Zurich University of Applied Sciences

certAInty – A Certification Scheme for AI systems (Innosuisse Project)

Centre for Artificial Intelligence (CAI)[1]
Institute of Applied Mathematics and Physics (IAMP)[2]
CertX AG

ricardo.chavarriaga@zhaw.ch[1] monika.reif@zhaw.ch[2]
frank-peter.schilling@zhaw.ch[1] joanna.weng@zhaw.ch[2]

Background:

The European Commission will adopt the Artificial Intelligence Act in early 2023. It will introduce a common regulatory and legal framework for artificial intelligence, covering all sectors (except military) and all types of artificial intelligence.

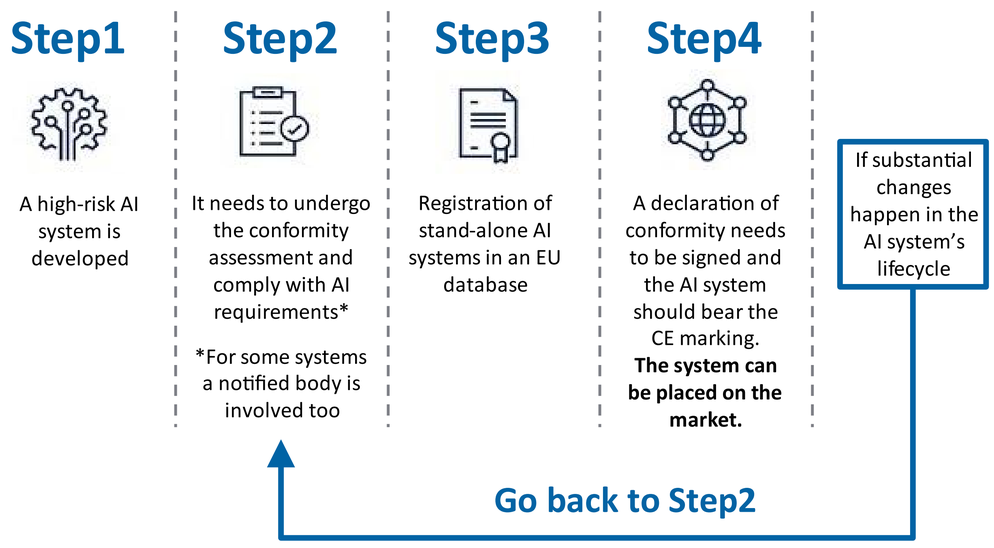

Figure 2 – The certification steps for high-risk AI-based systems (source: EU Artificial Intelligence Act)

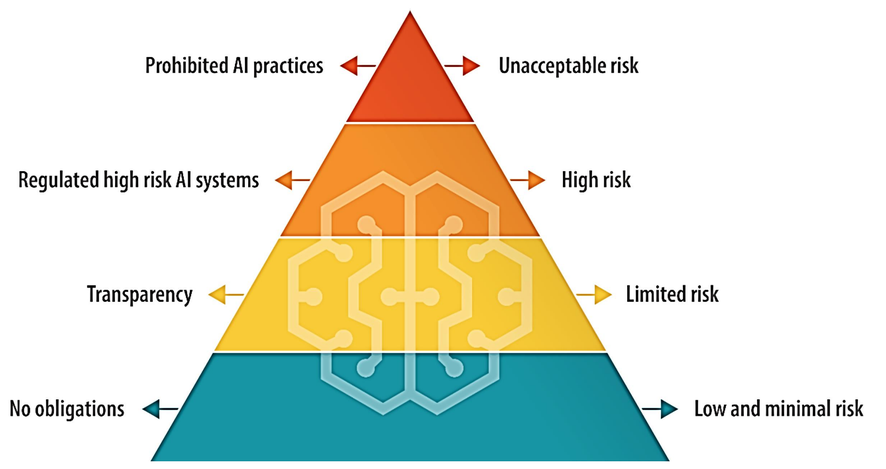

Figure 1 - The EU AI Act thus introduces a "product safety framework" around 4 risk categories.(source: EU Artificial Intelligence Act)

The AI act imposes requirements for market entrance and certification of high-risk AI-based Systems through mandatory CE-marking defining:

- Certification dimensions, e.g.: autonomy and control, transparency, reliability, and safety
- Certification workflow

Goals:

- Certification Scheme for AI-based systems, comprising specific requirements, criteria and measures
- Suite of technical and scientific methods for verification of relevant properties of the AI-based system which are required to enable the assessment of the compliance with relevant standards.

Approach:

- Certification of products and corresponding processes (including data, development, model, testing, operation)
- Considering all stakeholders such as developer, user, auditor, authority,…
- Covering the complete AI lifecycle

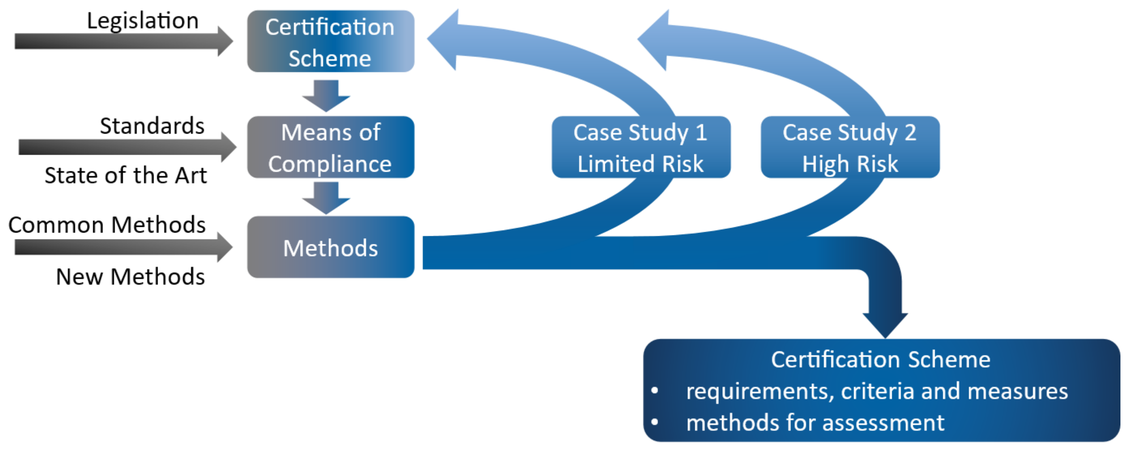

Figure 4 – The iterative approach for defining a certification scheme for limited-risk and high-risk AI-based systems

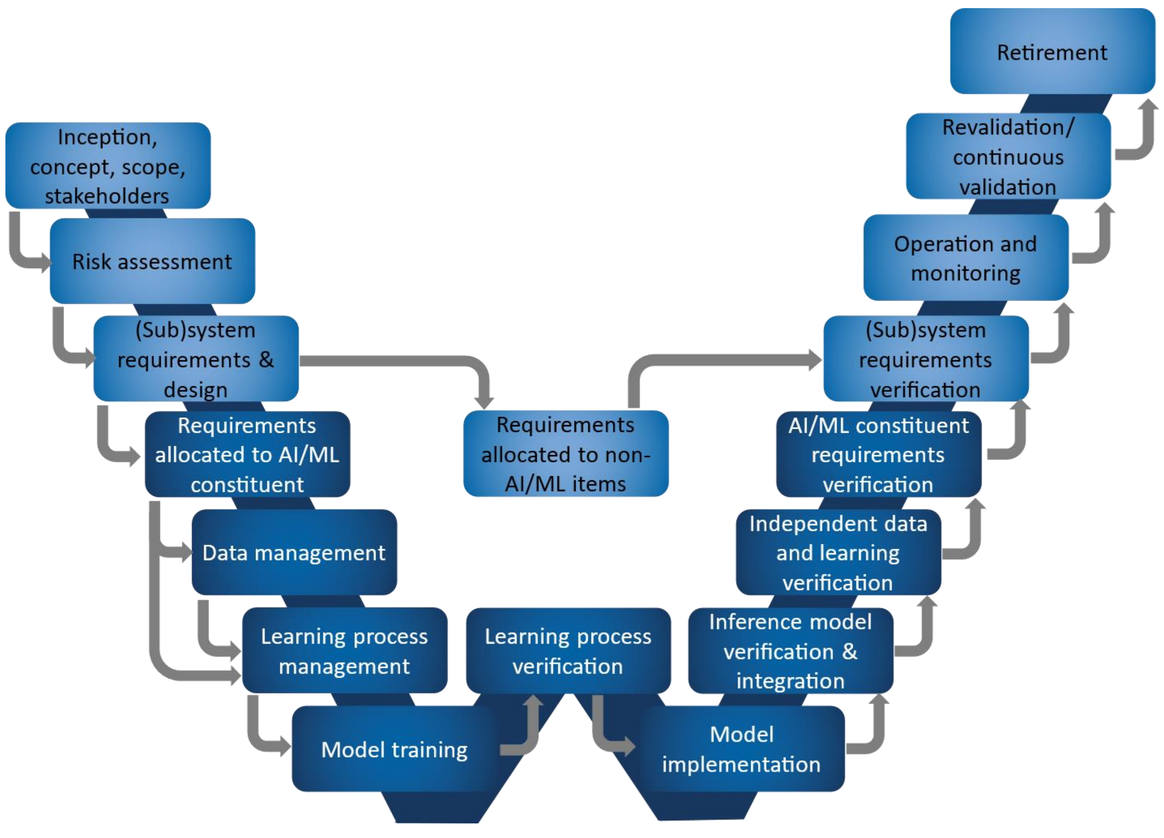

Figure 3 – The AI-based system lifecycle (source: EASA adapted)

An iterative approach is used:

- Starting from a first draft of the certification scheme, including the main objectives for achieving conformity with EU legislation, we identify the associated means of compliance based on the current state of the art
- Then, technical and algorithmic methods to assess certification requirements are identified and improved
- The certification scheme and corresponding methods will be evaluated in use cases of limited and high-risk categories, yielding a fully validated solution.