IML4E

Industrial Machine Learning for Enterprises

Deliverable D3.3

First version of tools for advanced model engineering

Project title:	IML4E
Project number:	20219
Call identifier:	ITEA AI 2020
Challenge:	Safety & Security

Work package:	WP3
Deliverable number:	D3.3
Nature of deliverable:	Report/Prototype
Dissemination level:	PU
Internal version number:	1.0
Contractual delivery date:	2022-11-30
Actual delivery date:	2022-12-14
Responsible partner:	University of Helsinki

Contributors

Editor(s)	Mikko Raatikainen (University of Helsinki)
Contributor(s)	Dorian Knoblauch (Fraunhofer Focus), Janis Lapins (Spicetech), Mikko Raatikainen (University of Helsinki), Saku Suuriniemi (Reaktor)
Quality assuror(s)	Mohamed Abdelaal, Software AG, Johan Himberg, Reaktor

Version history

Version	Date	Description
1.0	22-12-14	Version for publication

Abstract

This document describes the first version of the tools for advanced model engineering as complementary documentation for the software deliverable D3.3. The tools covered are the Model cards toolbox, Stevedore wrapper, CABC-mapper (Continuous-audit-based-certification-mapper), and Valicy tool. The methodological support of the tools is defined and will be refined in the other deliverables of the IML4E project. Moreover, the methods and techniques will be assessed by the use cases of the IML4E project.

Keywords

MLOps, model cards, certification, testing.

Executive Summary

This document describes the initial version of the version of tools for advanced model engineering. The tools are the Model cards toolbox, Stevedore wrapper, CABC-mapper (Continuous-audit-based-certification-mapper), and Valicy tool. This document is a complementary description of tools while the tools themselves are software tools. We shortly summarize the tools using a common technology sheet format in this document while the documentation of each individual tools provides more detailed technical description. We report those tools that have reached their first public release. The future work includes developing the tools to be more mature and integrate them with IML4E framework and OSS platform. Moreover, these methods and techniques will be realized and assessed in the case studies of the IML4E project.

Table of contents

1 Introduction

1.1 Role of this Document

The purpose of this document is to provide a complementary description for the first version of methods and techniques for advanced model engineering of the IML4E project. The documentation of each individual tools provides more detailed technical description, e.g., in the GitHub readme-file. The tools are software tools developed within the project. On the one hand, the methodology for applying the tools is covered in deliverable D3.2 and will be refined more extensively in deliverable D3.4. On the other hand, the tools will be refined and extended, possibly adding new tools in D3.5. Moreover, the tools will be assessed in the use cases of the IML4E project. The document focuses on ML model engineering and quality assurance being parallel with the data engineering-focused deliverable of work package 2 of the IML4E project.

1.2 Intended Audience

The intended audience of the present document is composed primarily of the IML4E consortium for the purpose of understanding the tools and advancing ML model engineering. However, this document is public and can provide an overview of the advances in the IML4E project to wider audience. This document describes methods and technologies for the technically-oriented audience rather than the general public or layman.

1.3 Definitions and Interpretations

The terms used in this document have the same meaning as in the contractual documents referred in [FPP] with Annexes and [PCA] unless explicitly stated otherwise.

1.4 Applicable Documents

Reference	Referred document
[FPP]	IML4E – Full Project Proposal 20219
[PCA]	IML4E Project Consortium Agreement
[D3.1]	Baseline methods and techniques for advanced model engineering
[D3.2]	First version of methods and techniques for advanced model engineering
[D3.4]	Second version of methods and techniques for advanced model engineering

Table 1: Contractual documents.

2 Model Cards Toolbox

General Information	
Name	Model cards toolbox
Provider(s)	University of Helsinki
Topic(s) Covered	Model engineering, model maintenance
Description	Model cards toolbox is a set of tools integrated to GitHub actions to create, validate and visualize model cards semi-automatically. Model cards are ledgers for model-related information, such as performance tests or measures and their results for ethical concerns, in a machine-readable form that can be rendered to suitable presentation for different stakeholders, including the non-technical audience.
Innovation	☐I1: High quality and interoperable data preparation infrastructures for trustworthy ML ☐I2: Scalable MLOps techniques and tools for critical application domains ☒ I3: An MLOps Methodology ☐I4: An experimentation and training platform ☐I5: Pre-standardization work on cross-domain engineering for AI-systems
Related KPIs	☒ ML service and process automation ☐Increased service delivery capability/new products ☐Human or/and computational resources ☐Effectiveness of data usage ☒ Finding defects
Business Impact	☐ New AI enabled services ☐ Fast and efficient deployment of ML products and services ☒ Increased trust in AI enabled products and services ☐ New MLOps consulting service
Examples (Use Cases)	Demonstrated using Wine quality dataset (https://archive.ics.uci.edu/ml/datasets/wine+quality)
Technical Information	
OS	GitHub actions.
Technology Environment	Model card representation in YAML.
Synergies (Other Tools)	CABC-mapper
Additional Information	
License	☒ Open Source ☐Proprietary
Link	https://github.com/CompliancePal/modelcard-action

3 Stevedore Wrapper Class

General Information	
Name	Stevedore wrapper class
Provider(s)	Reaktor
Topic(s) Covered	Model engineering
Description	Stevedore is a wrapper class and generic API, as well as Podman/Docker build automation for Python ML models. A specific use case is a set of machine learning models that may be composed so that they should be tested and packaged together. This, by no means, excludes the use on a single model.
Innovation	☐I1: High quality and interoperable data preparation infrastructures for trustworthy ML ☐I2: Scalable MLOps techniques and tools for critical application domains ☒ I3: An MLOps Methodology ☐I4: An experimentation and training platform ☐I5: Pre-standardization work on cross-domain engineering for AI-systems
Related KPIs	☐ML service and process automation ☒ Increased service delivery capability/new products ☐Human or/and computational resources ☐Effectiveness of data usage ☐Finding defects
Business Impact	☐ New AI enabled services ☒ Fast and efficient deployment of ML products and services ☐ Increased trust in AI enabled products and services ☐ New MLOps consulting service
Examples (Use Cases)	
Technical Information	
OS	Python, Docker
Technology Environment	
Synergies (Other Tools)	
Additional Information	
License	☒ Open Source ☐Proprietary
Link	https://github.com/reaktor/ml-py-stevedore

4 CABC-Mapper

General Information	
Name	CABC-Mapper
Provider(s)	Fraunhofer Fokus
Topic(s) Covered	Model training, MLOps lifecycle
Description	The CABC-mapper (Continuous-audit-based-certification) collects artifacts during the MLOps lifecycle and maps them to a predefined REST interface. In this way further measurement tools can process the obtained information in a standardized way. For the mapper to work it requires plugins for each software component that facilitates the MLOps process or that runs in the pipelines. The initial set of plugins covers the IML4E experimentation platform as well as the use cases.
Innovation	☐I1: High quality and interoperable data preparation infrastructures for trustworthy ML ☐I2: Scalable MLOps techniques and tools for critical application domains ☒ I3: An MLOps Methodology ☐I4: An experimentation and training platform ☒ I5: Pre-standardization work on cross-domain engineering for AI-systems
Related KPIs	☒ ML service and process automation ☐Increased service delivery capability/new products ☐Human or/and computational resources ☐Effectiveness of data usage ☒ Finding defects
Business Impact	☐ New AI enabled services ☐ Fast and efficient deployment of ML products and services ☒ Increased trust in AI enabled products and services ☐ New MLOps consulting service
Examples (Use Cases)	
Technical Information	
OS	Python, Docker
Technology Environment	Kubeflow, MLflow
(Other Tools) Synergies	Related to Model cards toolbox
Additional Information	
License	☒ Open Source ☐Proprietary
Link	https://gitlab.fokus.fraunhofer.de/ml-cse/cabc-mapping (Invite on request: dorian.knoblauch@fokus.fraunhofer.de)

5 VALICY

General Information	
Name	VALICY – a tool for virtual validation of AI & complex software applications
Provider(s)	Spicetech GmbH
Topic(s) Covered	Virtual validation of AI & complex software application, training of state dependent field data to train an AI model for prediction of states
Description	An AI core that runs different competing AI instances to train from application data and drive the testing of input parameters towards critical parameter conditions close to the tested application's decision boundaries, thereby identifying characteristics of examined application by automated inheritance of hyper-parameters. With an increasing number of evaluated results trained by AI models, the AIs within VALICY always improve their own prediction capabilities. The estimated remaining uncertainty of the sampled multi-dimensional space is provided as a stop criterion for VALICY jobs, along with the number of evaluated runs. Data to and from the AI application is stored in a database and transferred via a REST-API. For ease of data transfer, an additional API class writes results using pandas.DataFrame via the API. The frontend allows inspecting the results.
Innovation	☐I1: High quality and interoperable data preparation infrastructures for trustworthy ML ☒I2: Scalable MLOps techniques and tools for critical application domains ☐I3: An MLOps Methodology ☐I4: An experimentation and training platform ☒I5: Pre-standardization work on cross-domain engineering for AI-systems
Related KPIs	☒ML service and process automation ☐Increased service delivery capability/new products ☒Human or/and computational resources ☐Effectiveness of data usage ☒Finding defects
Business Impact	☒ New AI enabled services ☒ Fast and efficient deployment of ML products and services ☒ Increased trust in AI enabled products and services ☐ New MLOps consulting service
Examples (Use Cases)	The VITAREX Pose Estimation Use Case was successfully integrated to VALICY within the course of the IML4E Plenary meeting in Budapest in November 2022.
Technical Information	
OS	Docker containers
Technology Environment	Python machine learning, MySQL, Docker, REST-API, Swagger
(Other Tools) Synergies	
Additional Information	
License	☐Open Source ☒ Proprietary
Link	Valicy.de, API: https://api.valicy.de/docs

6 Conclusions

This document covered the first version of tools for advanced model engineering in the IML4E project. The set of tools will be extended in the course of the project, and the tools will be further developed. Specific attention will be paid to integrating into the IML4E OSS platform to be an integrated part of the existing tool pipeline. In addition, to provide better integration in terms of MLOps methodology, the tools and their methods will be integrated explicitly into the IML4E framework.