A Process Assessment Model for AI-enabled Medical Device Software

Gilbert Regan [0000-0002-5023-6914], Buddhika Gayashani Jayaneththi [0009-0008-7813-3942]

Fergal Mc Caffery [0000-0002-0839-8362]

Regulated Software Research Centre, Dundalk Institute of Technology, Dundalk, Ireland
gilbert.regan@dkit.ie

Abstract. AI-enabled medical device software can enhance diagnostics, treatment planning, patient monitoring, and workflow automation. However, these benefits will only be fully realised if relevant stakeholders can trust, and thus adopt this software. Each stakeholder group faces unique trust challenges, for example clinicians can have a lack of trust in AI decisions and particularly in black box AI models, leading to fear of liability and damage to reputation. Similarly, patients have concerns about their safety in addition to concerns about data security and privacy of their sensitive health data. To address this issue, we have developed a process reference model and a process assessment model for AI-enabled medical device software, the purpose of which is to assist organisations to develop trustworthy and regulatory compliant AI-enabled medical device software. These models help ensure compliance with industry standards and best practices and improve process maturity by identifying gaps and areas for improvement. In this paper we present an overview of the software level processes contained within a new process reference/assessment model for AI-enabled medical device software. This new process reference/assessment model contains amendments to 8 existing traditional software development and support processes, and the addition of 3 new processes.

Keywords: Trustworthy AI, AI-enabled medical device software, medical device software, process reference model, process assessment model, artificial intelligence, process assessment, software process improvement, artificial intelligence

1 Introduction

AI-enabled devices are devices that include one or more AI-enabled device software functions (AI-DSF). An AI-DSF is a device software function that implements one or more AI models to achieve its intended purpose [1]. Within the healthcare domain, artificial intelligence (AI) is being used for various purposes such as detection of disease, management of chronic conditions, delivery of health services, and drug discovery [2]. Examples of AI use in healthcare include: AI system used for making a diagnosis of the cardiac diseases with the help of cardiac images [3]; movement-detecting device for predicting early stroke [4].

For AI-enabled Medical Device Software (AIeMDS) to be adopted by relevant stakeholders, and for society to reap all its potential benefits, the AIeMDS must be trustworthy. Trustworthiness is the demonstrable likelihood that the system performs according to designed behavior under any set of conditions as evidenced by characteristics including, but not limited to, safety, security, privacy, reliability and resilience [5]. Some examples of stakeholders concerns about adopting AI that is not trustworthy include: clinicians concerns about reputational and legal risk; patients concerns about inaccurate/harmful outcomes, unfair/discriminatory treatment, personal data capture and loss of privacy; regulators and society as a whole concerns about certification, inappropriate use of citizen data, cascading AI failures, reduced human connection, and the scaled use of inaccurate, biased or privacy invading AI technologies on citizens which can entrench bias, inequality and undermine human rights, such as the right to privacy [6].

There are a number of high-profile frameworks for trustworthy AI led by or affilliated with government actors. These include: (i) the European Unions(EU) Ethics Guidelines for Trustworthy AI [7], which identifies and describes the ethical principles required for ethical and robust AI, translates these ethical principles into seven requirements for an AI system to meet throughout the lifecycle, and offers an assessment list to operationalize the requirements; (ii) The European Union Artificial Intelligence Act (EU AI Act) [8] which establishes mandatory requirements for trustworthy AI, including requirements for high risk systems such as data governance, documentation and record keeping, transparency and provision of information to users, human oversight, robustness, accuracy, and security; (iii) The National Institute of Standards and Technology AI Risk Management Framework (NIST) [9] which was mandated by the United States Congress to develop an AI Risk Management Framework (AI RMF) to offer guidance for the development and use of trustworthy AI.

Another method for assuring AIeMDS quality and trustworthiness is through assuring the quality and trustworthiness of the software development process used to develop the software. This assurance can be provided through assessing the development process for its adherence to relevant medical device regulations, standards and guidance documents, and through software development best practices. A framework entitled MDevSPICE® (see section 2), was developed by the Regulated Software Research Centre at Dundalk Institute of Technology for the purpose of conducting assessments on medical device software development processes. Section 3 provides the methodology for developing a new AIeMDS assessment framework which we entitle AI-MDevSPICE. Section 4 provides a brief overview of the additional processes, and amendments made to existing MDevSPICE® processes, resulting in a new AIeMDS assessment framework.

2 Related Work

MDevSPICE® is a framework primarily aimed at assessing a medical device software organisations software development process and thus identify any gaps or weaknesses in the organisations' software development processes. The assessment is an assessment

of how the development process adheres to regulatory requirements, including medical device standards and guidelines and the software development best practices that a software development organisation in the medical device domain has to adhere to. These weaknesses or gaps then provide a roadmap for how the organisation can improve their development processes. The mantra being that a higher quality software development process should lead to higher quality software. The methodology for the development of the MDevSPICE® framework have been published here [10].

The MDevSPICE® process assessment framework contains a process reference model (PRM), a process assessment model (PAM) which is similar to ISO/IEC 15504–5 (SPICE) [11], and an assessment method. A PRM describes a set of processes necessary for developing, managing, or improving software and system engineering activities. Each process is defined in terms of purpose and outcomes rather than specific methods. The outcomes describe the expected results when a process is performed successfully. The MDevSPICE® PRM, published as IEC/TR 80002-3:2014 [12], consists of system lifecycle processes, software lifecycle processes and supporting processes. A PAM is an extension of the PRM and includes process performance indicators such as base practices and work products. Base practices (BPs) are the fundamental activities that must be performed to achieve the intended outcomes of a process, while Work Products (WPs) are artifacts that provide evidence of process execution.

The PRM was developed in line with ISO/IEC 24774 [13] which provides requirements and recommendations for the description of processes. The resultant PRM is an integration of requirements from ISO 12207:2008 [14] which is the generic software lifecycle process standard, IEC 62304 [15] which is the medical device software lifecycle process standard, ISO 13485 [16] which is the quality management system standard, and ISO 14971[17] which is the standard for risk management in medical devices.

The PAM base practices were derived from process implementation steps in IEC 62304, ISO/IEC 15504-5 and IEC 80002-1[18]. IEC 80002-1 provides guidance on the application of ISO 14971 to medical device software. Additional base practice information was then derived from the FDA guidance documents on premarket submission [19], software validation [20] and off-the-shelf [21] software.

The benefits of MDevSPICE® can be summarized as follows:

- It provides a structured framework for software process improvement.
- It is aligned with IEC 62304 and other key regulatory standards.
- It provides a capability maturity model (like SPICE/ISO 15504) to assess software process effectiveness.
- It reduces regulatory burden by demonstrating a mature development process.

3 AI-MDevSPICE Development Approach

As MDevSPICE® is a framework primarily aimed at assessing a medical device software organisations software development process, it was decided that the optium approach to developing AI-MDevSPICE was to amend MDevSPICE® to include MDS that contained AI functionality. This approach entailed the adoption of the following 4 step process:

Step 1. Update MDevSPICE®. Some of the standards that MDevSPICE® were based on have been revised/withdrawn, therefore MDevSPICE® needed updating. For instance, ISO 15504-5:2012 [11] was withdrawn and replaced by ISO 33061:2021 [22]. ISO 33061 combines some of the 15504-5 processes, for example, ISO 15504-5 has *System* Architecture Design and *Software* Architecture Design Processes whereas ISO 33061 has one 'Architecture definition process. Therefore, outcomes and base practices are very different between ISO 15504-5 and ISO 33061. MDevSPICE® system level processes were based on 15504-5, so all system level processes need to be rewritten to conform with ISO 33061. Similarly, some of the MDevSPICE software lifecycle processes have outcomes/base practices from ISO 15504-5 so these needed amended, for example, 5 of the 9 Change request management process outcomes were taken from 15504-5.

Step 2. Identify AI related standards/guides/regulations that could possibly provide input to AI-MDevSPICE. Initially, the British Standards Online database was searched using the search strings 'AI' and 'Artificial Intelligence'. This initial search was conducted during second week of April 2024 and returned a total of 79 standards. A scan of these standards, through reading title/introduction/scope, to determine if they were related to AI system/software development process, eliminated 65 standards. This search was repeated monthly throughout year 2024 and a further 5 possibly relevant standards were identified, resulting in a total of 19 standards. A search of the FDA website using search term AI and category 'medical device' revealed a number of guidance documents [23-27] that could provide input to AI-MDevSPICE, while regulations to consider were the EU AI Act [8] and the General Data Protection Regulations (GDPR) [28]. Snowballing lead to the identification of more documents to consider [29,30,31,32]

Step 3. Identify any new AI-specific processes. One particular standard, ISO 5338 [33] identified in step 2, provided AI system lifecycle processes. This standard provided 3 processes which were specific to AI development, that is Knowledge acquisition, Data engineering, and Continuous validation. This standard provided process description, outcomes and activities (base practices) for each process. These 3 processes were added to the MDevSPICE® architecture to complete the AI-MDevSPICE architecture for Software lifecycle and Support processes (see Table 1, Section 4).

Step 4. Identify any amendments to existing MDevSPICE® processes. This step involved analyses of standards/regulations/guides identified in step 2. The purpose of the analysis was to elicit requirements from the documents that could impact the existing MDevSPICE® processes in terms of Outcomes, Base Practices, Notes, or Work Products. Techniques used to complete the analysis were memoing and constant comparison. These techniques are often used in Grounded Theory. The analysis elicited requirements (some of which were repetitive across documents) from the following documents: ISO 23894 [34], IEC 63450 [35], ISO 5338 [33], and documents mentioned previously [8, 23-25, 28-32].

4 Overview of AI-MDevSPICE

Table 1 provides 11 AI-MDevSPICE software lifecycle processes and 6 AI-MDevSPICE support processes. These Support processes help ensure the smooth execution, maintenance, and enhancement of software projects.
The column after each process indicates whether, as a result of the introduction of AI functionality, the process is a new process (N) to the traditional medical device software lifecycle processes, or whether the process has been amended (A). An 'X' indicates no change to the process. Table 1 indicates that there are 2 new medical device software lifecycle processes (Knowledge acquisition and Data engineering) and 1 new medical device support process (Continuous validation). Additionally, Table 1 indicates that there are 6 amended medical device software lifecycle processes and 2 amended medical device support processes.

Table 1 Medical Device Software Lifecycle and Support Processes

Medical Device Software Lifecycle Processes	**N, A or X**	**Medical Device Support Processes**	**N, A or X**
1. Software Development Planning	A	1. Configuration Management	A
2. Software Requirements 3. Analysis	A	2. Software Release	X
4. Software Architectural Design	A	3. Software Problem Resolution	X
5. Software Detailed Design	X	4. Software Change request Management	X
6. Software Risk Management	A	5. Software Maintenance	A
7. Knowledge Acquisition	N	**6. Continuous Validation**	N
8. Data Engineering	N		
9. Software Unit Implementation and Verification	A		
10. Software Integration and Integration Testing	X		
11. Software System Testing	A		

4.1 New Processes

Section 4.1 provides an overview of the purpose and content of the 3 new processes of Knowledge acquisition, Data engineering, and Continuous validation.

Knowledge Acquisition Process

The purpose of the knowledge acquisition process is to provide the knowledge necessary to create the AI models. It includes knowledge about the domain and the problem. This practice includes collecting, structuring, and integrating information into AI systems to improve learning, reasoning, and decision-making. This process is crucial for building expert systems, knowledge graphs, and machine learning models. For a

machine learning-based AI system, knowledge is used to guide the tasks of data selection, data preparation and model engineering. Practices involved in this process include: defining the scope and criteria for knowledge acquisition; seeking sources of knowledge; extract knowledge; manage the results of knowledge acquisition. Knowledge sources can include:

(i) Human Experts → Interviews, surveys, and domain expertise;

(ii) Structured Data → Databases, spreadsheets, ontologies;

(iii) Unstructured Data → Text, images, videos, sensor data;

(iv) Scientific & Technical Documents → Research papers, manuals;

(v) Crowdsourced & Open Data → Wikidata, GitHub, public datasets. Additionally, the knowledge acquisition process should ensure that all gathered knowledge is traceable to its source.

Data Engineering Processes

The purpose of AI data engineering process is to make sure data can be used to create and verify AI models. This process involves the practices of:

(a) Acquiring or selecting data from different sources; The manufacturer should, (i) specify the number of required data sets, (ii) specify the inclusion and exclusion criteria for individual data sets, (iii) specify quality control of data, (iv) analyse the factors that might cause a bias and provide a list of potential biases, (v) specify a distribution of input data that is representative for the target system / population

(b) Conduct data labelling /annotation; When using tools for labelling, considerations should include an evaluation of the features and functionalities of such tools and the proper validation of such tools to ensure the high quality of labelled data.

(c) Analyse and explore data for understanding of the domain, the problem and data issues.

(d) Analyse data on an ongoing basis to ensure it is of sufficient quality. The manufacturer should validate that the test and training data meet the specified criteria.

(e) Data lineage and data provenance is documented. Since training data can determine the behaviour of an AI system, it is important to understand its source, how it was processed, its owner and its rationale, in case there are any issues with the data or its need to be renewed.

(f) Data is cleaned, merged and prepared. This operation includes the operations of: data extraction, merging, cleaning, filtering, correcting, augmenting, conversion, encoding and dealing with missing values.

(g) Sensitive data is protected through careful handling and privacy-preserving techniques, and it is ensured that any recording and use of personal information in the data are in compliance with applicable laws and legal requirements, for example the GDPR.

Continuous Validation Process

The purpose of the continuous validation process is to monitor that AI models keeps performing satisfactorily, or to demonstrate performance of the AI model over time, as desired behaviour can change. Practices of this process include:

(a) A post-market surveillance plan is compiled specifically for the product. The plan should be approved and lists all the relevant data sources to be monitored. Additionally the plan should: (i) describe for each data source how, how often and by whom data is collected (ii) specify how data has to be analysed, including requiring that quality

metrics such as sensitivity and specificity are monitored. (iii) specify the data to be collected to be able to analyse whether the data in the field is consistent with the expected data or training data. (iv) set requirements to collect and analyse data to assess how the use of the system changes over time. (v) for continuous learning systems, specify if and how often which data sets have to be retested after algorithm updates. (vi) for continuous learning systems specifies how, and how frequently changes in the algorithm updates are assessed. (vii) lists threshold values that trigger actions. (viii) The threshold values include quality metrics. (ix) These threshold values include features. (x) The plan specifies the frequency and content of compiling post-market surveillance reports

(b) Monitoring of data drift and concept drift, and monitoring any other requirements that are expected to change over time such as execution time, transparency and fairness.

(c)Assess risk: The manufacturer should establish a post-market risk management system. This should include: (i) A specification on how, how often and by whom the state of the art is monitored and re-assessed. (ii) The state-of-the-art assessment takes latest algorithms for machine learning and for improving interpretability into account. (iii) The state-of-the-art assessment takes alternatives for the "ground-truth" respectively the gold standard. (iv) There is a specification on how, how often and by whom post-market data are evaluated for new or changed hazards, hazardous situations and risks. − The post-market risk analysis searches for (adverse) behavioural changes or (foreseeable) misuse. For products that have been placed on the market for more than one-year post-market risk management activities are documented.

(e) Deciding whether to perform maintenance on the AI model in the case of any deviations,

(f) Apply guard rails if they have been defined by applying boundaries on the output data, or by defaulting to an alternative safe model in case of deviations.

4.2 Amended Processes

Software Development Planning

The amendment to this process includes the requirement for the software development plan to include or reference an AI Algorithm development plan. This algorithm plan should consider the following factors:

(a) Governance (Regulatory and legal compliance such as GDPR, EU AI Act, Data governance, Ethical and responsible AI principles), and Objectives (problem the AI algorithm will solve)

(b) Resourcing (Human resources, Computational resources, Software and AI development tools), and Competency (such as data engineering, AI ethics and responsible AI, M/L algorithms, Deep learning architectures, Maths, Medicine etc,)

(c) Transparency (provide documentation on how AI models make decisions) and Traceability (data traceability, traceability in how decisions are made and documented).

(d) Data Strategy: Sources, Quality, Preprocessing, Security and \compliance.

(e) Ethics and fairness (Ensure AI aligns with ethical values such as fairness, accountability, transparency, and privacy).

(f) Risk management for safety, performance, and fundamental rights.

(g) Security and data protection.

(h) Algorithm selection (Identify problem type, then identify algorithm type then consider algorithm selection criteria e.g Accuracy v Interpretability) and Model design (define model architecture, feature engineering, Hyperparameter optimisation., Model evaluation metrics.

(i) Training and Validation: Training strategy, Validation approach, Hyperparameter tuning.

(j) Scalability (ability of an AI system to efficiently handle increasing amounts of data, computations, and user demands without compromising performance), and Observability (the ability to monitor, understand, and debug AI models throughout their lifecycle).

(k) Interpretability (The extent to which a human can understand the cause of a model's decision) and Explainability (The ability to describe a model's behaviour in human-understandable terms).

(l) Evaluation metrics: Performance, Fairness, Robustness, Error analysis.

(m) Development workflow: Tools and frameworks, Versioning, Reproducibility.

(n) Documentation and Reporting: Technical documentation, Model cards, Risk assessment/Impact reports.

Software Requirements Analysis

Base practice 1 of the software requirements analysis process requires that all software requirements are defined and documented. Extra consideration for this practice when developing AIeMDS include:

(a) The desired performance (level of correctness) of the model or models. Setting these requirements requires careful selection of the right metrics (e.g. minimal precision and minimal accuracy). Such requirements can include the range of input data for which the model is to perform within the required boundaries

(b) Considerations regarding the level of autonomy exercised by the AI system, e.g. whether there is a human-in-the- loop. If so, a definition of which decisions the human can take with regards to the AI system behaviour, such as setting or adjusting thresholds configuring the desired performance level of the AI system.

(c) Requirements on how to deal with unexpected behaviour of the system. For example, by establishing and applying additional deterministic rules to ensure safety

(d) Requirements on transparency and explainability. Machine learning models can be highly complex and, as a result difficult to understand. Depending on the situation, individuals can be entitled to an explanation as to how a model decision was made particularly when they are affected significantly (e.g. legally or financially)

(e) The organization informs individuals that they are interacting with an AI system in accordance with applicable legal requirements

(f) Continuous validation requirements

(g) Fairness requirements: It is important to set requirements for the fairness and inclusiveness of the algorithm and data for certain groups in society. Furthermore, AI system decisions should be based on clear and interpretable features so that fairness can be verified. Fairness metrics should be defined in order to set these requirements

(h) Privacy requirements: In cases where personal data are used. Informing individuals, providing them with control and protection of personal data are important. Also,

the choice of algorithm can be influenced by privacy considerations (e.g. differential privacy algorithms.

(i) Security requirements: In case there is an additional attack surface resulting from the use of AI. Typically, this includes: securing data that are used for either training or testing, protecting against input manipulation, protecting against "model inversion", and protecting against "model theft"

Software Architecture Process

Base practice 4 of this process requires the assignment of a software safety class. For AIeMDS, the degree of autonomy/automation and medical purpose are important factors in determining the safety classification, thus this base practice has been amended with the note to consider the following factors:

(a) Level of Task Automation which is the degree to which the output requires and receives review and approval by the user: (i) Fully automated, (ii) Conditionally automatic, (iii) Semi-automatic (iv) Manual

(b) Degree of Clinical Autonomy which is a spectrum of capacities or liberties to operate independently of a clinical user's guidance**:** (i) Independent/Autonomous, (ii) Conditionally independent/ autonomous,(iii) Supervised,(iv) Non-autonomous.

(c) Degree of Learning/Change Management Autonomy which describes the effectuation and control of training, learning and updates to the medical device software: (i) Self-learning/autonomous learning, (ii) Externally controlled user-driven learning/change,(iii) Externally controlled manufacturer-driven learning/change.

(d) Medical purpose: (i) Diagnosis, (ii) Prevention, (iii) Monitoring, (iv) Mitigation, (v) Prediction, (vi)Treatment,

(e) Intended Conditions/Diseases/ Disorders and Grade/Stage/Level: (i) Critical, (ii) Serious, (iii) Non-Serious condition or disease, including (iv) consideration of level of progression/stage/ grade (e.g., a chronic condition or an acute change in a chronic condition).

Software Unit Implementation and Verification Process

Base Practice 1 of this process requires implementation of software units. Notes have been added to this base practice to include the following tasks:

(a) Model preparation requirements include: (i) the manufacturer should deliberately select features for training, (ii) the manufacturer should deliberately divide the data into training, validation and test data, and provide justification for the ratio.

(b) Algorithm selection; Select an appropriate machine learning algorithm taking into account the type of model task (e.g. clustering, time series prediction, classification) and the technique that works best for the task at hand, which can also be determined by experimentation.

(c) Model training: (i) the manufacturer should document model specific data processing. (ii) if there are several quality metrics, the manufacturer should document the quality metrics for the model to which it wants to optimize the model and justify it based on the intended use. (iii) The manufacturer should avoid over-fitting. (iv) The manufacturer should verify that the training actually trains the model.

Base Practice 2 requires the establishment of unit verification procedures. Notes have been added to this base practice that a model verification test plan should include: (i) Objectives, Scope and Responsibilities, (ii) Test plan environment including what

tools are used for testing, hardware applicable, software frameworks, and test data, (iii) the criteria for the selection of test data, (iv) the plan for performing an impact assessment after implementing a change to the AI component, (v) the test methods to be used for the planned test, (vi) test plan stages including, data validation, engine validation, unit testing on individual components of the AI models, integration testing, functional testing, performance testing, data drift testing, robustness testing. (i) Bias and Fairness.

Base Practice 4 requires software units to be verified. Notes have been added to this base practice to include the following tasks: (i) As part of the generation of test results, the test data used shall be recorded. This includes all actual input and output data of the test. (ii) The manufacturer shall document objective evidence of the test execution and the test results in a test report. The test results shall be traceable to the test case and to the AI version.(iii) During the generation of test results, for any deviations or changes from the test specification, a complete description of the deviation, the justification and/or reason of the deviation shall be documented along with the acceptability of the results of the testing. Examples of deviations that could have an impact or lead to unexpected behaviour when testing AI/ML medical devices are: Changing the order of execution of test case; Changing the order of presentation of data to the system; Repeating some of the tests.

Software System Test Process

Base practice 1 of this process requires that tests are developed for integrated software product. For this base practice additional consideration needs to be given to: (i) there is a documented strategy for black box testing. (ii) the tests cover all software / product requirements (including non-functional requirements). (iii) the tests verify whether risk mitigation measures are effective. (iv) tests verify that the system safely manages unseen attacks. (v) there is a description of tested software version, test data, test environment (e.g., hardware), tester and evaluation of test results. (vi) after changes to the software, the tests are repeated unless the manufacturer can provide a rationale for skipping test activities. (vii) the tests are reproducible.

Configuration management Process

Outcome 1 of the configuration management process requires that items requiring configuration management are identified, defined and documented. For this outcome additional consideration needs to be given to: AI systems contain AI-specific artefacts that also require configuration management: the data that represents the model (e.g. rules, weights, parameters), documentation of AI elements, data and metadata. If machine learning is used, it can be beneficial to apply configuration management on the model combined with the data with which it was trained. This allows for traceability (e.g. for auditing and compliance) and for reproducing experiments. In the design and development stages, the organization should consider AI-specific source code management controls associated with AI-specific particularities (e.g. AI data engineering, model training).

Software Maintenance

Outcome 1 of the Software maintenance plan requires that a maintenance plan is developed to manage modification of products. For this outcome, consideration should be given to the FDA's Predetermined Change Control Plan (PCCP), which is a framework that allows manufacturers of AI/ML-based Software as a Medical Device (SaMD)

to predefine modifications to their software without requiring a new premarket submission each time an update is made. Key components include:

(a) Description of modifications.

(b) Software Change Protocol (SCP) which outlines the verification and validation (V&V) activities that will be conducted when a modification is made.

(c) Impact Assessment & Risk Management to evaluate how AI modifications could affect patient safety and device effectiveness.

(d) Transparency & Real-World Monitoring where Manufacturers must demonstrate how they will (i) Monitor real-world performance of AI/ML models (ii) Detect and mitigate issues like data drift, unexpected performance deviations, or adverse events. (iii) Provide transparency to end users.

Additionally, the software maintenance process notes that part of maintenance is monitoring the system. Because monitoring an AI model is so different from typical monitoring of a system, a dedicated process of continuous validation has been defined (see section 4.1). Furthermore, the software maintenance process contains a new base practice as follows: Modified models are verified and released: When a released model is updated, a modified model is created. The modified model shall be verified before it is taken into use. The manufacturer shall design, set and document a process to control the model release of the modified model.

Software Risk Management Process

The purpose of software risk management is to ensure that all risks related to software safety and security are addressed. Base practice 2 of the software risk management process requires the manufacturer to identify and analyse potential causes of a software item contributing to a hazardous situation. For this practice additional consideration needs to be given to:

(a) risks that occur specifically to the chosen ML libraries. Key risks include: (i) Data related risks such as bias and fairness issues, data leakage, poor data handling, (ii) Security risks such as adversarial attacks, dependency vulnerabilities, model extraction attacks, (iii) Performance and scalability risks such as memory and computation overhead, inefficient hyperparameter tuning, scalability issues, (iv) Interpretability and explainability risks such as opaque model behaviour, misuse of explainability tools.

(b) risks related to data such as: (i) the data used for building an AI system may not be a true or appropriate representation of the context or intended use of the AI system, and the ground truth may either not exist or not be available. Additionally, harmful bias and other data quality issues can affect AI system trustworthiness, which could lead to negative impacts (ii) Datasets used to train AI systems may become detached from their original and intended context or may become stale or outdated relative to deployment context (iii) AI system dependency and reliance on data for training tasks, combined with increased volume and complexity typically associated with such data.

(c) risks related to data processing (e.g., during training). Risks can occur from errors in (i) format conversion, (ii) detecting and dealing with missing values, detecting and handling outliers, unit conversions, converting numeric into categorial values, loss of data, feature extraction.

5 Discussion

AI-MDevSPICE was developed based on standards/regulations/guides/frameworks published before December 2024. However, this is a rapidly evolving space with relevant AI documentation being published at an ever-increasing rate. For example, Figure 1 shows the number of standards published on the British Standards Online database using the search term 'Artificial Intelligence' for years 2021 to 2024. It is expected that year 2025 will continue this trend.

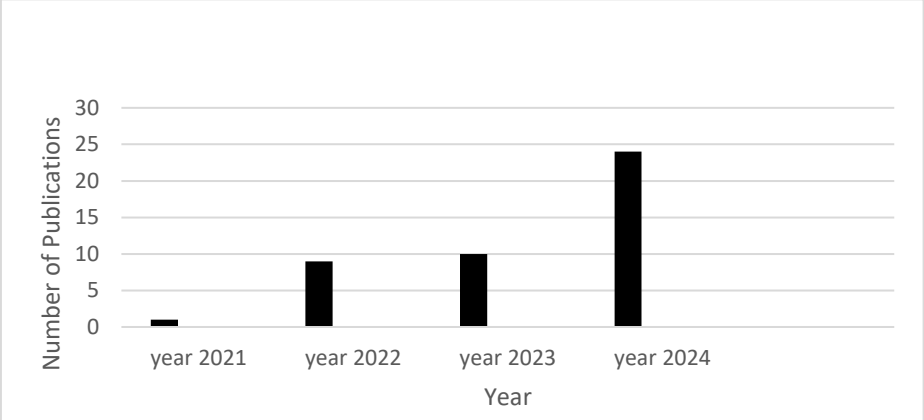

Fig. 1. Number of AI related publications per year in British Standards database

It is evident that the standards and regulations around AI are evolving rapidly as governments, organizations, and international bodies try to balance innovation with safety, ethics, and accountability. As an example, IEC 62304 [15], which is the medical device software lifecycle standard is being revised and it is expected that a new version, which will include development of AI technology in medical device software, will be published in year 2027. This new version will likely lead to some amendment to AI-MDevSPICE. The key takeaway is that just as the AI standards and regulatory landscape is evolving, the outlook is that AI-MDevSPICE is likely to also evolve.

6 Conclusion

The fact is that you cannot create software without process. And a better-quality development process translates to a better quality software. One well established method to create a better-quality software development process is to assess the current development process in order to identify any existing shortcomings against relevant standards and established best practices. MDevSPICE® is a medical device software specific process assessment framework. However, MDevSPICE® was developed before the relatively recent uptake of AI functionality in medical device software, and therefore MDevSPICE® does not contain the extra processes/requirements necessary for developing trustworthy AIeMDS. Therefore, in this paper we outline the development of AI-

MDevSPICE. AI-MDevSPICE amends and extends MDevSPICE® to include the processes/requirements necessary for developing trustworthy AIeMDS.

The current AI regulatory landscape is evolving rapidly as governments and international bodies seek to balance innovation with safety, ethical concerns, and societal impacts. The current AI-MDevSPICE is based on regulations/standards published before December 2024. However, as we anticipate further evolvement in AI standards and regulations throughout 2025, with some specific to the medical device software domain, we expect AI-MDevSPICE to also evolve.

Acknowledgments. This publication has emanated from research conducted with the financial support of Research Ireland (RI) under Grant number 21/FFP-A/9255, and by Dundalk Institute of Technology's Technical University Transfer Fund.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article..

References

1. FDA. Artificial Intelligence-Enabled Device Software Functions: Lifecycle Management and Marketing Submission Recommendations. (2025)
2. Datta, S., Barua, R., Jonali, D.: Application of Artificial Intelligence in Modern Healthcare System. In: Pereira, L. (ed.) Alginates. IntechOpen (2019). https://doi.org/10.5772/intechopen.90454.
3. Dilsizian SE, Siegel EL. Artificial intelligence in medicine and cardiac imaging: Harnessing big data and advanced computing to provide personalized medical diagnosis and treatment. Current Cardiology Reports. 2014;16:441
4. Villar JR, González S, Sedano J, et al. Improving human activity recognition and its application in early stroke diagnosis. International Journal of Neural Systems. 2015;25:1450036
5. National Institute of Standards and Technology**. "**Framework for Cyber-Physical Systems: Volume 2, Working Group Reports," NIST Special Publication 1500-202, June 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-202.pdf
6. Lockey,S.,Gillespie,N.,Holm,D.,Someh,I.: A Review of Trust in Artificial Intelligence: Challenges, Vulnerabilities and Future Directions. In. Proceedings of the 54th Hawaii International Conference on System Sciences pp.5463-5472. Hawaii International Conference on System Sciences (2021)
7. European Commission High-Level Expert Group on Artificial Intelligence: Ethics Guidelines for Trustworthy AI," April 8, 2019, https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf.
8. European Commission: 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206, (2021).

9. National Institute of Standards and Technology: AI Risk Management Framework: Initial Draft," March 17, 2022, https://www.nist.gov/system/files/documents/2022/03/17/AI-RMF-1stdraft.pdf.
10. Lepmets,M. et al.: Development of MDevSPICE® – the medical device software process assessment framework. Journal of Software: Evolution and Process. 27:565–572 (2015)
11. ISO/IEC 15504-5. Information technology – Software process assessment – An exemplar software lifecycle process assessment model. in 15504. 2004.
12. IEC TR 80002-3: Medical device software -- Part 3: Process reference model of medical device software life cycle processes (IEC 62304). 2014. IEC: Geneva, Switzerland. pp. 23.
13. ISO/IEC 24774 - Systems and Software Engineering – Life Cycle Management - Guidelines for Process Description. 2010. Geneva, Switzerland. pp. 15.
14. ISO/IEC. ISO/IEC 12207:2008 – Systems and Software Engineering – Software life cycle processes. ISO/IEC: Geneva, Switzerland, 2008.
15. IEC. IEC 62304: Medical Device Software – Software Life-Cycle Processes. IEC: Geneva, Switzerland, 2006.
16. ISO 13485: Medical Devices – Quality Management Systems – Requirements for Regulatory Purposes. ISO: Geneva, Switzerland, 2003.
17. ISO 14971 – Medical Devices – Application of Risk Management to Medical Devices. ISO: Geneva, Switzerland, 2009.
18. IEC. IEC TR 80002-1 – Medical Device Software – Part 1: Guidance on the Application of ISO 14971 to Medical Device Software. IEC: Geneva, Switzerland, 2009
19. FDA. Guidance for the content of premarket submissions for software contained in medical devices. 2005, p. 20.
20. FDA. General principles of software validation; final guidance for industry and FDA staff. 2002. p. 43.
21. FDA. Guidance for industry, FDA reviewers and compliance on – off-the-shelf software use in medical devices. 1999. p. 26.
22. ISO 33061: Information technology — Process assessment — Process assessment model for software life cycle processes, 2021
23. FDA: Proposed Regulatory Framework for Modifications to Artificial Intelligence / Machine Learning (AI / ML) -Based Software as a Medical Device (SaMD) - Discussion Paper and Request for Feedback. (2019)
24. FDA: Predetermined Change Control Plans for Machine Learning-Enabled Medical Devices: Guiding Principles (2023)
25. FDA: Good Machine Learning Practice for Medical Device Development: Guiding Principles (2021)
26. FDA**:** Transparency for Machine Learning-Enabled Medical Devices: Guiding Principles
27. FDA: Marketing Submission Recommendations for a Predetermined Change Control Plan for Artificial Intelligence-Enabled Device Software Functions (2024)
28. European Commission: Regulation (EU) 2016/679 of the European Parliament on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

29. NIST: Artificial Intelligence Risk Management Framework (AI RMF 1.0) (2023)
30. ITU-T FG-AI4H DEL2.2: Good practices for health applications of machine learning: Considerations for manufacturers and regulators (2022)
31. European Commission: Directive (EU) 2019/882 of the European Parliament of 17 April 2019 on the accessibility requirements for products and services
32 De La Cruz,R.: The Application of IEC 62304 for AI and Other Technologies: It's Not Rocket Science, It's Computer Science'. In AAMIARRAY https://array.aami.org/content/news/application-iec-62304-ai-and-other-technologies-s-not-rocket-science-s-computer-science (2023)
33. ISO 5338: Information technology — Artificial intelligence — AI system life cycle processes (2023)
34. ISO 23894: Information technology — Artificial intelligence — Guidance on risk management (2023)
35. IEC 63450: Testing of Artificial Intelligence / Machine Learning-enabled Medical Devices-Draft (2024)