

Describing software architecture in the programmable world: Method to incorporate ethical and security concerns and trace requirements in software architecture.

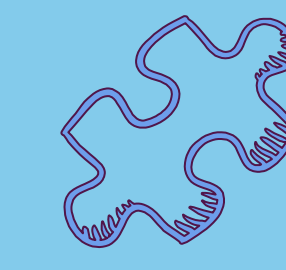
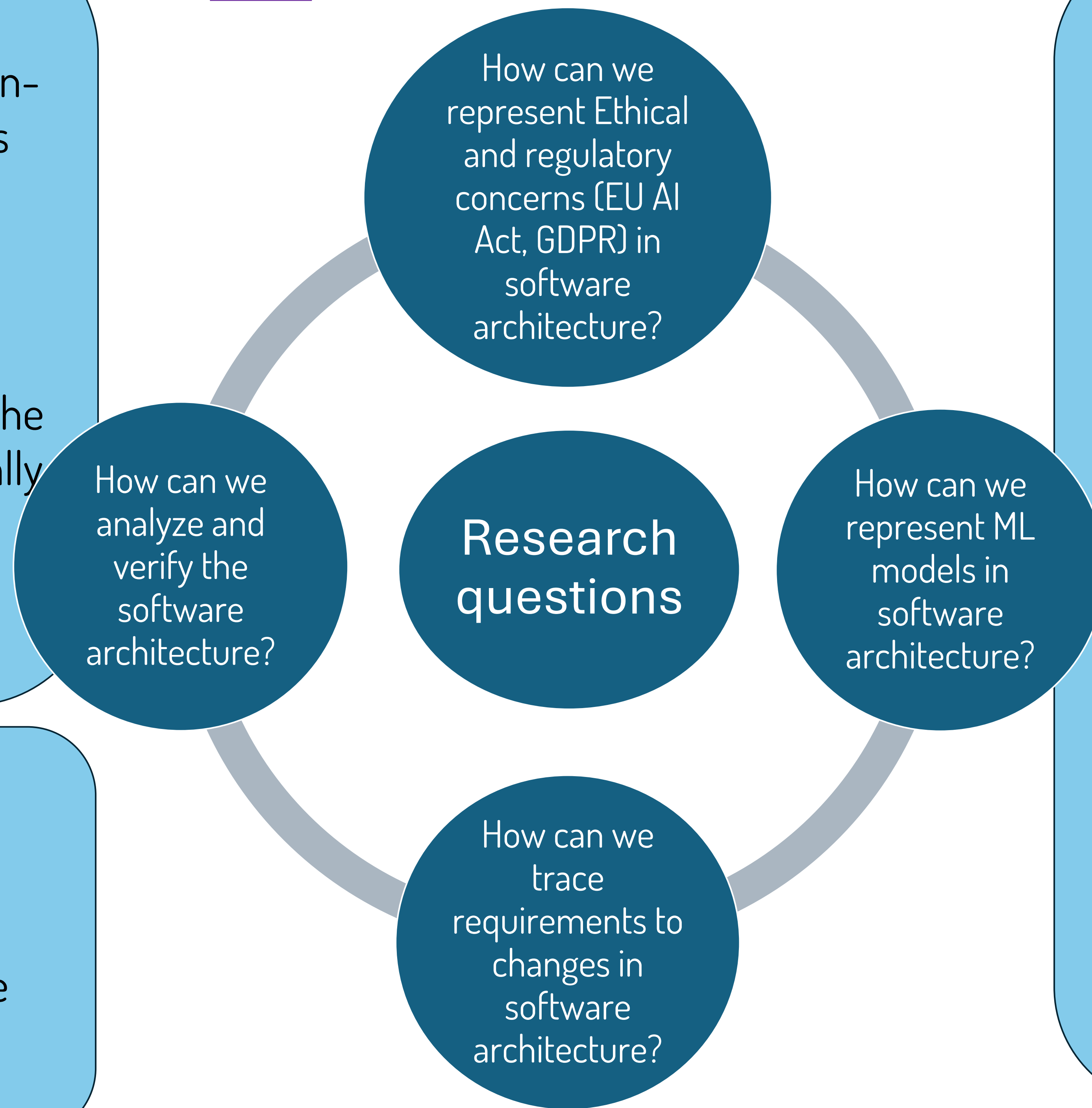


Motivation:

- Difficulty in representing NFR (Non-Functional Requirements) such as security, ethics, and regulations.
- Lack of representation tools of AI/ML model details in software architecture.
- Limitation in running analysis on the validity of an architecture, especially in terms of NFRs.
- Tracing requirements regarding changes in the architecture.



Research questions:



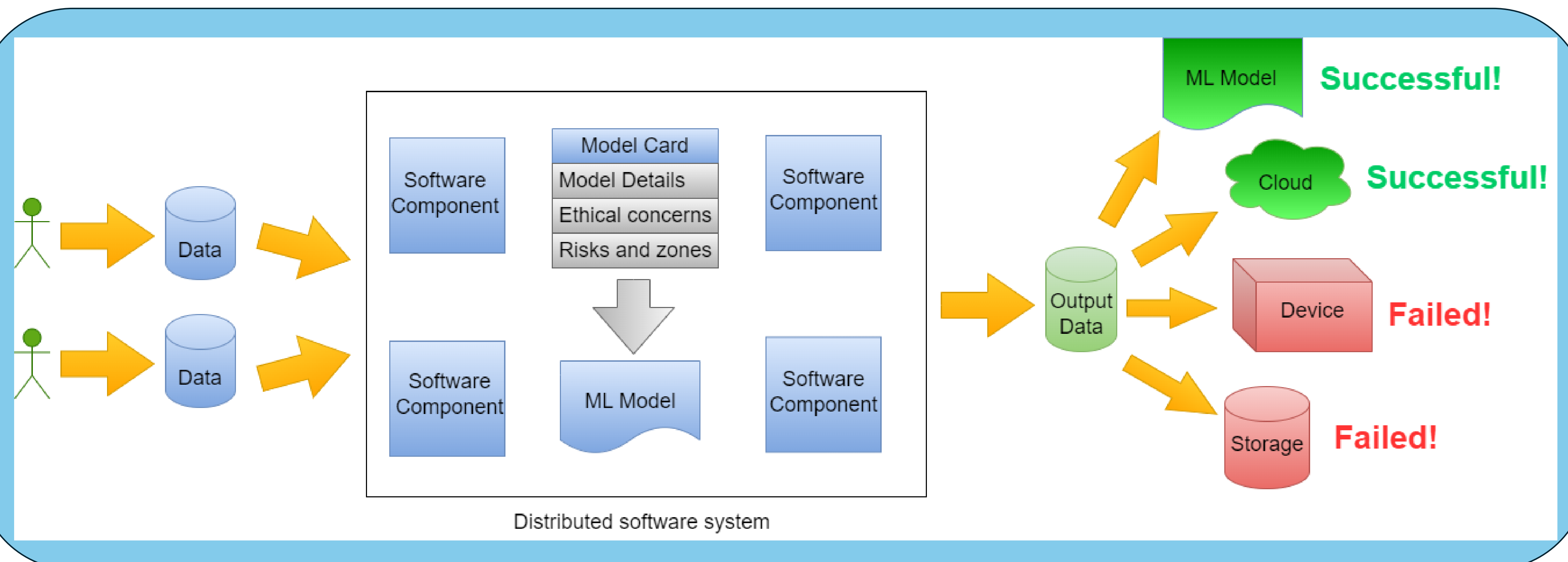
Core topics:

- A machine-readable software architecture.
- Concept of ADL (Architecture Description Language) and similar solutions to describe architecture.
- Concept of Model cards to define AI/ML models.
- Concept of Zoning to define risky and safe zones.
- Implement methods to define regulations.
- Define methods to run analysis of the architecture
- Define suitable method for tracing requirements to changes.
- Tool support



Objective:

To define "privacy and regulation-aware" software architecture for the "programmable world".

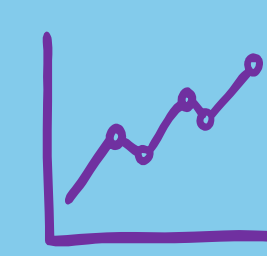
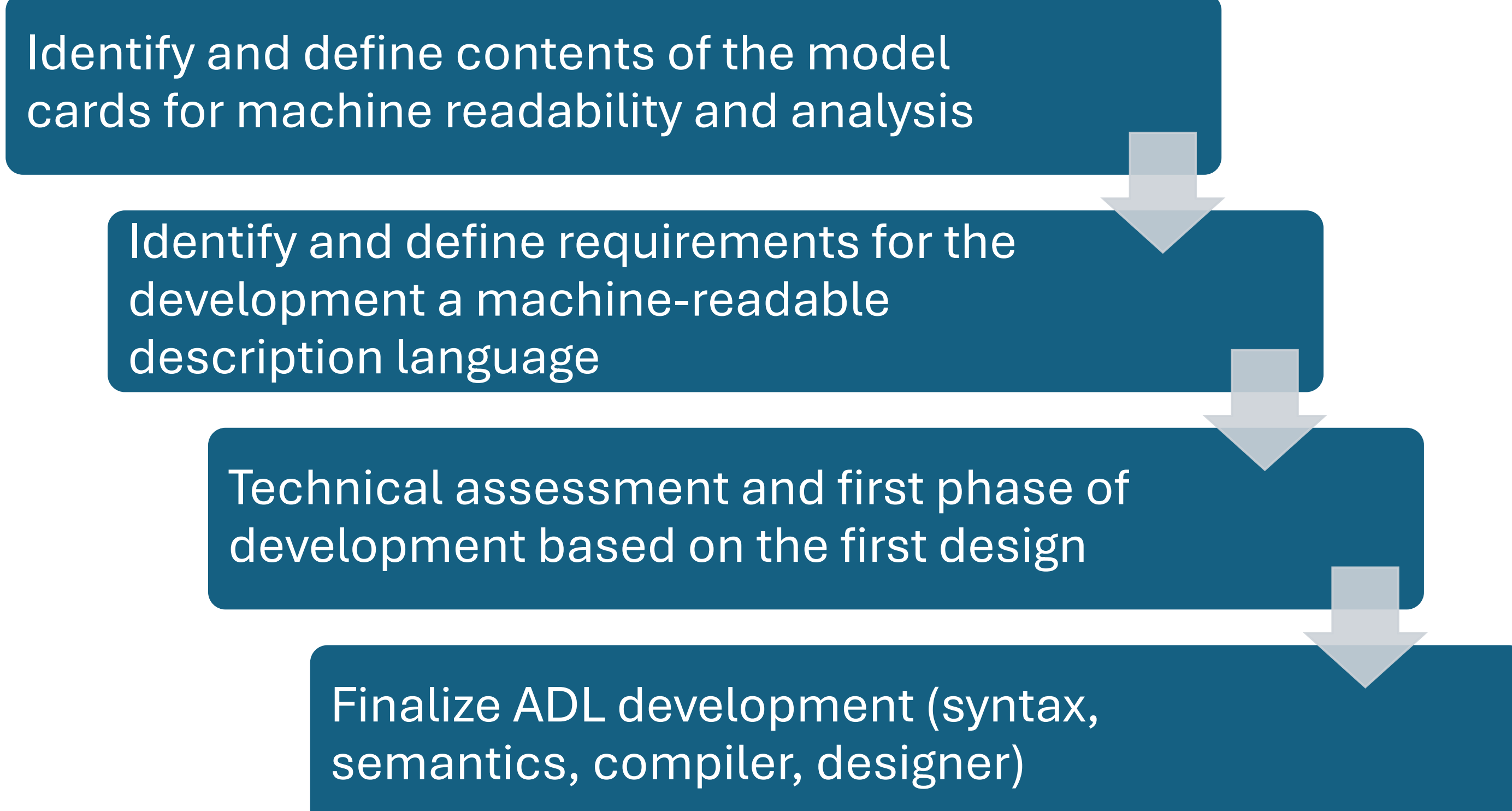


Ongoing work

- Investigate the content of the existing model cards.
- Define the content of the model cards for machine readability and analysis.

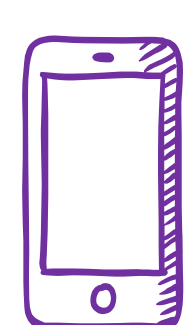


Approach



Next steps

- Comparison of the proposed model card content with the previous versions.
- Define requirements for the description language in form of a vision paper.
- Define semantics of the description language.



Contact Information

Ali Mehraj
Tampere University
ali.mehraj@tuni.fi



Connect to LinkedIn