How AI Impacts the Digital Products and Services Performance in a Critical Context?

Benoit Huyot
cortAIx Factory SAS, France
benoit.huyot@thalesgroup.com

Juliette Mattioli
Thales SA, cortAIx, France
juliette.mattioli@thalesgroup.com

Xavier Bec
Thales Global Services SAS, France
xavier.bec@thalesgroup.com

***Abstract*—The Deliver Digital Products and Services (DDPS) framework is conceived to streamline the development and operation of digital-first solutions by reducing organizational silos and enhancing collaboration between operations engineering and product management. It integrates agile, DevOps, and "Shift Left" principles and is structured around five continuous, iterative activities: Explore & Plan; Build & Deliver; Release & Deploy; Operate & Support; and Performance Assessment & Learning. In light of the large-scale deployment of artificial intelligence (AI) in digital products and services, as well as the emergence of new AI-specific regulatory frameworks, the DDPS process requires adaptation. In particular, the EU AI Act introduces the notion of "intended purpose" as a central criterion for AI governance, tightly coupling liability and compliance obligations to the operational context of use. The development of trustworthy AI thus necessitates a holistic, lifecycle-oriented approach that integrates legal, ethical, and technical considerations across design, deployment, and operational phases.**

Keywords- Digital Products; Deliver Digital Products and Services (DDPS); DDPS Process; Trustworthiness Assessment.

I. INTRODUCTION

The "**Deliver Digital Products and Services**" (DDPS) process focuses on creating, distributing, and managing digital solutions, often AI-based, delivered mainly via online or networked environments rather than physical formats. These offerings include software, mobile apps, cloud platforms, streaming services, and digital marketplaces, designed to meet specific user needs in a fully dematerialized way. Unlike physical products that require production, shipping, or installation, digital products and services are delivered instantly and accessed anywhere with an internet connection, providing high convenience and flexibility.

Digital products and services typically run on public, private, or hybrid clouds, enabling automated distribution without local installation or hardware changes. Providers handle updates and scalability, matching capacity to demand and maintaining performance without physical reconfiguration. Automated deployment enables continuous, largely transparent roll-out of new features, security patches, and performance improvements with minimal disruption. These solutions are mainly operated and supported remotely using advanced monitoring, maintenance, and customer support tools [1]. Real-time tracking of performance, security, and system health enables proactive issue resolution. Support is provided via online channels such as chat-bots, help centers, and ticketing systems, delivering fast, efficient, contactless assistance while reducing costs and enabling scalable, round-the-clock support across regions.

The DDPS process applies only to these digital-first solutions, not to traditional or hybrid offerings that still rely on physical components or manual interventions. The framework is built to maximize efficiency, scalability, and user-centricity in a rapidly evolving digital landscape.

Trustworthy AI relies on legal, ethical, and technical foundations, reflected in requirements such as robustness, effectiveness, reliability, usability, human agency, and oversight [2]. It spans the entire AI lifecycle, from design and engineering to deployment and operation [3], and covers both technical systems and the actors and processes around them. This holistic view treats trust not only as a property of a digital product or service, but also as the result of relationships among stakeholders such as AI engineers, scientists, domain experts, and leaders. It focuses on understanding each stakeholder's perspective and maintaining trust as objectives, environments, and conditions change. The aim is to provide a practical framework for stakeholders to systematically assess and ensure the trustworthiness of AI-based DDPS.

After introducing in section III-A the DDPS activities [4], we will examine the integration of AI into digital products and services in the core of section III. It aims to support a robust design and delivery process that reliably generates effective solutions by rigorously meeting user and business needs, while ensuring compliance with applicable standards and regulations underlined in section II. This work builds on the results of the French initiative "Confiance.ai" which introduced a structured framework to assess the reliability of AI-based systems presented in section IV, especially those using machine learning, while simultaneously reducing the costs associated with over exploitation, engineering, and operational inefficiencies.

II. AI REGULATORY AND NORMATIVE LANDSCAPE

We first outline the AI regulatory and normative landscape we must follow. The EU AI Act defines a framework for high-risk AI systems to ensure safety, reliability, and ethical soundness [2]. High-risk domains include critical infrastructure, transportation (including aeronautics), medical devices, and essential public services. "High-risk" status follows a systematic assessment of a system's potential to harm human welfare or undermine fundamental societal values. A key feature is the presumption of conformity through harmonized standards, fostering trust, transparency, and accountability among AI developers, providers, and users [5]. Figure 1 presents the broad spectrum of standards for AI data, performance, and governance that underpin trustworthy and responsible AI.

Specific safeguards, including cybersecurity and functional safety measures, are central to regulations for high-risk AI sys-

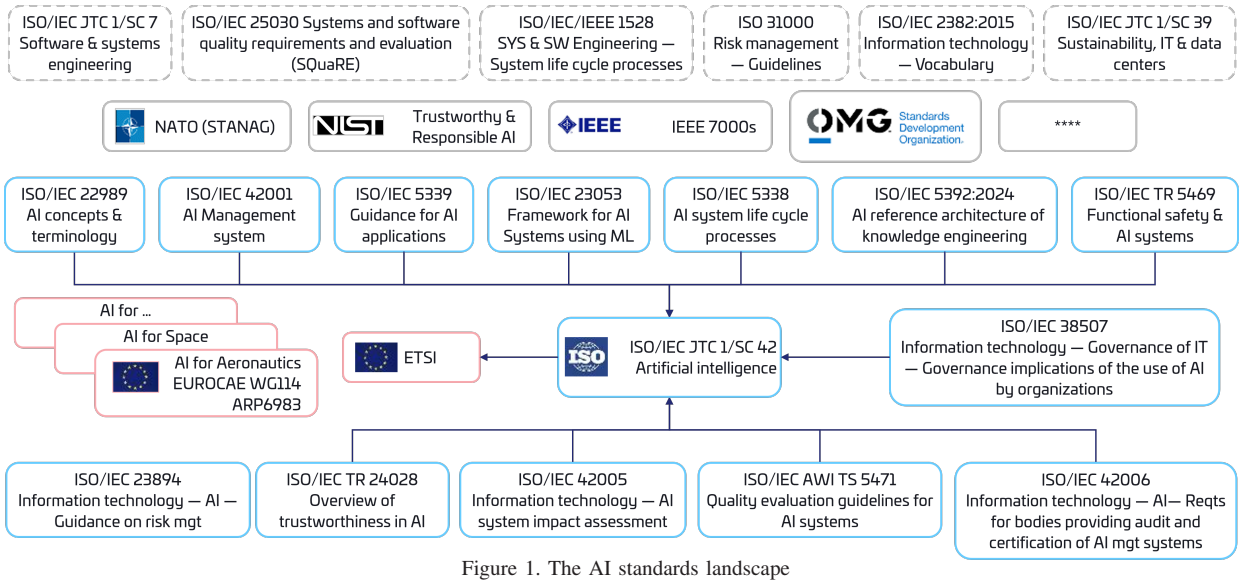

Figure 1. The AI standards landscape

tems. They go beyond conventional IT security by addressing AI-specific vulnerabilities through systematic risk assessments that identify and mitigate threats such as adversarial attacks, data poisoning or manipulation, and model drift. Unlike traditional digital services, AI-driven DDPS often exhibit emergent behaviors that cannot be fully predicted at the design stage. This unpredictability requires a fundamental rethink of the end-to-end design, development, and delivery of digital products and services to properly integrate AI components. The implications of this reconfiguration are examined in the next section.

III. Deliver Digital Products and Services Process

The engineering DDPS process (see figure 2) is conceptualized as a comprehensive end-to-end lifecycle framework that systematically enhances the cross-functional collaboration necessary to securely and efficiently design, develop, deploy, and operate digital products and services [6]. Its principal objective is to mitigate organizational and functional silos and to decrease both the frequency and complexity of handovers between operations engineering and product management.

A. Usual DDPS Workflow

The DDPS process embraces the concepts and culture of agility, DevOps and Shift left [4]. It is inspired by already existing concepts, Agile at scale frameworks, studies such as Team Topologies and Accelerate. It is founded on a "Continuous Everything" paradigm, within which five activities are executed on an ongoing, uninterrupted basis.

- "**Explore and Plan**": The objective is to continuously explore markets and customer needs, while also managing roadmap, capacity, budget, and organization.
- "**Build and Deliver**": Based on the roadmap, objective is to continuously take features and enablers from the Program Backlog and implement them in a continuous delivery process.
- "**Release and Deploy**": In alignment with the "Release on Demand" paradigm, the objective is to manage candidate releases throughout the entire delivery pipeline, culminating in their deployment into the production environment.
- "**Operate and Support**": The objective is to ensure continuous, uninterruptible service delivery and comprehensive technical support for end users.
- "**Measure and Learn**": Based on a data-driven culture, objective is to establish a framework for the implementation of continuous improvement, as well as ongoing learning and experimentation, both with regard to the quality of the products and services delivered and the optimization of the efficiency of operational activities.

Based on work on the life cycle of an AI based system [7] [8] and the workflow described above, we refined the overall DDPS process to integrate the induced issues of embedding AI [9].

B. Explore and Plan of an AI-based DDPS

The adoption of the EU Artificial Intelligence Act represents a significant milestone in the governance of AI, as it establishes the "**intended purpose**" as a foundational legal and conceptual criterion for delineating the scope, accountability structures, and regulatory compliance obligations applicable to AI systems. This notion encompasses the specific objectives of AI solution (AI-systems as well as AI-based digital products and services) deployment, the functional characteristics of these systems, and the technical and socio-organizational contexts in which they are conceived, designed, developed, and operated. By systematically linking liability regimes and compliance duties to the intended purpose, the AI Act constructs a comprehensive and robust regulatory framework that governs AI solution through a differentiated, risk-based approach. The primary objective of the "explore and plan" stage is to delineate the operational domain within which the AI-based digital product or service is required to function and to ensure that it

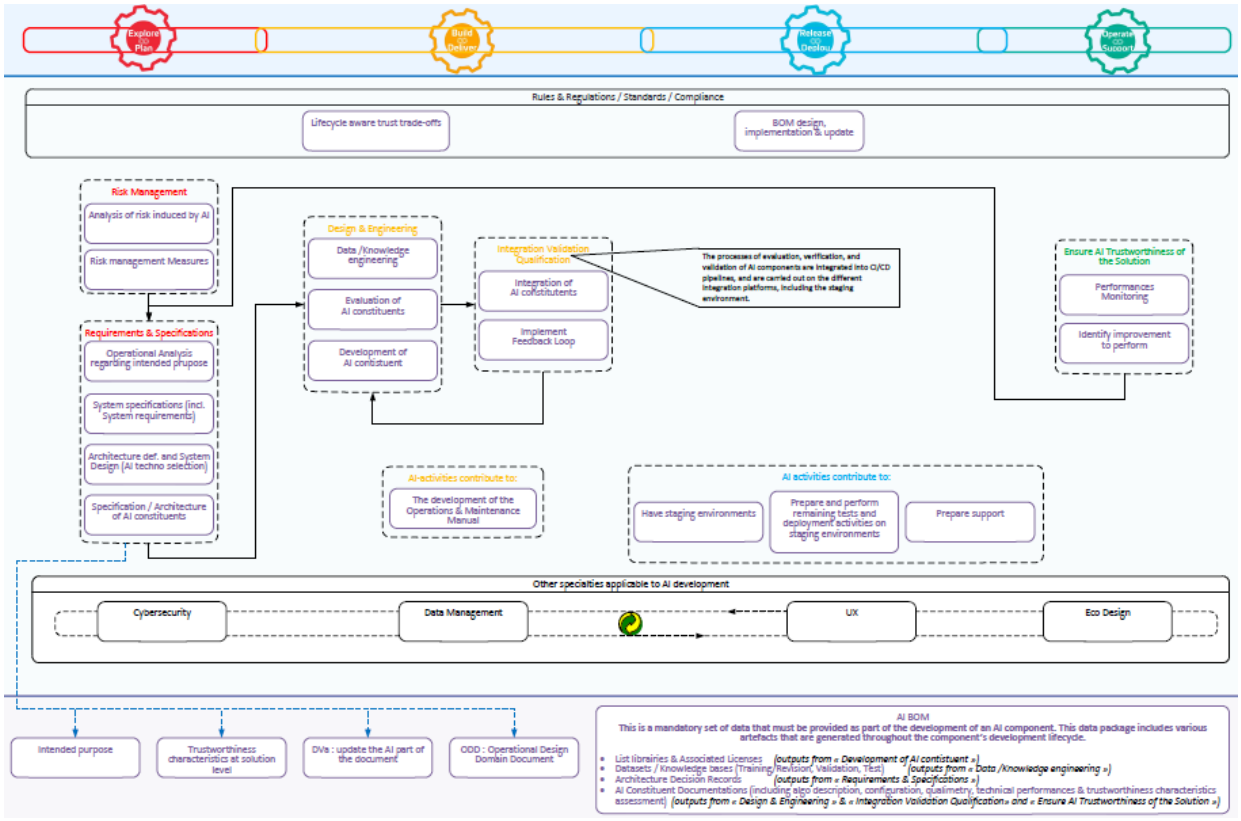

Figure 2. The AI-based Digital Products and Services Delivery Process

continues to operate as intended over time under all reasonably foreseeable operating conditions. This includes the systematic consideration of edge and corner cases, as well as potential failure scenarios, in order to mitigate unintended consequences that could endanger human life or compromise mission-critical functions.

Accordingly, the Intended Purpose Summary shall be articulated in a concise, clearly delineated statement specifying the system's functional capabilities, the entities or data upon which it operates, the intended user groups, and the operational context in which it is expected to be deployed. The Operational Design Document (ODD) [10] provides a formal description of the operational environment and the associated operating conditions. The development and analysis of the ODD have been initiated based on the preliminary formulation of the Intended Purpose. Thus, the "Risk Management" activity and the "Requirements and Specification" activity, which includes the ODD description, constitute the principal components of the "Explore and Plan" phase.

C. Build and Deliver of an AI-based DDPS

The aim of build and deliver is to produce AI constituents and integrate them into an operational version of the system. It includes design, documentation, implementation as well as integration and testing it results on a potentially releasable version of the system [11].

Once the risk analysis, the ODD, the functional architecture of the digital solution, and the associated technological choices have been finalized, the subsequent step consists in specifying each individual constituent. Multiple implementation streams, each dedicated to a specific constituent, may proceed in parallel, encompassing specification, development and implementation, unit-level evaluation, and delivery for integration. In addition, the design phase aims to examine the available data required to train the model and to define the functional and non-functional requirements of the AI constituent. These requirements should guide the design of the architecture of the AI-based digital product or service, the definition of the model-serving strategy, and the construction of a comprehensive test suite for the future AI constituent.

The subsequent phase, entitled "Integration, Validation, and Qualification," is dedicated to assessing the suitability of artificial intelligence (AI) techniques for the problem at hand through the implementation of a proof-of-concept for the AI component. In this phase, we iteratively execute several activities, including the identification and refinement of an appropriate AI algorithm for the target problem, as well as data engineering, knowledge engineering, and algorithm engineering. The principal objective of this phase is to produce a robust and reliable AI component that is ready for deployment [12].

D. Release and Deploy of an AI-based DDPS

The primary objective of this phase is to implement the solution incorporating one or more AI components by applying established DevOps practices, including systematic testing,

management and deployment of release candidates, continuous delivery, and operational monitoring.

Even when the majority of verification and validation activities are shifted left and executed on a continuous basis, certain activities must still be conducted immediately prior to release and deployment into the production environment. This phase includes the preparation and execution of the remaining tasks, such as operational readiness activities, deployment of the release to a staging environment, and subsequent validation and testing on that platform. Only upon successful completion of these activities is the release authorized for deployment into the production environment.

Certain AI constituent, particularly those grounded in data-driven approaches such as machine learning (ML), necessitate continuous operational monitoring to identify deviations during runtime. Consequently, the use of dedicated monitoring and management tools is mandatory [13]. The inherently static nature of trained ML models can lead to suboptimal performance in dynamically evolving environments. As a result, ML models must be capable of adapting to changes, including component wear and aging, as well as emerging data biases, in order to mitigate obsolescence caused by concept drift. Nonetheless, the specification of appropriate performance metrics for deployment monitoring is inherently problem-dependent. The recent proliferation and deployment of large language models (LLMs) further accentuate and amplify these challenges.

E. Operate and Support of an AI-based DDPS

The integration of AI components into products necessitates dedicated activities to systematically evaluate AI trustworthiness, with particular emphasis on the “Operate and Support” phase of the lifecycle. This phase encompasses all operational dimensions, focusing on day-to-day execution and customer service delivery, while ensuring that AI-enabled digital products and services consistently remain trustworthy.

To this end, a structured, formalized, and reproducible assessment framework is employed to evaluate key trustworthiness attributes, including effectiveness, reliability, security, validity, explainability, and accountability. The use of such a framework supports the continuous improvement of system quality and contributes to an enhanced overall customer experience [14].

As with cybersecurity, where an “Ensure Cybersecurity of the Solution” activity is embedded in operations, AI trustworthiness is maintained through a dedicated “Ensure AI Trustworthiness of the Solution” sub-activity [15]. During operations, this sub-activity continuously monitors and assesses AI performance, reliability, security, and validity so the solution keeps meeting its objectives. Monitoring mechanisms enable early detection and anticipation of issues such as model drift, helping to avoid or reduce service disruptions [13]. Explainability and traceability mechanisms further support efficient maintenance. When deviations, deficiencies, or non-compliance with trustworthiness requirements are found, corrective actions—such as model retraining, updates, or technical/procedural fixes—are initiated and tracked via the backlog to maintain alignment with defined trustworthiness criteria.

IV. Trustworthiness Performance Assessment

Assessing trustworthiness in AI-based products and services is a multifaceted challenge that goes beyond traditional metrics such as model accuracy or computational efficiency, requiring a holistic, systemic approach to ensure reliability, safety, and alignment with human and societal values [16]. Trustworthiness is a dynamic attribute that must be continuously monitored, validated, and adapted throughout the entire lifecycle of an AI-based digital product or service. This complexity stems from AI’s inherent uncertainty, stochastic behavior, and emergent risks, which differ from traditional software systems. Therefore, trustworthiness assessment must consider interactions between technical components, human oversight, and operational environments, all of which shape overall performance and dependability. This engineering activity, grounded in a data-driven culture, supports continuous improvement—a core value of the DDPS process—and is transversal to the four previous activities. Its main purpose is to continuously identify, track, and implement improvement actions by defining and reviewing KPIs relevant to the digital program. This step corresponds to the "Measure and Learn" activity in the DDPS process.

Assessing trustworthy performance requires shifting from a model-centric view to a Product- or Services-level one. Traditional AI evaluation focuses on model metrics like accuracy, precision, or recall on curated datasets, but this is inadequate for high-stakes applications. What matters is the real-world behavior of the digital product or service, not the model alone. This demands integration testing to track how uncertainties propagate through the solution, how human–machine interfaces support effective oversight, and how deterministic cybersecurity protocols can override AI outputs when they breach laws or ethical constraints.

Another key part of assessing trustworthiness is evaluating performance metrics, which must align with the real-time demands of high-risk applications [17]. Computational efficiency, particularly latency, where delays in processing could lead to failures. The worst-case execution time must be rigorously guaranteed to ensure that the system responds within safe operational windows.

A key challenge in assessing reliability is ensuring that training and validation datasets or knowledge bases are representative, since AI products are only as reliable as the data or knowledge used to design them. A model may perform well in the lab or on specific datasets but fail in real-world deployment, where variability, edge cases and environmental noise differ from the original data. This divergence occurs when the operational design domain (ODD)—the range of conditions in which the system is expected to operate—is not adequately reflected in the design data or knowledge. Reliability assessment must therefore rigorously validate information quality (data and knowledge) against real-world distributions [18] and test the digital solution’s ability to remain stable and predictable within its ODD.

TABLE I. MAIN KEY PROFILES

Role	Responsibilities	Key Skills
AI Engineers	Design, train, and optimize AI models. Implement robustness enhancements (*e.g.,* cyber attack or misuse).	MLOps/AIOps, Computer Science, Algorithm engineering
Data Analyst	Curate and preprocess datasets. Ensure data quality and representativeness.	Data Cleaning, Feature Engineering, Bias Detection.
AI Scientists	Develop and validate new AI constituents taking into account trustworthiness characteristics such as transparency and/or explainability.	Data-driven AI, Knowledge-based AI, Hybrid AI, Explainable AI (XAI), Visualization Tools
Domain Experts	Support Operational analysis regarding the intended purpose. Contribute to the Operational design domain definition	Domain Knowledge (*e.g.,* Defense, Aerospace, Cyber & Digital).
AI Leader	Ensure the AI system aligns with regulatory and ethical standards. Conduct bias audits and fairness assessments.	Recognized AI expert, AI discipline, master the regulatory framework, standards & Digital Ethics Charter
End Users	Provide real-world feedback on solution performance and usability through the feedback loop instanciated in the solution.	Domain-Specific Knowledge, User Experience (UX) Feedback.
AI Security Experts	Assess vulnerabilities specific for AI (*e.g.,* model inversion attacks, data poisoning). Implement defensive mechanisms (*e.g.,* differential privacy).	AI cyber security, Prompt Injection, Watermarking, etc.
Human Factors Engineers	Design user interfaces that present AI decisions clearly and intuitively. Ensure human oversight is effective.	UX/UI Design, Human-Computer Interaction (HCI), Cognitive Engineering.

AI products' stochastic variations in outputs, even when identical, complicate trustworthiness evaluations as they exhibit a non-deterministic nature. This makes regression, testing, certification, and auditing challenging due to the need for consistency to demonstrate compliance with safety standards. Ensuring repeatability is essential for safety-critical applications, where variations could lead to harmful consequences. Reproducibility is crucial for maintainability, certification, and auditability, mandatory in regulated industries like healthcare and aviation.

AI-based solutions are more complex because their dependability must hold not only technically but also under unforeseen failures and changing environments. Unlike traditional software, whose dependability can often be guaranteed, AI products and services rely on statistical performance trade-offs and require a risk-based approach to maintain safety and cybersecurity. Availability must be backed by fallback mechanisms that trigger when the AI encounters out-of-distribution inputs or low-confidence cases. Reliability covers not just uptime but stable performance over time, especially under concept drift. Safety and security require verifying that the system avoids catastrophic risks. Maintainability is critical due to AI's data-driven nature, demanding continuous retraining and adaptation to stay effective.

The usability of AI systems now includes multiple dimensions beyond traditional user-friendliness. Transparency, adaptability and alignment with human cognitive and ethical expectations are now key factors in trustworthiness assessments. Even if a system is technically proficient, it may still fail if its decision-making processes are opaque or does not offer explanations for its actions. Human-in-the-loop is a critical component of trustworthiness in areas such as healthcare diagnostics, autonomous vehicles and cybersecurity.

The governance and ethical dimensions of trustworthiness assessment emphasize the need for accountability, fairness and compliance. AI systems must be designed and deployed in a manner that respects fundamental rights, avoids discriminatory biases and ensures transparency. Standards such as ISO/IEC 42001 provide a structural framework for implementing governance mechanisms. Continuous monitoring facilitated by MLOps and AIOps frameworks is essential to detect performance degradation, data drift or ethical deviations over time; wher MLOps (resp. AIOps) focuses on the operationalization of ML (resp. AI) models, ensuring that they are deployed efficiently and maintained effectively in production environments. In contrast, ML/AI Engineering is primarily concerned with the development and the maintenance of an AI-based solution.

This lifecycle governance ensures that AI solutions remain aligned with their original design specifications and adapt to evolving realities without compromising robustness, explainability, reliability or fairness. Finally, the link between technical performance and human factors is key to trustworthiness assessment.

V. CONCLUSION

Integrating AI into digital products and services introduces technical and non-technical challenges. Major efforts aim to resolve these and enable early, cost-effective, and safe industrial AI deployment. The main challenges are: (i) trustworthiness—the product's ability to reliably deliver the expected service; and (ii) industrial efficiency—achieving this trustworthiness within acceptable cost and resource limits. Addressing these requires revising engineering practices to account for AI-specific characteristics and requirements. In this context, the paper re-examines the DDPS process with AI components integrated throughout its lifecycle.

But AI is not limited to the domain of computer science; it is also enabling the emergence and transformation of professional

roles across multiple sectors [9]. Some of the principal positions that are being newly created, especially in Thales's professional families or substantially redefined through the adoption of AI include data and AI scientists, AI engineers, AI security specialists, etc. (see Table. I).

For example, data and AI scientists are primarily concerned with the development and formalization of AI components, whereas AI engineers focus on the full spectrum of activities required to operationalize these components and deploy them in practical settings. It is often advantageous for these roles to be treated as distinct specializations, functioning collaboratively within a team, with clearly differentiated and complementary skill sets applied accordingly. Key profiles such as AI engineers, domain specialists, legal and compliance experts, and human–machine interaction designers—must jointly assess risks, transparency needs, and mechanisms for effective human oversight. Under the fully applicable EU AI Act [2], high-risk AI systems must offer full traceability to support accountability and regulatory supervision. This goes beyond traditional documentation, requiring continuous, tamper-proof audit trails across the AI lifecycle.

Our approach has been tested on a concrete use case: digital NOTAM [19]. A NOTAM (Notice to Airmen) is a standardized system providing pilots with time-critical information on airports, airspace, navigation aids, and other facilities affecting flight safety and operations. Conventional NOTAMs use a telegraphic, highly abbreviated format that is often ambiguous but still interpretable by humans. Digital NOTAMs, by contrast, must formalize aeronautical information for unambiguous machine processing while preserving all operationally significant nuances. Developing a trustworthy digital NOTAM therefore requires a rigorous process to ensure operational efficiency by reducing processing time, resource use, and reliance on manual interpretation; and safety and accuracy [20], by reducing ambiguity and misinterpretation and improving the reliability of flight operations data. Because Thales operates in aerospace, digital identity, defense, and security, this creates requirements for governance, operational controls, and technology infrastructure, and thus for new engineering artefacts such as the mandated AI Bill of Materials (AI-BOM), which provides traceability and detailed documentation of libraries, datasets, architectural decisions, and AI component specifications. This DDPS process is already used at Thales in various operational and research contexts and is integrated into engineering workflows to systematically reinforce AI governance.

REFERENCES

[1] K. Hui and P. Chau, "Classifying digital products", *Communications of the ACM*, vol. 45, no. 6, pp. 73–79, 2002.

[2] L. Floridi, "The European legislation on AI: a brief analysis of its philosophical approach", *Philosophy & Technology*, vol. 34, no. 2, pp. 215–222, 2021.

[3] L. Giraldo et al., "White Paper Trustworthiness For AI in Defence: Developing Responsible, Ethical, and Trustworthy AI Systems for European Defence", European Defence Agency (EDA), Tech. Rep., 2025.

[4] P. Müller, *Integrated engineering of products and services*. Fraunhofer Verlag, 2014.

[5] H. Sohier et al., "The Engineering of AI Evaluation and Scoring: Overview and Insights", in *2025 IEEE International Systems Conference (SysCon)*, IEEE, 2025, pp. 1–8.

[6] J. De Sordi et al., "Development of Digital Products and Services: Proposal of a Framework to Analyze Versioning Actions", *European Management Journal*, vol. 34, no. 5, pp. 564–578, 2016.

[7] K. Quintero et al., "An end-to-end method for operationalizing trustwothiness in AI-based critical systems", in *15th Int. Conf. on Performance, Safety and Robustness in Complex Systems and Applications*, 2025.

[8] L. Mattioli et al., "Evaluation of Robustness, Reliability, and Safety of an Artificial Intelligence Based System", in *16th Int. Conf. on Performance, Safety and Robustness in Complex Systems and Applications*, 2026.

[9] L. Korada, "AIOps and MLOps: Redefining Software Engineering Lifecycles and Professional Skills for the Modern Era", *Journal of Engineering and Applied Sciences Technology. SRC/JEAST-388. DOI: doi. org/10.47363/JEAST/2023 (5)*, vol. 271, pp. 2–7, 2023.

[10] T. Myklebust et al., "Definition of the system, operational design domain, and concept of operation", in *The AI Act and The Agile Safety Plan*, Springer, 2025, pp. 19–27.

[11] M. Adedjouma et al., "Engineering Dependable AI Systems", in *2022 17th Annual System of Systems Engineering Conference (SOSE)*, IEEE, 2022, pp. 458–463.

[12] J. Mattioli et al., "AI Engineering to Deploy Reliable AI in Industry", in *2023 Fifth International Conference on Transdisciplinary AI (TransAI)*, IEEE, 2023, pp. 228–231.

[13] F. Kaakai and P. Raffi, "Towards Multi-Timescale Online Monitoring of AI Models: Principles and Preliminary Results", in *SafeAI, AAAI's Workshop on Artificial Intelligence Safety*, vol. 3381, 2023.

[14] E. Popkova, "Quality of Digital Product: Theory and Practice", *International Journal for Quality Research*, vol. 14, no. 1, p. 201, 2020.

[15] A. Awadid et al., "Towards engineering processes to guide the development of trustworthy ml systems", in *2024 IEEE International Symposium on Systems Engineering (ISSE)*, IEEE, 2024, pp. 1–6.

[16] A. Awadid et al., "AI Systems Trustworthiness Assessment: State of the Art", in *Workshop on Model-based System Engineering and AI, 12th International Conference on Model-Based Software and Systems Engineering (Modelsward)*, 2024.

[17] J. Mattioli et al., "Towards a holistic Approach for AI Trustworthiness Assessment based upon Aids for Multi-Criteria Aggregation", in *SafeAI - The AAAI's Workshop on Artificial Intelligence Safety*, vol. 3381, 2023.

[18] J. Mattioli et al., "Information Quality: the Cornerstone for AI-based Industry 4.0", *Procedia Computer Science*, vol. 201, 2022.

[19] J. Mattioli et al., "A Brief Overview of Key Quality Metrics for Knowledge Graph Solution Illustration on Digital NOTAMs", in *Proceedings of the AAAI Symposium Series*, vol. 7, 2025, pp. 206–213.

[20] A. Awadid et al., "Reframing the System Engineering Lifecycle for AI Systems: An Intended Purpose-Driven Approach", in *9th International Conference on Software and System Engineering (ICoSSE 2026)]*, 2026.