fixed-wing small aircraft or helicopters). The principle of inverse relationship between probability of occurrence and severity of the outcomes is however a constant across all EASA soft rules, including for systems (e.g. ATM/ANS) or infrastructures (e.g. aerodromes) for which no EASA certification specifications as detailed as CS 25 exist.

What is very important to note is that the AMC CS 25-1309 defines [17]:

> **Failure**: An occurrence, which affects the operation of a component, part, or element such that it can no longer function as intended, (this includes both loss of function and malfunction). Errors may cause Failures, but are not considered to be Failures. In other words a failure normally affects electric, electronic or mechanical hardware, but not software.

> **Failure Condition**: A condition having an effect on the aeroplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events. So a failure condition includes not only failures, but also any potential error or malfunction caused by software.

The definition of failure condition equally applies to software based on AI. Therefore aircraft designers should consider possible errors introduced by AI applications during respective system safety assessment, even if the software is not deterministic. The same principle applies to ATM/ANS systems.

9. EASA soft rules on software

AMC 20-115D [8] describes an acceptable means, but not the only means, for showing compliance with the applicable airworthiness regulations with regard to the software aspects of airborne systems and equipment in the domain of product certification or European Technical Standard Orders (ETSOs) authorisation.

AMC 20-115D [8] applies to applicants for and to Holders of Design Approvals (DAHs), as well as to developers of airborne systems and equipment containing software to be installed on type-certified aircraft, engines, and propellers, or to be used in ETSO articles.

AMC 20-115D [8] provides guidance for establishing software life cycle planning, development, verification, configuration management, quality assurance and certification liaison processes to be

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

used in the development of software for airborne systems. The guidance provided in referred industry standards is in the form of:

a) objectives for software life cycle processes;
b) activities that provide a means for satisfying the objectives; and
c) descriptions of the evidence indicating that the objectives have been satisfied.

The cornerstones of AMC 20-115D are [8]:

a) the software Design Assurance Level (DAL) of a software component should be based on the contribution of software to potential failure conditions as determined by the system safety assessment (see previous paragraph);
b) the DAL establishes the rigour necessary to demonstrate compliance of the software with the applicable requirements;
c) In any case the DAL shall not be confused with a reliability parameter (e.g. Mean Time Between Failures - MTBF), since software is not subject to wear and it does not require periodic maintenance.

However, AMC 20-115D [8]and associated industry standards are applicable to deterministic software and their details may not be exhaustive, or applicable to AI.

And in fact, the EASA first usable guidance [12]for Level 1 ML applications clarifies that, for software aspects of AI/ML, the provisions of AMC 20-115D for product certification projects would provide confirmation that the software life cycle is properly managed. But, nevertheless, the guidance in AMC 20-115D [8] would most probably need to be complemented to address specific issues linked to the implementation of an AI/ML model into software, such as memory management issues.

Since system safety assessment is covered in the previous paragraph and since EASA believes that current AMC 20-115D would need to be complemented, it is recommended to apply it during the HAIKU Project, to determine the DAL, but not beyond.

10.EASA soft rules on cyber-security

In addition to the ISMS, based on technology-agnostic legally-binding rules adopted by the EC, EASA is working on implementation of the rules and on several initiatives to better address cybersecurity risks in aviation and so improving resilience and fostering built-in security.

In fact, besides its institutional rulemaking activity, EASA is working at improving international collaboration on the subject as well as at promoting the sharing of information amongst aviation stakeholders mainly through the European Centre for Cybersecurity in Aviation (ECCSA[26]), in collaboration with CERT-EU and ENISA.

[26] https://www.easa.europa.eu/en/eccsa

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

More in detail, EASA has published AMC 20-42 [12] which describes an acceptable means, but not the only means, to show compliance with the applicable rules for the certification of aviation products (i.e. aircraft, engines and propellers) and respective parts and equipment. Of course compliance with this AMC is not mandatory and, therefore, an applicant may elect to use an alternative means of compliance. However, any alternative means of compliance must meet the relevant requirements and be accepted by EASA.

This AMC applies to manufacturers of products and parts, and to DAHs and it is based on the following general principles:

a) the information systems of the products, parts or equipment identified should be assessed against any potential Intentional Unauthorised Electronic Interaction (IUEI) security threat and vulnerability that could result in an unsafe condition. This risk assessment is referred to as a 'Product Information Security Risk Assessment' (PISRA) and is described in this AMC;
b) The result of the PISRA, after any necessary means of mitigation have been identified, should be that either the systems of the product or part have no identifiable vulnerabilities, or those vulnerabilities cannot be exploited to create a hazard or generate a failure condition that would have an effect that is deemed to be unacceptable against the certification specification and the AMC including industry standards for the product or part considered;
c) When a risk needs to be mitigated, the applicant should demonstrate that the means of mitigation provide sufficient grounds for evaluating that the residual risk is acceptable. The means of mitigation should be provided to the operators in a timely manner;
d) Once the overall risk has been deemed to be acceptable, the applicant should, if necessary, develop ICA to maintain the information security risk of the systems of the product or part at an acceptable level, after the entry into service of the product or part.

It is recommended that aircraft operators wishing to integrate airborne applications based on AI, verify that the manufacturer of the aircraft or system complies with AMC 20-42 [11].

11.EASA soft rules on aerodromes

Following the performance-based approach, EC Regulation 139/2014 [43] does not contain any technical details on aerodrome physical characteristics or equipment used at aerodromes. Therefore, in the regulation there are no provisions on software. However, its Annex I includes software among aerodrome equipment:

> '**aerodrome equipment'** means any equipment, apparatus, appurtenance, software or accessory, that is used or intended to be used to contribute to the operation of aircraft at an aerodrome;

This regulation is complemented by soft rules published by EASA, namely AMC/GM for aerodrome operations and management and certification specifications for aerodrome design (CS-ADR-DSN) [14]. AI is neither mentioned in the AMC/GM to Regulation 139/2014 [43], nor in CS-ADR-DSN.

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

However, while software is mentioned only once in CS-ADR-DSN with reference to a specific system, three general GM apply to software, including if based on AI, as presented in Table F. 6.

Table F. 6 - Reg. EU 139/2014, Annex I, Relevant provisions about aerodrome equipment

Paragraph	Subject	Content	Applicability to AI
GM1 ADR.OR.D.005(b)(5) Management system of aerodrome operator (b)(4)	Safety performance monitoring and measurement	The following generic aspects/areas could be considered: (1) … (4) controls, including hardware, software, special procedures or procedural steps, and supervisory practices designed to keep operational activities on track	Any failure condition caused by software should be reported, recorded and analysed, including applications based on AI
GM1 ADR.OR.F.045(b)(5) Management system of Apron Management Service (AMS) provider	as above	as above	as above
GM1 ADR.OPS.A.055 Tools and software	software verification	(a) A means by which requirement can be met, is through verification of software applied to a known executable version of the software in its target operating environment. (b) Verification of software is a process of ensuring that the software meets the requirements for the specified application or intended use of the	software verification applies in principle also to AI, even if techniques may be different from those applied to deterministic software

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

		aeronautical data and aeronautical information. (c) The verification of software is an evaluation of the output of an aeronautical data and/or aeronautical information software development process to ensure correctness and consistency with respect to the inputs and applicable software standards, rules and conventions used in that process	

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

Annex G - Industry standards on AI and on application of AI in aviation

1. Standards and tools for Software (SW) development

As described in paragraph 2.4.4.3, EASA AMC 20-115D applies to applicants for and to Holders of Design Approvals (DAHs), as well as to developers of airborne systems and equipment containing software to be installed on type-certified aircraft, engines, and propellers, or to be used in ETSO articles.

The technical content of the EUROCAE and corresponding RTCA standards is absolutely equivalent. Among them the most relevant is ED-12C[20], which provides guidance for the production of airborne SW ensuring a level of confidence in safety that complies with airworthiness requirements.

ED-12C [20] covers the entire life-cycle of airborne SW starting with definition of system requirements derived from operational requirements and other considerations such as safety, security and required performance. The safety requirements result from the system safety assessment process and may include functional, integrity and reliability requirements, as well as design constraints.

The system safety assessment process determines and categorises the failure conditions of the system in terms of probability of occurrence and severity of the effects.

System requirements allocated to SW, including safety requirements, are developed and refined into SW requirements that are verified by the SW verification process activities. d. Safety-related requirements, including safety strategies, design constraints and design methods, such as, partitioning, dissimilarity, redundancy, or safety monitoring. In cases where the system is a component of another system, the requirements and failure conditions for that other system may also form part of the system requirements allocated to software.

According to the EASA guidelines, the SW DAL is applicable also to AI/ML applications.

However, AMC 20-115D [8]and ED-12C [20]only address initial airworthiness of aircraft and related airborne systems and equipment. They do not formally apply to SW embedded e.g. in ATM/ANS systems or aerodrome equipment.

And in fact, EASA AMC6 ATM/ANS.OR.C.005(a)(2) on safety support assessment and assurance of changes to the functional system includes provisions on SW assurance processes which should determine the rigour to which the evidence and SW arguments are produced. This AMC uses the term Software Assurance Level (SWAL), which is equivalent to SW DAL.

The rigour should increase with the safety criticality of the service supported by the SW, which is exactly the principle used in ED-12C.

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

Related EASA GM4 to AMC6 ATM/ANS.OR.C.005(a)(2) lists several industry standards which could be used by the ATM/ANS SP to assign DAL/SWAL to SW components. Among them, EUROCAE ED-12C [20] and ED-153 [19]. However, EASA does not recommend using any of them in relation to SWAL/DAL, leaving the SP free to choose.

ED-153 [19] was issued in 2009 and never amended, since the taxonomy proposed therein is different from the one in ED-12C [20]. Use of the latter is the most widespread in aviation. The scope of SW mentioned in the EU/EASA rules on aerodromes (i.e. EC Regulation 139/2014) is limited to tools used to generate aeronautical information. Therefore, EASA GM2 ADR.OPS.A.055 on tools and software states that tools can be qualified meeting point 2.4.5 (Aeronautical Data Tool Qualification) of EUROCAE ED-76A [26] or equivalent RTCA DO-200B [119]. However, ED-76A makes explicit recommendation to use EUROCAE ED-215 or equivalent RTCA DO-330, which are standards supplementary to ED-12C.

Table G. 1 - ED-12C and equivalent DO-178C

SW DAL	Description
A	SW whose anomalous behaviour, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a catastrophic failure condition for the aircraft
B	SW whose anomalous behaviour, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a hazardous failure condition for the aircraft
C	SW whose anomalous behaviour, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a major failure condition for the aircraft
D	SW whose anomalous behaviour, as shown by the system safety assessment process, would cause or contribute to a failure of system function resulting in a minor failure condition for the aircraft

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

E	SW whose anomalous behaviour, as shown by the system safety assessment process, would cause or contribute to a failure of system function with no effect on aircraft operational capability or pilot workload

2. Standards for cyber-security

All the documents listed in the table above were developed by EUROCAE WG 72 (Aeronautical Systems Security), working jointly with RTCA Special Committee (SC) 216 and they apply only to initial and continuing airworthiness of avionics.

However, WG 72 has already delivered additional standards on security of aeronautical systems, not limited to airborne applications, among which those reported in Table G. 3.

One could note that EC Delegated Regulation 2022/1645 [61], mandating ISMS for some aviation organisations, is expected to be complementary to an EC Implementing Regulation, in progress in January 2023. Jointly, these two Regulations will mandate ISMS for all aviation organisations, possibly from 2025/Q4.

Both Regulations are based on EASA Opinion 03/2021 [14], in turn proposed by NPA 2019-07. The latter however did not propose any AMC/GM for ISMS.

However, Appendix A of EUROCAE ED-201A[30] recognises that ISO/IEC 27005:2022 comprehensively covers ISMS for any organisation, not limited to aviation and that the mentioned ISO/IEC standard is fully compliant with the prescriptions of ICAO Annex 17 [101]for ISMS.

Application of ISO/IEC 27005:2022, complemented by EUROCAE more detailed standards (e.g. ED-201A[30], ED-205A[31], etc) as appropriate, would allow certification of ISMS by Notified Bodies (NBs), which would reduce the burden for certification of ISMS by aviation authorities. This may happen, as AltMoC, even in the absence of explicit recognition by EASA.

At the moment of writing this document there is no duplication of activities between EUROCAE WG 72 and WG 114; the latter dealing with AI/ML. In other words, the industry standards presented in this paragraph could apply even when the SW applications are based on AI/ML.

Furthermore EUROCAE WG 72 is developing:

- A new ED/DO document to address ISMS, whose publication is expected in 2024/Q3. This ED is not expected to deviate from ISO/IEC 27005:2022 although it may add more details; and
- A new ED/DO document addressing minimum standards for the generation, storage, and delivery of data, including Operational Flight Programs, sensitive maintenance data records and other security relevant data to complement ED-201A. Publication of such ED is expected by the end of 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

Table G. 2 -EASA/EUROCAE and RTCA standards

Document	Description	Status
ED-202A/DO-326A[25] Airworthiness Security Process Specification	Guidance for activities for aircraft development and certification, to handle the threat of UEI to aircraft safety and is intended to be used in conjunction with other applicable guidance material	Published in June 2014. MoC for AMC 20-42 for organisations involved in initial airworthiness (e.g. DOA, POA). Update expected in 2024 Q2
ED-203A/DO-356[27]Airworthiness Security Methods and Considerations	Detailed guidance for architecture and design of avionics in relation to cybersecurity.	Published in June 2018. MoC for AMC 20-42
ED-204A/DO-355[29]Information Security Guidance for Continuing Airworthiness	Guidance for maintaining security of avionics throughout the SW lifecycle, including ICA from manufacturer and interaction with systems used during ground operations or maintenance.	Published in June 2014. MoC for AMC 20-42 for organisations involved in aircraft operations and in continuing airworthiness (e.g. CAMO, MOA).

Table G. 3 -WG 72, Standards on security of aeronautical systems

Document	Description	Status
ED-201A [30] Aeronautical Information Systems security information guidance	Guidance for implementation of ISMS for all aviation organisations involved in the life cycle of aeronautical information, from data originators, to AIS SP to all users and equipment (ground or airborne) which uses such information.	Published in December 2021.
ED-205A[31]	Guidance for activities for development and certification of	Published in July 2022. Possible MoC for EC Regulation 2017/373, although not

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

Process standard for security certification and declaration of ATM/ANS ground systems	ATM/ANS ground systems, to handle the threat of UEI. Not exhaustive for ISMS by ANSPs	explicitly mentioned by EASA in the related AMC/GM
ED-206[32] Guidance on security event management	Detection of security threats, response and recovery, in the context of ISMS	Published in June 2022. A document revision (ED-206A) is expected in 2024/Q4

3. Gaps for standards on AI

According to the gap report released in December 2022 by the American National Standard Institute (ANSI) a gap exists for use of AI during fully autonomous UA flights:

ANSI believes that to fill this gap further research is needed and in the end it recommends:

Table G. 4 - ANSI, Gaps for standards on AI

Rec.	Text	Comments
1)	Develop standards and guidelines for the safety, performance, and interoperability of fully autonomous flights, taking into account all relevant factors needed to support the seamless integration of UAS into US National Airspace. System (NAS). These include: type of aircraft/UA, operators/pilots/crew, air traffic controllers, airspace service suppliers/providers, lost link procedures, human factors/human-machine interactions as well as levels of human intervention, etc.	Contrary to EU/EASA, in the USA until the end of 2022 there were no clear rules for operations in the UAS specific category. This recommendation must therefore be put in the less developed UAS context and it is not fully applicable to the EU.
2)	Encourage the development of standards to address fully autonomous flights, per the	Necessary industry standards instead are not yet fully developed even in the EU or on the global scale.

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

	FAA Reauthorization Act of 2018 and the needs of the UAS industry and end users.	Efforts should be concentrated on EUROCAE WG 114 which is already active on the matter, but until the end of 2022 has not yet released any published standard. WG 114 should however work synergistically with ISO and SAE which already have experience on the subject.
3)	Encourage the development of consistent, uniform, harmonised, standardised, and aviation field-acceptable definitions of terms like autonomy, automation, autonomous, AI, machine learning, deep learning, etc. This will lay a foundation for identification of correct and incorrect definitions/ terminologies.	already covered in paragraph 3.3

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

Annex H - References

[1] American National Standard Institute (ANSI. 2022, *ANSI UAS Roadmap - Gap report Dec 2022*

[2] American Society for Testing and Materials (ASTM), 2019, Technical Report TR1-EB, *Autonomy Design and Operations in Aviation: Terminology and Requirements Framework*

[3] Christensen Clayton, 1997, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail (Management of Innovation and Change)*

[4] Comisión de Investigación de Accidentes e Incidentes de Aviación Civil (Spain), 1979, *A-102/1977 y A-103/1977. Accidente Ocurrido el 27 de Marzo de 1977 a las Aeronaves Boeing 747, Matrícula PH-BUF de K.L.M. y Aeronave Boeing 747, matrícula N736PA de PANAM en el Aeropuerto de los Rodeos, Tenerife (Islas Canarias)*, https://www.mitma.es/organos-colegiados/ciaiac/publicaciones/informes-relevantes/accidente-ocurrido-el-27-de-marzo-de-1977-aeronaves-boeing-747-matricula-ph-buf-de-klm-y-aeronave-boeing-747-matricula-n736pa-de-panam-en-el-aeropuerto-de-los-rodeos-tenerife-islas-canarias

[5] Council, 1985a, *Resolution of 7 May 1985 on a new approach to technical harmonisation and standards*

[6] Council, 1985b, *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* [1985] OJ L 210/28

[7] EASA, 2014, *Certification Specifications (CS)and Guidance Material (GM) for Aerodromes Design* (CS-ADR-DSN) as lastly amended by issue 6 0f 30 March 2022

[8] EASA, 2017, *AMC 20-115D Airborne Software Development Assurance Using EUROCAE ED-12 and RTCA DO-178*, ED Decision 2017/020/R

[9] EASA,2018, Commission Implementing Regulation (EU) 2018/139

[10] EASA, 2019, *Management of information security risks*, NPA 2019-07 of 16 January2019

[11] EASA, 2020, *Artificial Intelligence Roadmap. A human-centric approach to AI in aviation*, Cologne

[12] EASA, 2021a, AMC 20-42 Airworthiness information security risk assessment, introduced by Amendment 18 to AMC 20 on 01 January 2021

[13] EASA, 2021b, Concept Paper: *First usable guidance for Level 1 machine learning applications,* Issue 01

[14] EASA, 2021c, *Opinion No 03/2021 on Management of information security risks* of 11 June 2021

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

[15] EASA, 2022a, *Certification Specifications and Guidance Material for Aerodrome Design,* CS-ADR-DSN, Issue 6 of 29 Mar 2022

[16] EASA, 2022b, *Easy Access Rules for Airworthiness and Environmental Certification (Regulation* EU No 748/2012)

[17] EASA, 2022c, *AMC and GM to Regulation (EU) 2021/664 on a regulatory framework for the U-space*, issue 1 of 16 December 2022, Annex to Executive Director (ED) Decision 2022/022/R https://www.easa.europa.eu/en/downloads/137405/en

[18] EASA, 2022d, *CS 25.1309 Equipment, systems and installations and related AMC*, in Easy Access Rules for Large Aeroplanes (CS 25) (Amendment 27)(pdf), updated on 21 December 2022, https://www.easa.europa.eu/en/downloads/136694/en consulted on 08 January 2023

[19] EUROCAE, 2009, *Guidelines for ANS SW safety assurance*

[20] EUROCAE, 2012a, *ED-12C, Software Considerations in Airborne Systems and Equipment Certification*, including corrigendum 1 of February 2021

[21] EUROCAE, 2012b, ED-215, *Software Tool Qualification Considerations* of 1 January 2012

[22] EUROCAE, 2012c, ED-216, *Formal Methods - Supplement to ED-12C and ED-109A* of 1 January 2012

[23] EUROCAE, 2012d, ED-217, Object-Oriented Technology and Related Techniques - Supplement to ED-12C and ED-109A of 1 January 2012

[24] EUROCAE, 2012e, ED-218, *Model-Based Development and Verification - Supplement to ED-12C and ED-109A* of 1 January 2012

[25] EUROCAE, 2014, ED-202A/DO-326A, A*irworthiness Security Process Specification* of June 2014

[26] EUROCAE, 2015, ED-76A, Standards for Processing Aeronautical Data

[27] EUROCAE, 2018, ED-203A, Airworthiness security methods and considerations

[28] EUROCAE, 2019, Terms of Reference (ToR) of WG-114 Artificial Intelligence in Aeronautical Systems of 4 June 2019

[29] EUROCAE, 2020, ED-204A, Information security guidance for continuing airworthiness

[30] EUROCAE, 2021, ED-201A, Aeronautical Information Systems security information guidance

[31] EUROCAE, 2022a, ED-205A, Process standard for security certification and declaration of ATM/ANS ground systems

[32] EUROCAE, 2022b, ED-206, Guidance on security event management

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

[33] EUROCONTROL, 2020, The FLY AI Report -Demystifying and Accelerating AI in Aviation/ATM, developed by the European Aviation/ATM AI High Level Group (EAAI HLG), 05 March, 2020 https://www.eurocontrol.int/publication/fly-ai-report

[34] European Council, 1985, 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 (consolidated version)

[35] European Commission (EC), 2001, Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (consolidated version)

[36] EC, 2001a, Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use

[37] EC, 2002, [10] Directive 2002/21 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L108/33

[38] EC, 2004, Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency

[39] EC, 2006, Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) (consolidated version)

[40] EC, 2009, Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys (consolidated version)

[41] EC, 2012a, *Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations* as lastly amended by Commission Implementing Regulation 2022/203 of 14 February 2022

[42] EC, 2012b, *Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations* pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council, as lastly amended by Commission Implementing Regulation (EU) 2022/2203 of 11 November 2022

[43] EC, 2014, Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (consolidated version)

[44] EC, 2014a, *Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes* pursuant to Regulation

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

(EC) No 216/2008 of the European Parliament and of the Council, as lastly amended by Commission Delegated Regulation (EU) 2022/2074 of 20 July 2022

[45] EC, 2015, *Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security*, as lastly amended by Commission Implementing Regulation (EU) 2022/1174 of 7 July 2022

[46] EC, 2017, *Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight,* repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011, as lastly amended by Commission Implementing Regulation (EU) 2022/938 of 26 July 2022

[47] EC, 2018, European Commission, Staff Working Document, Evaluation of 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 Accompanying the document Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the Application of the Council Directive on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (85/374/EEC) (SWD (2018)157)

[48] EC, 2018a, Communication 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*, Brussels, 25.4.2018 – (COM(2018) 237 final)

[49] EC, 2018b, Directorate-General for Research and Innovation, European Group on Ethics in Science and New Technologies, *Statement on artificial intelligence, robotics and 'autonomous' systems*: Brussels, 9 March 2018, Publications Office, 2018

[50] EC, 2019a, *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft*, as lastly amended by Commission Implementing Regulation (EU) 2022/525 of 1 April 2022

[51] EC, 2019b, *Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures*

[52] EC, 2019c, Directorate-General for Justice and Consumers, Liability for artificial intelligence and other emerging digital technologies, Brussels, 27.11.2019

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

[53] EC, 2019d, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, Building Trust in Human-Centric Artificial Intelligence, Brussels, 8.4.2019 – (COM(2019) 168 final)

[54] EC, 2020a, Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, Brussels, 19.2.2020 – (COM(2020) 64 final)

[55] EC, 2020b, *White paper on Artificial Intelligence – A European approach to excellence and trust*, Brussels, 19.2.2020 – (COM(2020) 65 final)

[56] EC, 2021a, Proposal for a *Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts*, Brussels, 21.4.2021 – (COM(2021) 206 final)

[57] EC, 2021b, Commission staff working document impact assessment accompanying the proposal for *a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts,* Brussels, 21.4.2021 – (SWD(2021) 84 final, part 1/2)

[58] EC, 2021c, *Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space*

[59] EC, 2021d, *AI Watch – Defining Artificial Intelligence 2.0. towards an operational definition and taxonomy for the AI landscape*, (JRC Technical Report), Luxemburg, 2021

[60] EC, 2021e, European Commission, Directorate-General for Justice and Consumers, Karner, E., Koch, B., Geistfeld, M., *Comparative law study on civil liability for artificial intelligence*, Publications Office of the European Union, 2021.

[61] EC, 2022a, Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the EP 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 EC Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending EC Regulations (EU) No 748/2012 and (EU) No 139/2014

[62] EC, 2022b, *Proposal for a directive of the European Parliament and of the Council on liability for defective products*, Brussels, 28.09.2022 – (COM(2022) 495 final)

[63] EC, 2022c, Commission staff working document impact assessment report Accompanying the document *Proposal for a Directive of the European Parliament and of the Council on liability for defective products*, Brussels, 28.09.2022 – (SWD(2022) 316 final)

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

[64] EC, 2022d, *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)*, Brussels, 28.09.2022 – (COM (2022) 496 final)

[65] EC, 2022e, Commission staff working document impact assessment report Accompanying the document *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence* Brussels, 28.09.2022 – (SWD(2022)319 final)

[66] European Parliament Research Service (EPRS), 2020, Artificial intelligence: from ethics to policy, Brussels, June 2020 – (PE 641.507)

[67] European Union (EU), 1986, *Single European Act*, Official Journal of the European Communities, L 169, 29 June 1987

[68] EU, 2001, DIRECTIVE 2001/95/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 December 2001 on general product safety

[69] EU, 2002a, Directive 2002/21/EC of the European Parliament (EP) and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (Framework Directive) [2002] OJ L108/33

[70] EU, 2002b, Regulation (EC) No 1592/2002 of the EP and of the Council of 15 July 2002 on *common rules in the field of civil aviation and establishing a European Aviation Safety Agency,* repealed in 2008

[71] EU, 2002c, *Regulation (EC) No 2320/2002 of the EP and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security*

[72] EU, 2004, Regulation (EC) No 549/2004 of the EP and of the Council of 10 March 2004 laying down the *framework for the creation of the single European sky (the framework Regulation)*, as lastly amended by Regulation (EC) No 1070/2009 of the EP and of the Council of 21 October 2009

[73] EU, 2006, Directive 2006/42/EC of the EP and of the Council of 17 May 2006 on *machinery*, and amending Directive 95/16/EC (recast) [2006] OJ L 157/49

[74] EU, 2008a, Regulation (EC) No 216/2008 of the EP and of the Council of 20 February 2008 on *common rules in the field of civil aviation and establishing a European Aviation Safety Agency*, and repealing Council Directive 91/670/EEC, Regulation (EC) No 1592/2002 and Directive 2004/36/EC

[75] EU, 2008b, Regulation (EC) No 300/2008 of the EP 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, as lastly amended by Commission Regulation (EU) No 18/2010 of 8 January 2010

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

[76] EU, 2009, Regulation (EC) No 1108/2009 of the EP and of the Council of 21 October 2009 *amending Regulation (EC) No 216/2008 in the field of aerodromes, air traffic management and air navigation services* and repealing Directive 2006/23/EC

[77] EU, 2010, Regulation (EU) No 996/2010 of the EP and of the Council of 20 October 2010 on the *investigation and prevention of accidents and incidents in civil aviation* and repealing Directive 94/56/EC, as lastly amended by Regulation (EU) 2018/1139 of the EP and of the Council of 4 July 2018

[78] EU, 2014, Regulation (EU) No 376/2014 of the EP and of the Council of 3 April 2014 on the *reporting, analysis and follow-up of occurrences in civil aviation*, amending Regulation (EU) No 996/2010 of the EP and of the Council and repealing Directive 2003/42/EC of the EP and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007, as lastly amended by Regulation (EU) 2018/1139 of the EP and of the Council of 4 July 2018

[79] EU, 2016a, Consolidated (2016) version of the *Treaty on the Functioning of the EU* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E/TXT

[80] EU, 2016b, Regulation (EU) 2016/679 of the EP 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 - GDPR)

[81] EU, 2016c, Directive 2016/680/EU 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

[82] EU, 2016d, *Directive (EU) 2016/1148 of the EP and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*

[83] EU, 2018, Regulation (EU) 2018/1139 of the EP 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

[84] EU, 2018a, Regulation 2018/1725/EU of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal

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

data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

[85] EU, 2022, Directive (EU) 2022/2555 of the EP and of the Council of 14 December 2022 on *measures for a high common level of cybersecurity across the Union,* amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[86] EUR-Lex, 2022, *Supporting telecommunications networks and digital service infrastructures across Europe* (Summaries of legislation) – available here: https://eur-lex.europa.eu/EN/legal-content/summary/supporting-telecommunications-networks-and-digital-service-infrastructures-across-europe.html

[87] Federal Aviation Administration (FAA), 2023, Smartsheet External Small Airplane All Categories Report, https://www.faa.gov/sites/faa.gov/files/small_airplane_issues_list_jan2023.pdf consulted on 21 January 2023

[88] L. Floridi, 2018, *Soft Ethics and the Governance of the Digital*. *Philos. Technol.* 31, 1–8 (2018).

[89] L. Floridi, J. Cowls, 2022, A Unified Framework of Five Principles for AI in Society . In Machine Learning and the City, S. Carta (Ed.).

[90] Heinrich H. W., 1931, *Industrial Accident Prevention, A Scientific Approach*

[91] HLEG, 2018, *A definition of AI: Main capabilities and scientific disciplines*, Brussels, 18.12.2018

[92] HLEG, 2019, *Ethics Guidelines for Trustworthy AI*, Brussels, 8.4.2019

[93] HLEG, 2020a, The Assessment List for Trustworthy Artificial Intelligence (ALTAI), Brussels, 16.07.2020

[94] HLEG, 2020b, Sectoral considerations on the policy and investment recommendations for trustworthy artificial intelligence, Brussels, 23.07.2020

[95] International Civil Aviation Organisation (ICAO), 1944, *Convention on International Civil Aviation*, Doc 7300/9, 9th edition, 2006

[96] ICAO (2022) Artificial Intelligence (AI). Available at: https://www.icao.int/safety/Pages/Artificial-Intelligence-(AI).aspx (Accessed: January 31, 2023).

[97] ICAO, 1989, *Human Factors Digest No.1*, Circular 216-AN/131

[98] ICAO, 2016, Annex 19 to the Chicago Convention, *Safety Management*, 2nd 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

[99] ICAO, 2018a, Annex 6 to the Chicago Convention, *Aircraft Operations, Part I — International Commercial Air Transport — Aeroplanes*, Eleventh Edition, July 2018

[100] ICAO, 2018b, *Safety Management Manual* (SMM), Doc 9859, 4th edition, 2018

[101] ICAO, 2020, Annex 17 to the Chicago Convention, *Safeguarding International Civil Aviation Against Acts of Unlawful Interference*, 11th Edition, March 2020

[102] ICAO, 2022, Annex 14 to the Chicago Convention, Volume I, Aerodrome Design and Operations, Ninth Edition, July 2022

[103] International Standard Organisation (ISO), 2015a, *ISO 9001:2015 Quality management systems — Requirements*

[104] ISO, 2015b, *ISO/IEC 19793:2015 Information technology — Open Distributed Processing — Use of UML for ODP system specifications,* https://www.iso.org/standard/68641.html

[105] ISO, 2022a, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, ISO/IEC 27001:2022

[106] ISO 2022b, ISO 23629-12:2022 *UAS traffic management (UTM) — Part 12: Requirements for UTM service providers*

[107] ISO/IEC, 2022c, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, ISO/IEC 27005:2022, https://www.iso.org/standard/80585.html

[108] ITU-T, 2016, *Key findings, recommendations for next steps and future work, Deliverable 5 by Focus Group on Aviation Applications of Cloud Computing for Flight Data Monitoring* https://www.itu.int/pub/T-FG-AC-2016-5

[109] JARUS, 2021, *Terms of Reference* (ToR), v8.0, 2021

[110] JARUS, 2023, *Automation and Autonomy for UAS*, v0.5, 11 January 2023

[111] Masutti A., Tomasello F., 2018, *International Regulation of Non-Military Drones*

[112] J. Morley, L. Floridi, L. Kinsey, A. Elhalal (2020). From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles into Practices. Sci Eng Ethics. 2020 Aug;26(4):2141-2168.

[113] Pesquet-Popescu B., 2021, EUROCAE WG114–SAE G34: a joint standardisation initiative to support Artificial Intelligence revolution in aeronautics, slides presented to FlyAI webinar on 28 April 2021 https://www.eurocontrol.int/sites/default/files/2021-04/flyai-4-thales.pdf

[114] Radio Technical Commission for Aeronautics (RTCA), 2011a, DO-178C, *Software Considerations in Airborne Systems and Equipment Certification* of 13 December 2011

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

[115] RTCA, 2011b, DO-330, *Software Tool Qualification Considerations* of 13 December 2011;

[116] RTCA, 2011c, DO-333, *Formal Methods - Supplement to DO-178C and DO-278A* of 13 December 2011

[117] RTCA, 2011d, DO-332, *Object- Oriented Technology and Related Techniques Supplement to DO-178C and DO- 278A* of 13 December 2011

[118] RTCA, 2011e, DO-331, *Model-Based Development and Verification Supplement to DO-178C and DO-278A* of 13 December 2011

[119] RTCA, 2015, DO-200B, *Standards for Processing Aeronautical Data*

[120] Society of Automotive Engineers (SAE), 2014, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, J3016 (APR2021), revised April 2021-04

[121] Tomasello F., 2013, Lecture on *EASA: il pilastro centrale per la safety regulation del 'total aviation system*', delivered on 16 May 2013 during the Seminar on Safety delle operazioni aeronautiche nella regolamentazione europea, organised by State University Parthenope in Napoli (IT)

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