IML4E

Industrial Machine Learning for Enterprises

Dorian Knoblauch, Jürgen Großmann

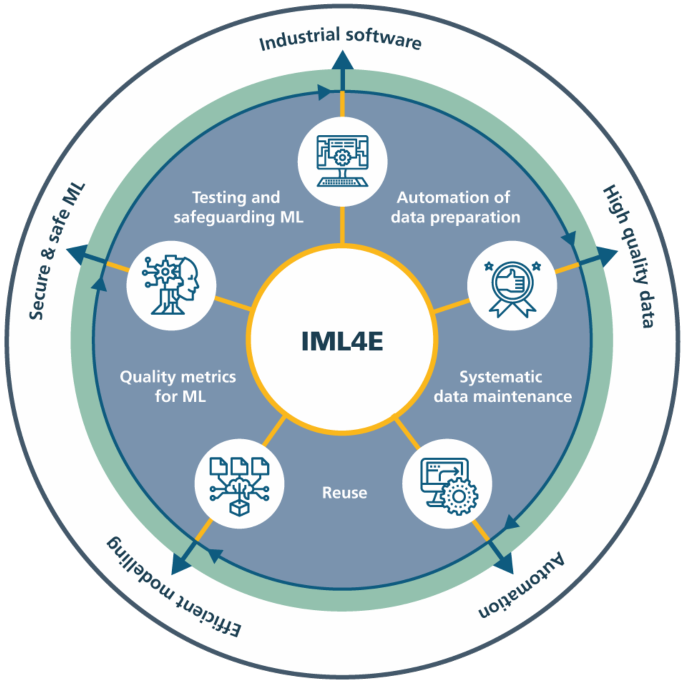
Continuous Auditing Based Certification for ML-enabled Systems

IML4E at a Glance

Industrial Machine Learning for Enterprises

European project to enable **development and quality assurance of intelligent services and intelligent software** on an industrial scale**.**

- **High quality and interoperable data preparation infrastructures for trustworthy ML**
- **Scalable MLOps techniques and tools for critical application domains**
- **MLOps Methodology**
- **Experimentation and training platform (I4) as well as pre standardization work**



IML4E Basics and Partners

ITEA Call

Call AI 2020 addressing the ITEA Challenge Safety & Security

Duration:

- 06/2021 – 05/2024

Resources:

- 70 PY

12 Partners (5 Ind/3 SME/3 Univ/1 RO):

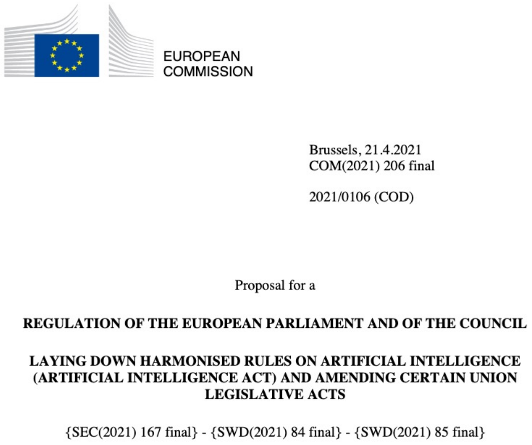
- **Germany:** Fraunhofer, Siemens AG, Software AG, Spicetech GmbH (funded by BMBF)
- **Finland:** Basware, Granlund Oy, Reaktor Innovations, Silo AI, University of Helsinki
- **Hungary:** Budapest University of Technology and Economics, University of Debrecen, Vitarex Studio Ltd

Continuous Audit-based Certification for ML

Regulatory pressure trustworthy AI

- **Proposal for a Regulation laying down harmonised rules on artificial intelligence**
- Defines different risk categories for AI systems
- Makes risk management and explicit risk mitigation mandatory for high-risk AI systems

- Assuring quality is a mean of mitigating risk.
- Quality attributes are a way of describing quality e.g., robustness, correctness, fairness etc.
- Certification is a way of providing trust in quality



EUROPEAN
COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

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

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

Challenges for Certification of ML

Technology related challenges

- **Complexity:** ML targets complex problems, using complex software infrastructure, and the adaptation of millions and sometimes billions of parameters**.**
- **Stochasticity challenge:** ML is a stochastic approach leading to areas of non-determinism and stochasticity that may lead to non-reproducibility in training and may result to unforeseen decision.
- **Stability:** ML-based applications are not necessarily robust (adversarial examples, concept drift).
- **Lack of transparency:** Decisions can often not be completely understood.

Process related challenges

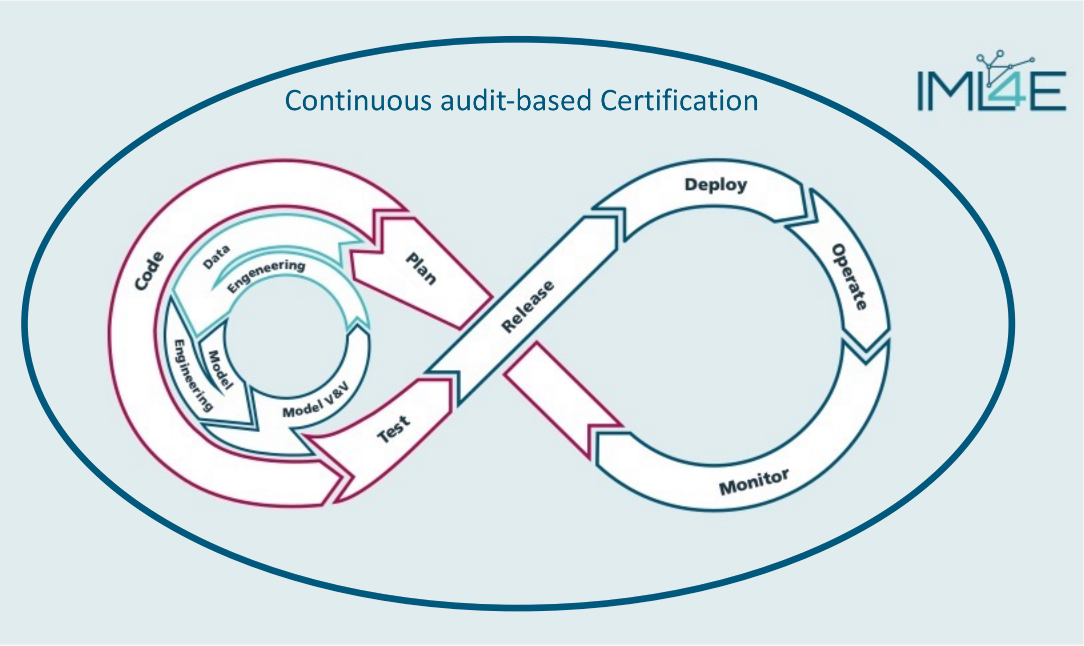
- **Highly iterative optimization approach** in contrast to the construction of classical software.
- Dependence on **data and data quality.**
- **Classical V&V means are not easily transferable.** New V&V techniques and procedures are required.
- **Interdisciplinarity and heterogeneous qualification** required (data science, safety experts, software engineers, domain experts).

Certification apraoaches for ML

- DevOps is a quite established agile process for deploying software in frequent and qualitative manner.
  - Anisetti et. al. evaluating CI/CD artifacts for their continuous certification scheme.
- Granlund et. al. defines and evaluates a MLOps process that produces regulatory compliant models.
  - ML-Model considered as "locked" and becomes part of a product. The whole product gets then verified.
- We have developed and evaluated the approach of continuous audit-based certification for security certification of cloud services in previous works.

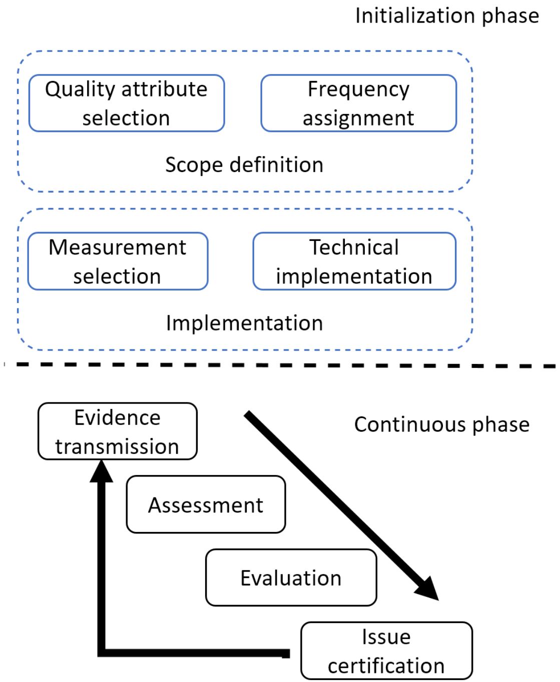
Continuous audit-based certification

- Lifecycle oriented approach for certification
- Considers development and operation
- Allows for high-frequency audits
- Based on automated measurements and tests



Requirements for implementation

- New processes and activities for audits and certification
- Redefinition of roles and responsibilities
- Flexible set of quality attributes that are operational on scale (measurable, automatable, combinable)
- Trustworthy technical infrastructure for certification
  - Flexible auditing architecture
  - Auditing API to adapt to existing MLOps infrastructures
  - Trustworthy execution environment
  - Certificate registry



Main roles in CABC

Certification body

- defines the rules for the certification process
- lays out the criteria under which an audit is conducted
- suspends a certification according to the audit report
- **provides a registry of the ongoing certification process (trusted resource for scope and certification status)**

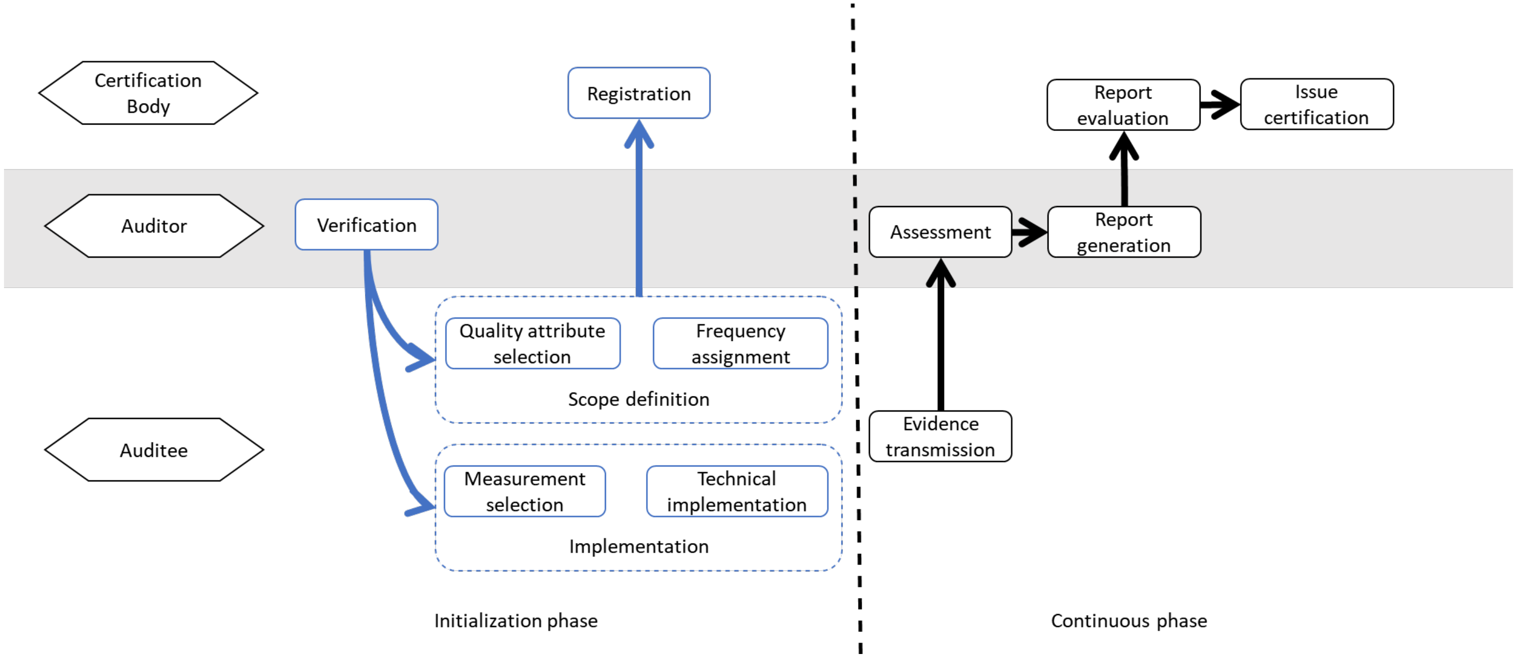
Auditee

- owns the ML-System
- defines the scope which includes selecting the required attributes and the frequency in which they get assessed.
- **implements the technicalities of the assessment in the MLOps environment**

Auditing party

- conducts the audit under the rules of the certification body
- verifies the scope provided by the auditee for its suitability and its adherence to given requirements.
- verifies the initial setup of the continuous auditing and facilitate the automated measurements and assessments at operation.
- provides the means to receive the evidence from the auditee

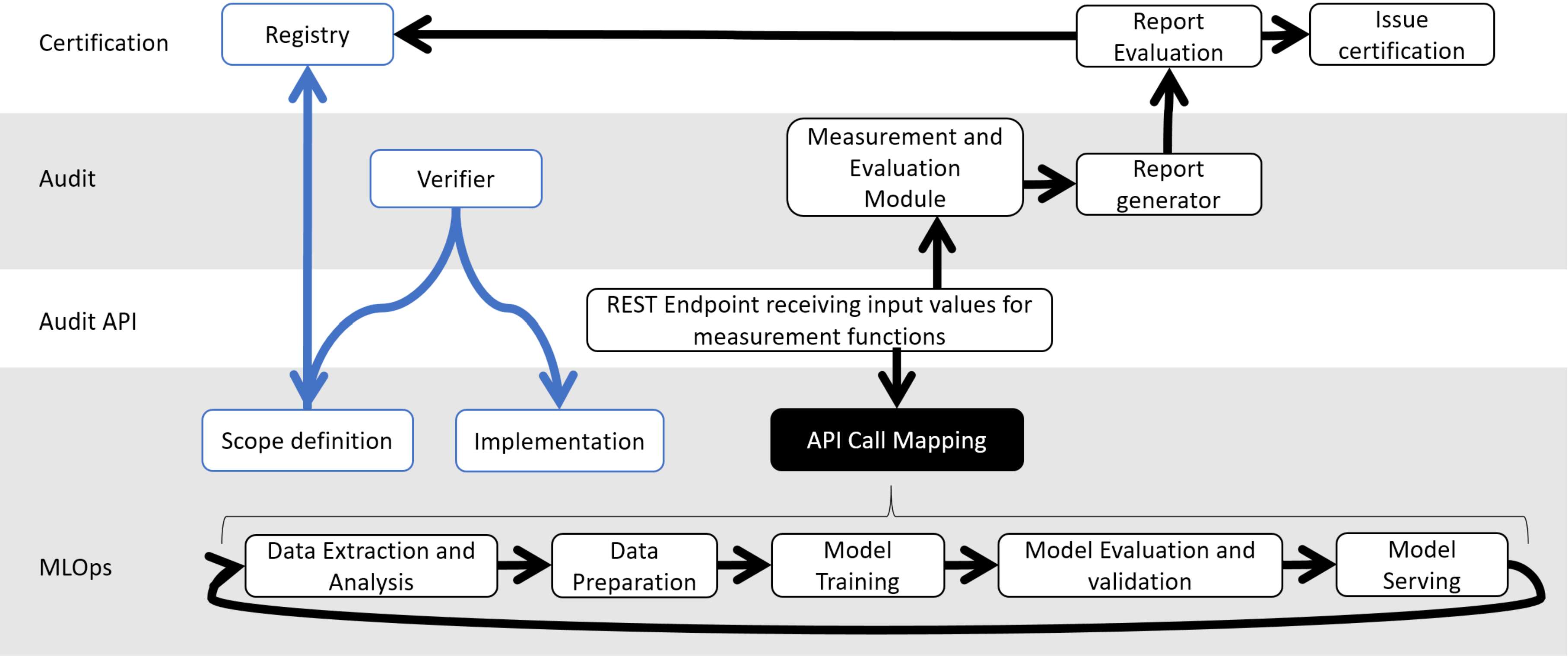
Processes, roles and responsibilites



Layered Architecture

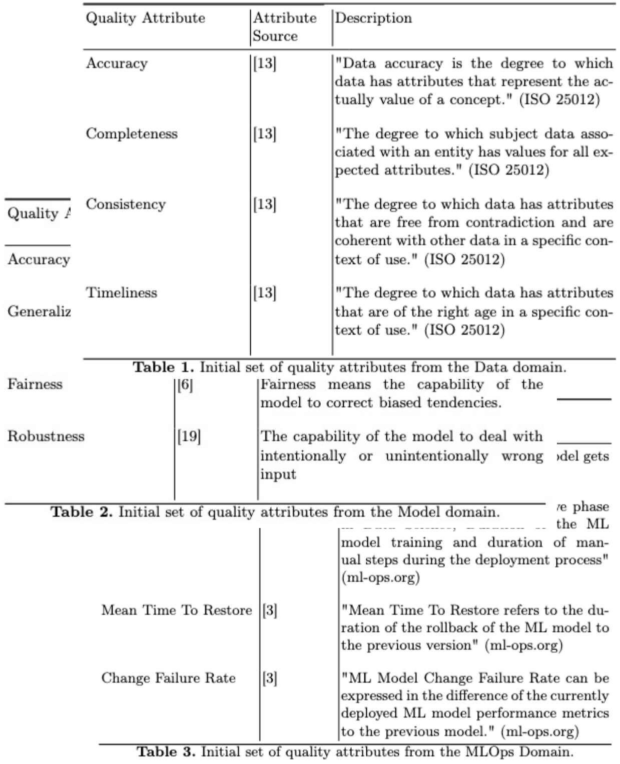
- **Certification layer:** provides means to evaluate the audit report and to inform the stakeholder on the certification status.
- **Audit layer:** supports the verification of the scope and the implementation. Provides means to ensure temper resistance and allows for evaluation of the measurements
- **Audit API layer (integration layer)**: provide means to request evidence from the audited party to the auditor. Defines the measurements and ensures that the system under audit provides the corresponding values
- **MLOps layer:** MLOps process implementation that runs on the premises of the audited party. Provides measurement and testing tools. Evidence gets submitted to the corresponding endpoint of the Audit API.

Layered Architecture



Quality Attribute Catalogue

- Standards for machine learning systems are still emerging.
- Starting with a minimal set of quality attributes collected from ISO 25012 and the state of the art.
- Addressing three MLOps quality domains with different characteristics:
  - **Data quality:** taken from ISO 25012, measurements are performed on static artifacts
  - **Model quality:** compiled from different state of the art contributions,
  - **MLOps quality:** evaluates MLOps process quality as a valuable indicator of product quality



Quality Attribute	Attribute Source	Description
Accuracy	[13]	"Data accuracy is the degree to which data has attributes that represent the actually value of a concept." (ISO 25012)
Completeness	[13]	"The degree to which subject data associated with an entity has values for all expected attributes." (ISO 25012)
Consistency	[13]	"The degree to which data has attributes that are free from contradiction and are coherent with other data in a specific context of use." (ISO 25012)
Timeliness	[13]	"The degree to which data has attributes that are of the right age in a specific context of use." (ISO 25012)

Table 1. Initial set of quality attributes from the Data domain.

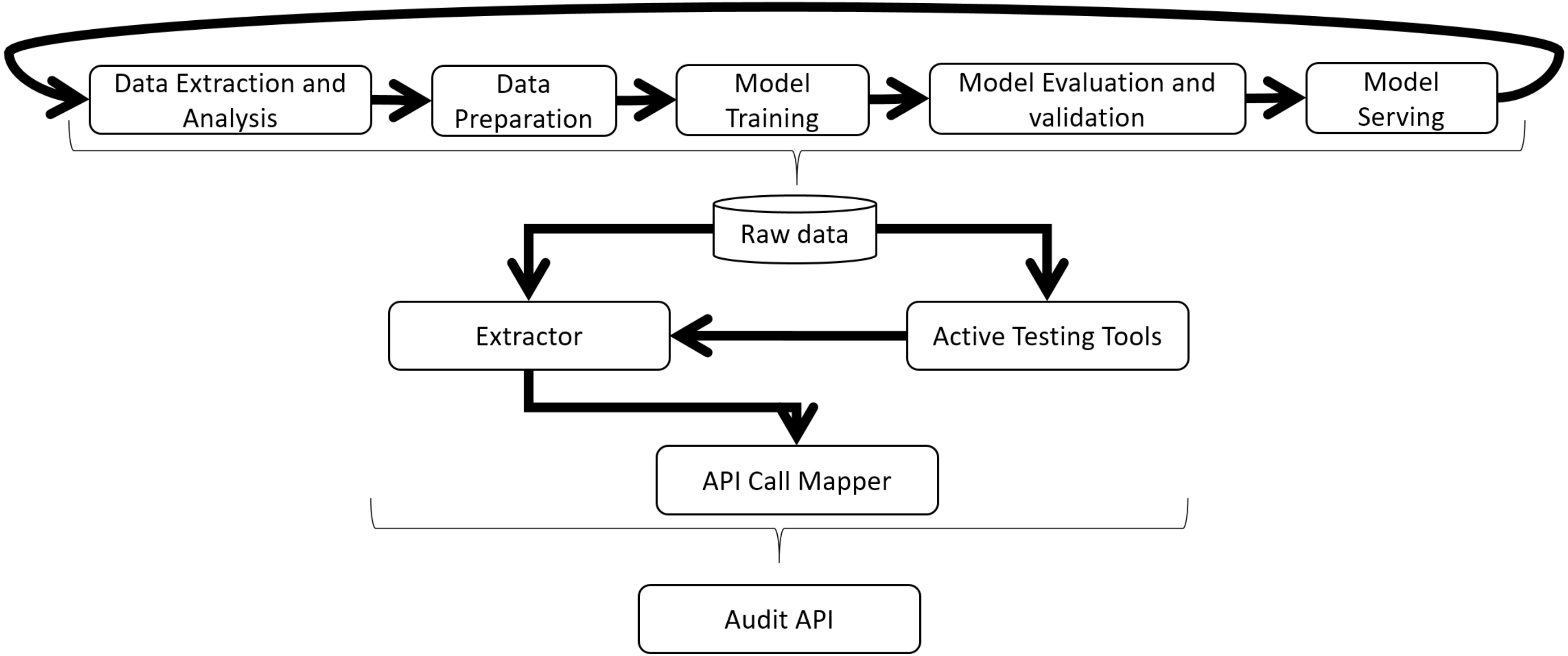
Quality A		
Accuracy		
Generaliz		
Fairness	[6]	Fairness means the capability of the model to correct biased tendencies.
Robustness	[19]	The capability of the model to deal with intentionally or unintentionally wrong input

Table 2. Initial set of quality attributes from the Model domain.

		odel gets
		ve phase the ML model training and duration of manual steps during the deployment process" (ml-ops.org)
Mean Time To Restore	[3]	"Mean Time To Restore refers to the duration of the rollback of the ML model to the previous version" (ml-ops.org)
Change Failure Rate	[3]	"ML Model Change Failure Rate can be expressed in the difference of the currently deployed ML model performance metrics to the previous model." (ml-ops.org)

Table 3. Initial set of quality attributes from the MLOps Domain.

Mapping of artifacts to parameters



Status

- CABC already evaluated and piloted in the area of Cloud Security (https://www.sec-cert.eu/)
- Currently implementing automated measurements based on artifacs of MLFlow

Potential Contribution to ETSI

Potential Work Items with ETSI MTS

- TR: CABC scheme describing processes, roles and the high level architecture for CABC
- TR: MLOps/ML QA life cycle. Describing QA measures along the MLOps/ML life cycle
- TR: Testing ML (basic testing approaches to test ML)
- TR: ML fault and failure taxonomy
- TR: ML Audit API: Measureable quality attributes and (their binding to the Audit API)

IML4E Contact

IML4E project coordinator:

Jürgen Großmann,
Fraunhofer FOKUS

Email: juergen.grossmann@fokus.fraunhofer.de

Phone: +49 30 3463 7390

Web: https://iml4e.org

National contacts

National coordinator Germany: Mohamed Abdelaal, Software AG

Email: Mohamed.Abdelaal@softwareag.de Phone: +49 6151-92-2144

National coordinator Finland: Jukka K Nurminen, University of Helsinki

Email: jukka.k.nurminen@helsinki.fi Phone: +358 50 4836 442

National coordinator Hungary: Péterné Czeiszing, Vitarex Studio Ltd

Email: czeiszing.erika@vitarex.hu Phone: +36 1 466 7404

SPONSORED BY THE
Federal Ministry
of Education
and Research

BUSINESS
FINLAND

National Research, Development
and Innovation Office
Hungary

PROJECT FINANCED
FROM THE NRDI FUND