Final Report for Staffing (6-15)

___________________________ _______________

Akbar Sultan Date
NASA, AOSP Director
Aeronautics Research Mission Directorate (ARMD)

______________________________ ________________

Steve Bradford Date
FAA, Chief Scientist
Architecture & NextGen Development

PAGE LEFT INTENTIONALLY BLANK

Executive Summary

The Federal Aviation Administration (FAA) Reauthorization Act of 2018, Section 741, instructs the FAA to develop a research plan for the certification of new technologies into the National Airspace System (NAS). This Research Plan fulfills this mandate by providing an assessment of existing gaps and challenges in certifying new Artificial Intelligence (AI) applications in the NAS and defining a strategy and three-step approach to address these gaps.

Traditional software assurance practices used by the FAA and international entities do not provide sufficient consideration of new and emerging technologies. Existing practices do not consider assurance requirements for the data-driven learning aspects of Machine Learning (ML), nor do they address challenges in evaluating the trustworthiness (e.g., technical robustness, "explainability," algorithm determinism and ethics) of AI technologies. In addition, current practices rely on low-level traceability of system requirements and repeatable testing requirements, which is not appropriate or feasible for many AI technologies. This Research Plan identifies gaps in current software assurance practices, evaluates emerging best practices and efforts in meeting AI certification challenges, and recommends changes or amendments to existing FAA certification requirements.

The mission of the FAA is to provide the safest and most efficient airspace system in the world. A growing number of aviation applications of AI demonstrate how new algorithms can increase the accuracy of predictions and identify trends or correlations that may be difficult for humans to identify (e.g., traffic forecasting and weather patterns). AI can be considered an umbrella term for a collection of approaches, such as ML, that mimic human cognition with hardware and software. While the benefits of AI are clear, the evolving, non-deterministic nature of these algorithms presents challenges for the air traffic management (ATM) industry regarding the certification of these new technologies.

The purpose of this Research Plan is to specify the research and steps needed to develop an approach to certify AI applications in the NAS. To carry out the Research Plan, the FAA will partner with the National Aeronautics and Space Administration (NASA) to develop an AI Certification Framework as well as to assess the feasibility of AI applications for certification using ongoing FAA and NASA joint AI-based research and development efforts. The FAA will also engage with industry and international standards bodies to stay informed of related efforts.

The Research Plan consists of three steps: (1) research the certification needs for new technologies, (2) validate and verify the certification framework, and (3) develop an implementation strategy for the certification framework. By fulfilling these steps, the FAA will be able to plan for and support the safe and secure implementation of future AI applications into the NAS.

Table of Contents

List of Figures

List of Tables

1 Introduction

The mission of the Federal Aviation Administration (FAA) is to provide the safest and most efficient airspace system in the world. A growing number of aviation applications of Artificial Intelligence (AI) and Machine Learning (ML) demonstrate how algorithms can increase the accuracy of predictions and identify trends or correlations that may be difficult for humans to identify. While the potential benefits of AI and ML are clear, the evolving, non-deterministic nature of these algorithms presents challenges for the air traffic management (ATM) industry, aircraft, and new entrants (e.g., Unmanned Aircraft System (UAS)) regarding the certification of these algorithms. The FAA has been tasked to develop a Research Plan to identify the research and steps needed to certify new technologies, including AI and ML algorithms.

1.1 AI and ML Overview

Even though AI has had a long history with increasingly rapid-paced advances, it has no universally agreed-on definition. The most widely cited text on AI provides extracts of no fewer than eight definitions of AI from other standard textbooks, stressing such terms as "thought processes," "reasoning," and "rationality" [1]. In a recent historical survey of the field, AI is defined as "that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment" [2]. Thus, AI also can be an umbrella term for a collection of approaches for imitating and/or augmenting human cognition with hardware and software.

One widely studied AI approach is ML, which refers to a set of techniques "designed to detect patterns in, and learn and make predictions from data" [3]. This approach is grounded in the belief that AI systems must learn to understand their environments (and problem domains) on their own, allowing machines to learn from examples and conduct tasks without explicit programming. There are many ML techniques, including deep learning (DL), genetic algorithms, neural networks, and reinforcement learning. Figure 1 provides context definitions for, and relationships and differences between AI, ML, and DL.

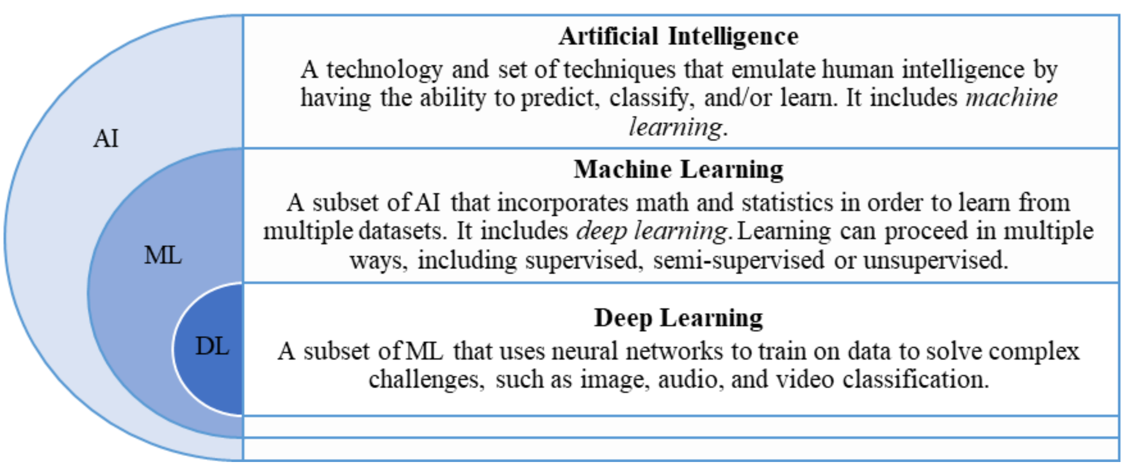

Figure 1: AI, ML, and DL Taxonomy

In ML, the system is "trained" using relevant sample (i.e., training) data and learns a predictive model to perform tasks without the explicit programming of rules that would be used in traditional decision-making processes. Learning generally proceeds in one of three ways:

- *Supervised learning*: The system uses labeled training data—that is, each element is designated as an input-output pair, where the output is the "correct" desired value that one wishes the system to learn to associate with a given input.
- *Unsupervised learning*: The system discovers structures in data on its own—that is, no reward signals are given to "nudge" the system as it processes the training data.
- *Reinforcement learning*: The system uses unlabeled training data—that is, it neither uses input-output pairs for training nor is completely unsupervised. For correct responses, it receives the same type of response as if supervised (e.g., response is "correct"). For incorrect responses, it is told only that an "incorrect response" was given but is not informed of what the correct response was.

While there are many different types of technologies under the term AI, ML is of particular interest because of the high level of research and development that has been applied across industry sectors to mature this technique. For the FAA, there are numerous potential opportunities for the use of ML to support various aviation-related activities. In *A Survey of Machine Learning Suitability for Air Traffic Management (ATM) Applications*, the authors identified multiple areas of ATM where ML techniques can be used for analysis and classification [4]. The applications described in this document provided methods to support an ATM decision-making framework and were expressed as general high-level concepts and three types of ML: supervised, unsupervised, and reinforcement learning.

1.2 Statutory Requirements

Section 741 of the FAA Reauthorization Act of 2018 directs the Administrator of the FAA, in consultation with National Aeronautics and Space Administration (NASA), to transmit a comprehensive research plan for the certification of new technologies into the National Airspace System (NAS). The plan must be informed by recommendations from the 2015 National Research Council's review of the FAA's 2014 Research Plan [5] and include the following elements:

- A description of the strategic and prescriptive value of the research plan;
- An explanation of the expected outcomes from executing the plan;
- An assessment of the FAA's plan to use research and development to improve cybersecurity over the next 5 years;
- An assessment of the current software assurance practices, and the desired level or attributes to target in the software assurance program; and
- Best practices in research and development used by other organizations, such as NASA, NavCanada, and Eurocontrol.

2 Document Purpose and Objectives

2.1 Purpose

The Research Plan specifies the research and steps needed to develop a framework for the certification of new technologies in the NAS.

2.2 Objectives

The Research Plan will accomplish this purpose through the following objectives:

- **Objective 1 – Identify software assurance best practices and gaps:** Analyze current FAA software assurance and certification processes to identify existing gaps for certifying AI technologies for ATM applications. Identify best practices for AI applications as well as ongoing international efforts to address AI certification challenges.
- **Objective 2 – Investigate feasibility of AI applications for certification:** Partner with NASA to identify a range of potential use cases for AI applications. Leverage ongoing FAA and NASA joint AI-based research and development efforts to inform the AI Certification Framework.
- **Objective 3 – Develop an AI Certification Framework:** Create an initial certification framework and validate the framework with use cases and ongoing AI-based activities. Then, plan for the integration of the framework by engaging with stakeholders.

3 FAA NextGen and NASA Partnership

The full range of FAA and NASA research and development capabilities will support the research activities described in this document through the following activities:

- Collaborate on ongoing and future efforts to research and explore AI applications for future implementation; these efforts may serve to inform and validate the AI Certification Framework.
- Collaborate with industry to identify and explore new technologies for certification.
- Stay informed of ongoing work by recognized international standards bodies (e.g., the International Civil Aviation Organization, the Society of Automotive Engineers (SAE), and the European Organisation for Civil Aviation Equipment (EUROCAE)) on AI/ML certification challenges and standards.

4 Certification Strategy

Traditional software development does not provide sufficient consideration of new and emerging technologies, such as AI and ML. The FAA may need to amend existing regulations, orders, policies, and procedures to address unique technical aspects of AI and ML and appropriately validate and verify AI technologies. Thus, the outcomes of the Research Plan must identify and provide validated solutions to the gaps and challenges found in existing software certification processes. This resulting AI Certification Framework will be based on existing guidelines for traditional software assurance; however, it must be adjusted to include AI-specific needs. Process improvements are needed to address the certification of new technologies throughout the software development life cycle, including:

- Amendments to existing requirements (e.g., model and requirements validation, testing, and verification) for new technologies that consider unique attributes of AI applications, and
- New checkpoints or revised certification documentation (e.g., AI suitability assessment or AI risk or trustworthiness assessment) for AI technologies.

The Research Plan and resulting AI Certification Framework are the foundational steps to the eventual certification of new AI applications in the FAA. Table 1 illustrates the proposed values and outcomes for AI certification.

Table 1: AI Certification Values and Outcomes

Values	**Outcomes**
1. Provide a basis and considerations for new and updated certification requirements for AI applications 2. Update existing FAA software assurance practices with AI software-specific criteria 3. Leverage existing processes and framework that are familiar to FAA staff 4. Approve new technologies with minimal additional effort 5. Set up the FAA to be a leader in aviation AI use and approval/certification 6. Increase understanding for developers of AI requirements early in the development process to improve the efficiency of FAA AI applications for software development	1. Outline gaps in current software assurance practices 2. Recommend additions or revisions to current FAA software approval processes 3. Consolidate AI certification best practices 4. Recommend technical checklists and amendments to specific FAA certification processes 5. Provide draft AI objectives and criteria for testing the AI certification process 6. Define certification requirements, policies, procedures, and regulations needed to enable use cases using AI applications

Determining changes necessary to existing software assurance and certification processes requires detailed research and analysis to inform certification requirements for AI applications. The following sections summarize an initial assessment of current software assurance practices, identified AI certification challenges, and cybersecurity research that will be further evaluated in the Research Plan.

4.1 Current Software Assurance Practices

The FAA's software assurance and certification practices are applicable to both airborne and non-airborne Communications, Navigation, Surveillance, and ATM (CNS/ATM) systems. The FAA recognizes the use of identical guidelines published by the Radio Technical Commission for Aeronautics (RTCA) and EUROCAE to demonstrate compliance with software assurance [6][7]:

- RTCA DO-178C (EUROCAE ED-12C), *Software Considerations in Airborne Systems and Equipment Certification* [8] and
- RTCA DO-278A (EUROCAE ED-109A), *Software Integrity Assurance Considerations for CNS/ATM Systems* [9].

These standards are referenced throughout the FAA's Safety Risk Management (SRM) process for system acquisitions and are considered the primary method of ensuring software design rigor [10]. However, the RTCA standards reflect a traditional software development process that poses some limitations to AI and ML technologies, such as the following:

- Traditional "development assurance" does not consider the challenges of AI and ML, such as trustworthiness, explainability, and correctness. Instead, "learning assurance" should be defined to take into account the dynamic, learning aspect of AI and ML [11]:
    - Trustworthiness ensures that AI application is lawful, ethical, and robust [12].
    - Explainability deals with the capability to provide the human with understandable and relevant information on how an AI/ML application is coming to its results [13].
    - Learning assurance refers to the confidence and evidence that the AI and ML algorithm created through a data-driven learning process meets given requirements [9][13].
- Current assurance practices require verification of repeatable and deterministic results that are not characteristic of many AI and ML technologies [14][12].
- Current assurance practices require complete traceability of system requirements, which may be difficult for AI and ML technologies that use learning or adaptive behaviors [14].
- Current assurance practices require repeatable, comprehensive testing of typical input ranges, which are difficult to define for AI and ML technologies that may have very large or dynamic input boundaries [14].
- Current assurance practices do not include considerations for the training and testing datasets used in ML technologies [12].

Furthermore, in addition to traditional software assurance processes, other methods of certification may be considered and applicable for AI technologies [15]. For example, the FAA's Overarching Properties initiative considered the use of property-based certification [16]. In a property-based method, the applicant must demonstrate that the software meets a pre-defined set of properties as opposed to the traditional process-based method, where the applicant must complete a pre-defined set of processes (e.g., RTCA DO-178C) throughout the software development life-cycle.

Currently, the FAA's Validation and Verification (V&V) process and Test and Evaluation (T&E) processes are applicable to traditional software development and technologies. The introduction of new technologies will likely require expansion of the current V&V and T&E processes to better support the challenges listed. Thus, the Research Plan must consider current FAA software assurance practices as a basis for the AI Certification Framework to ensure its future integration.

4.2 Best Practices and Certification Challenges

A number of organizations have begun to establish working groups or guidelines for the use of AI and ML technologies, but U.S. and international entities that develop relevant standards have yet to address fully the unique challenges related to the certification of AI applications. Table 2 lists some of these preliminary efforts that strive to develop best practices for AI and ML technology use in specific agencies or domains as well as for general use.

Table 2: Summary of Select International AI and ML Certification-Related Efforts

Entity	**Description**
FAA	The FAA updated its Order 1370.121A FAA Information Security and Privacy Program Policy in 2020 to include an appendix on AI [17]. The order addresses 10 evaluation factors for AI systems, levels at which AI systems can operate, ethical considerations, and operation requirements. In addition, the FAA and NASA completed a series of industry coordination activities in 2020 to further understand challenges related to AI and ML, including algorithm determinism, algorithm evolution, algorithm trust, bias, data applicability, security, transparency, and user trust [18].
European Union Aviation Safety Agency (EASA)	EASA released a roadmap in 2020 detailing three increasingly autonomous levels of AI and ML use in aviation, challenges in AI certification, and the need for an AI trustworthiness framework [19]. A 2021 draft concept paper describes the AI trustworthiness framework and use cases for Level 1 use of AI and ML (i.e., assistance to human) [13].
SAE and EUROCAE	The SAE and EUROCAE joint international committee on Artificial Intelligence in Aviation (SAE G-34/EUROCAE WG-114) is developing a series of standards related to AI certification for aviation products. A 2020 draft Statement of Concerns summarizes current gaps, challenges, and considerations in AI certification [12]. The joint working group includes members from industry and government agencies, including agencies in the U.S. and Canada.
U.S. Department of Defense (DOD)	DOD has developed guidelines for the use of autonomy in weapon systems. Directive 3000.09, updated in 2017, requires "rigorous" verification and validation as well as "realistic" testing and evaluation [20]. It recognizes the potential for unanticipated and emergent behavior, and that these algorithms may change as they continue to operate and learn.
U.S. Food and Drug Administration (FDA)	FDA published a proposed regulatory framework for reviewing premarket modifications to AI- and ML-based “Software as a Medical Device” in 2019 [21]. The framework offers a procedure for evaluating and monitoring the software throughout its life cycle with FDA checkpoints. FDA is updating the framework based on community feedback.
National Institute of Standards and Technology (NIST)	In 2019, NIST was tasked by Executive Order 13859, Maintaining American Leadership in Artificial Intelligence, to develop a plan for federal engagement in developing standards for the use of AI technologies.. In response, NIST identified nine focus areas for AI standards along with tools that will aid in advancing the adoption of AI technologies [22].
Dependable and Explainable Learning (DEEL)	The DEEL certification workgroup published a white paper detailing high-level properties necessary for ML certification as well as challenges of ML in certified systems [15].

The challenges associated with AI and ML technologies and certification are well documented and identified by many organizations. However, possible mitigations to these challenges still are being developed. Table 3 lists examples of commonly cited challenges and evaluation factors. While there is no existing AI certification process that can be leveraged, the Research Plan must consider the ongoing work of other U.S. and international organizations and standards bodies.

Table 3: Common Challenges and Evaluation Factors to AI Certification

Data	**Law & Ethics**	**Robustness**	**Safety & Security**	**Verification & Validation**
Data Governance Data Quality Privacy	Diversity Environmental Well-being Fairness Human Agency Human Oversight Liability Non-discrimination Societal Well-being	Accuracy Consistency Corrigibility Maintainability Reliability Technicality Stability Suitability	Recoverability Resiliency Safety Risk Management Security	Accountability Auditability Explainability Predictability Specifiability Traceability Transparency Understandability Verifiability

4.3 Cybersecurity and Data Security Research for AI Applications

The FAA's Cybersecurity Strategy 2020-2025 reiterates the agency's priorities of safety and security [23]. The strategy promotes collaboration of cybersecurity initiatives across the agency and defines five strategic cybersecurity goals. In particular, the strategy states the need to continue to advance cybersecurity in order to support new technologies. The AI Certification Framework, therefore, must consider the FAA's cybersecurity efforts and the corresponding need to ensure the secure adoption of new technologies.

FAA Order 1370.121A states that the FAA must evaluate all AI systems for various properties, including privacy and security [16]. Any personally identifiable information (PII), sensitive PII, or sensitive unclassified information transmitted or stored by AI systems must be protected in a way that complies with the overall FAA policy. In addition, all input, output, and core processing and storage components of AI systems must be adequately protected. FAA Order 1370.121A is based on NIST security and privacy controls [24]. The NIST cybersecurity concepts form the basis of information system and organizational requirements for federal systems and should be applicable for AI-based information systems as well.

As the FAA continues to advance its cybersecurity strategy, the agency also must explore potential new risks from the introduction of new technologies. For example, this may include new risks from increasingly automated systems that require less human interaction as well as risks from using data-driven learning techniques. Future ML applications such as Generative Adversarial Networks (GAN) may be researched for security assessments. The FAA should continue to collaborate with industry and other relevant entities to ensure that the agency is using current best practices to address cybersecurity risks for new technologies.

5 Research Plan Assumptions

The Research Plan is based on these assumptions:

1. The Research Plan focuses on the certification of new and emerging technologies under consideration by the FAA, and, in particular, on AI-based technologies.
2. The research will consider the certification of any type of software and service supporting ATM.
3. The research will consider the certification of software for all systems and service classifications, and the "system of systems" aspect of AI implementation, including but not limited to: human factors, system design/architecture, system integration, safety, and lifecycle management.
4. The research will assume the certification of hardware components is addressed by existing certification requirements.
5. The research will consider the certification of software under the following pathways:
    a) New FAA-led development of AI software from start to finish,
    b) Commercial off-the-shelf (COTS) AI software received in near-final form,
    c) Modified COTS AI software received and altered for use, and
    d) Previously certified AI software now used in another system or being updated in the same system.
6. The research will consider the integration of any new or modified certification processes within the context of current FAA software approval processes (e.g., V&V and T&E) and safety assurance expectations.
7. The research will maintain that all AI technologies must meet the certification requirements deemed applicable by the FAA; the certification pathway and level of rigor will differ depending on intended use, criticality, risk, and other factors.
8. The research will assume that the AI algorithm is "locked" and no longer learning prior to deployment.
9. The research will explore the requirements of data management, particularly for separation of training data from testing data and from data used for certification compliance test case demonstrations.

6 Research Plan Steps

The research will undertake a three-step approach to achieve the required outcomes and objectives.

- *Step 1: Research Certification Needs for New Technologies*
    - Conduct review of certification processes from other organizations as well as AI certification challenges and properties identified by other organizations.
    - Formulate a range of certification scenarios, pathways, and use cases applying the proposed certification framework to these use cases.
    - Assess factors contributing to the level of certification rigor (e.g., trustworthiness, risk, and suitability).
    - Identify gaps in current FAA system/software approval processes (e.g., model validation, requirements, and testing) and develop AI-specific requirements to address those gaps.
    - Develop an initial AI Certification Framework.
- *Step 2: Validate and Verify Certification Framework*
    - Review governance and standards needed from industry, international research groups, and other government agencies on system/software assurance compliance.
    - Apply the framework to AI use cases and ongoing research and development activities to identify improvements needed.
    - Update AI Certification Framework.
- *Step 3: Develop Implementation Strategy for the Certification Framework*
    - Consider strategies for the gradual adoption of the framework based on functionality and use of the AI technology.
    - Coordinate with stakeholders and engage with industry to identify amendments to current policy, regulations, and standards needed to support the new framework.

The approach above identifies the research and steps needed for the FAA to certify new technologies. There is an increasing level of interest and innovation in AI and ML applications, including those that will augment and improve current aviation services. However, while there are potential benefits of AI technologies, there are potential risks and challenges that will be evaluated to develop an AI Certification Framework. This will allow the FAA to update certification requirements that enable new use cases into the NAS using AI technologies.

Appendix A References

[1] S. Russell and P. Norvig. (2009). *Artificial Intelligence: A Modern Approach.* Pearson.

[2] N. Nilsson. (2009). *The Quest for Artificial Intelligence: A History of Ideas and Achievements.* Cambridge University Press.

[3] Andrew Ilachinski. (2017). *AI, Robots, and Swarms.* CNA, Arlington, VA.

[4] The MITRE Corporation. (2020). *A Survey of Machine Learning Suitability for ATM Applications.* McLean, VA.

[5] National Research Council. (2015). *Transformation in the Air: A Review of the FAA's Certification Research Plan*. The National Academies Press. Washington, D.C.

[6] FAA. (2017). *Airborne Software Development Assurance Using EUROCAE ED-12() and RTCA DO-178().* AC 20-115D.

[7] FAA. (2020). *Safety Risk Management Guidance for System Acquisitions.* Air Traffic Organization.

[8] Radio Technical Commission for Aeronautics. (2011). *Software Considerations in Airborne Systems and Equipment Certification.* DO-178C.

[9] Radio Technical Commission for Aeronautics. (2011). *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems.* DO-278A.

[10] FAA. (2020). *Safety Risk Management Guidance for System Acquisitions (SRMGSA).* Air Traffic Organization.

[11] International Civil Aviation Organization. (2019). *Artificial Intelligence and Digitalization in Aviation.* A40-WP/268.

[12] European Organisation for Civil Aviation Equipment. (2020). *Artificial Intelligence Considerations for Development and Certification Approval of Aeronautical Safety-Related Product: Statement of Concerns.* ER-022. Draft.

[13] European Union Aviation Safety Agency. (2021). *EASA Concept Paper: First Usable Guidance for Level 1 Machine Learning Applications.* Cologne, Germany.

[14] C. Wilkinson, J. Lynch, R. Bharadwaj, and K. Woodham. (2016). *Verification of Adaptive Systems.* DOT/FAA/TC-16/4.

[15] Dependable and Explainable Learning. (2021). *Machine Learning in Certified Systems.* DEEL Certification Workgroup. IRT Saint Exupéry. Toulouse, France.

[16] C. Michael Holloway. (2019). *Understanding the Overarching Properties*. Hampton, VA. NASA/TM-2019-220292.

[17] FAA Order 1370.121A. (2020). *FAA Information Security and Privacy Program & Policy.*

[18] Raj Pai and Parimal Kopardekar. “Investigating Feasibility and Application of Certification of Artificial Intelligence/Machine Learning Applications in ATM Systems.” NASA.

[19] European Union Aviation Safety Agency. (2020). *Artificial Intelligence Roadmap: A Human-Centric Approach to AI in Aviation.* Cologne, Germany.

[20] Department of Defense Directive 3000.09. (2017). *Autonomy in Weapons Systems.*

[21] Food and Drug Administration. (2019). *Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD).*

[22] National Institute of Standards and Technology. (2019). *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools.* U.S. Department of Commerce. Washington, D.C.

[23] FAA. (2019). *Cybersecurity Strategy 2020-2025.*

[24] National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations.* SP 800-53 Rev. 5.

Appendix B Acronyms

AI	Artificial Intelligence
AR	Augmented Reality
AMS	Acquisition Management System
ATM	Air Traffic Management
COTS	Commercial Off-The-Shelf
CNS	Communications Navigation Surveillance
DEEL	Dependable and Explainable Learning
DL	Deep Learning
DOD	Department of Defense
EASA	European Union Aviation Safety Agency
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FDA	Food and Drug Administration
GAN	Generative Adversarial Network
IAM	Identity and Access Management
IATF	International Aviation Trust Framework
ICAO	International Civil Aviation Organization
ML	Machine Learning
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SPII	Sensitive Personally Identifiable Information
SRM	Safety Risk Management
SUI	Sensitive Unclassified Information
T&E	Test and Evaluation
UAS	Unmanned Aircraft Systems
V&V	Validation and Verification Process
VR	Virtual Reality