Typ der Arbeit

- Projektarbeit

Titel
Increasing trust in AI systems
Beschreibung
This year or next, an EU regulation is to be enacted that will require a certificate from an independent body for AI systems that are used in safety functions. There are already approaches on how AI systems are to be developed and tested, although these have so far been limited to questionnaires on the part of the certifiers. The next step should therefore be to enable certification on a technical basis, to which this work makes a contribution. This work can be carried out as follows: 1. familiarisation with the topic of trustworthiness and certification of AI systems 2. derivation of the necessary measures for a safe AI system (robustness, transparency, adversarial attacks) 3. implementation of an AI system (alternatively: adaptation of an existing system) taking into account the given development methods 4. planning of the verification of the system 5. testing of the system using suitable methods The possible use case will be defined in accordance with one industry partner.
Voraussetzungen
Basic knowledge in Machine Learning, interest in the interaction between implementation and related processes, methods, tools
Studiengang
Informatik
Institut / Zentren

- Institut für Angewandte Mathematik und Physik (IAMP)

Interne Partner

- Keine