Position paper

The AI Act – An Investigation in Examples

14. February 2022

While we welcome the risk-based approach for the regulation of AI followed by the commission, we also expressed concerns regarding two fundamental points of the file, namely the definition of AI and the classification of high-risk[1]. The accurate capturing of what systems are AI and which of those pose a high risk is central to having an efficient and purposeful regulation of the technology within the European Union. As the Explanatory Memorandum of the AI Act states:

> *"The use of AI with its specific characteristics (e.g. opacity, complexity, dependency on data, autonomous behaviour) can adversely affect a number of fundamental rights enshrined in the EU Charter of Fundamental Rights ('the Charter')." (p. 10)*

We see that the described characteristics associated with AI can have negative consequences for fundamental rights and understand that these need to be addressed appropriately. However, we do not see the specific nature of the systems which can have such adverse impacts completely reflected in the definition of AI system in Article 3. Similar holds for the classification of high-risk. Although, the specific use cases are aimed at capturing only those AI systems that pose a risk "of violation of fundamental rights and safety of people", in our understanding this is not entirely achieved by the commission's proposal.

To show where our concerns are coming from, we below display a list of examples that was collected based on our understanding of a high-risk AI system according to the commission's proposal of the AI Act from 21. April 2021 (explicitly Articles 3 and 6, as well as Annexes I, II and III). The table is structured in two parts, based on the distinction in Annex II and III. In the first part of the table, the examples are either understood as a 'safety component' as defined in Article 3 or as products themselves falling under the legislation in Annex II. Additionally, the product containing the safety component or the example itself as a product needs to undergo a third-party conformity assessment. In the second part of the table, we list examples that in our understanding would fall into one of the use cases displayed as subpoints in Annex III. The table consists of four columns:

1) The example is described.
2) The form of implementation as it occurs in Annex I is specified.

Bitkom e.V.

Merle Uhl
Referentin Künstliche Intelligenz & Digitalisierung
T +49 30 27576-242
m.uhl@bitkom.org

Lukas Klingholz
Leiter Cloud & Künstliche Intelligenz
T +49 30 27576 101
l.klingholz@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

[1] https://www.bitkom.org/Bitkom/Publikationen/Bitkom-principles-for-the-Artificial-Intelligence-AI-act

3) For Annex II examples: the relevant legislation and whether it is understood as safety component or product itself is stated. For Annex III examples: the specific use case that we understand the example to fall into is stated.
4) Our considerations of why we have concerns classifying the example as high-risk AI system.

Why we question an example's categorization as high-risk AI system based on our understanding of the AI Act has potentially two reasons:

- Either, the example is in our understanding not AI in the sense that it comes with characteristics which potentially can affect fundamental rights in a way that would call for specific requirements
- Or, we do not see that the AI systems poses "a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights" that calls for the requirements formulated in the AI Act

We would hope to start a discussion based on this collection of examples and the associated considerations - to better understand the legislative proposal and its intention, as well as its targeting and, thus, successfully implement the risk-based approach. We also intend to use some of these examples to kick-off an exchange on the user-provider-relationship. They already outline some of the uncertainties we see us confronted with regarding the distribution of responsibilities within the value chain of an AI system.

Basis for Categorization

Article 3 - Definitions

(1) 'artificial intelligence system' (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

(14) 'safety component of a product or system' means a component of a product or of a system which fulfils a safety function for that product or system or the failure or malfunctioning of which endangers the health and safety of persons or property;

Article 6 - Classification rules for high-risk AI systems

1. Irrespective of whether an AI system is placed on the market or put into service independently from the products referred to in points (a) and (b), that AI system shall be considered high-risk where both of the following conditions are fulfilled:

(a) the AI system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonisation legislation listed in Annex II;

(b) the product whose safety component is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment with a view to the placing on the market or putting into service of that product pursuant to the Union harmonisation legislation listed in Annex II.

2. In addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk.

+ Annex I

+ Annex II

+ Annex III

Annex II

	Example	Listed in Annex I	Listed in Annex II	Explanation
1.	Development of assistant tools for oncologic diagnoses (MRI, immunohistochemistry, etc.) using machine learning approaches	(a) Machine learning	A. 11./12. Product	Assistant tools could be developed using machine learning methods to a level of satisfactory performance and then be finalised (NO learning during use, static algorithm). Although, such a tool would not substantially differ from conventional software considered a Medical Device or IVD (AI use only for development), it would per Art. 6(1) be considered a 'high-risk' application with all related requirements.
2.	Medical devices, Picture Archiving and Communication System (PACS) that supports healthcare professionals in diagnosis by providing examination data (such as images) with parallel loading of a patient's prior and current examination data, based on patient identifiers.	(b) Logic-based approach	A. 11. Product	Matching examinations to patients and prior examinations to current examinations is done by using patient identifiers, patient names, and information on examined body parts and imaging modality. This matching is performed through queries to the underlying database of the PACS. According to Art. 6(1), this device would be classified as 'high-risk' AI, which we consider to be an inappropriate classification and resulting regulatory treatment.

3.	Medical devices, Radiological reporting software: Report creation with predefined report templates and automatic population of image-based findings for structured and free-text reporting	(b) Logic-based approach	A. 11. Product	Radiological report templates are configured in the software system, and any observations or findings made by the healthcare professional on a patient's images can be automatically filled into the reporting template, following a structured report format. According to Art. 6(1), this device would be classified as 'high-risk' AI, which we consider to be an inappropriate classification and resulting regulatory treatment.
4.	Medical devices, medical decision-support software	(b) Logic-based approach	A. 11. Product	The software is processing medical information (e.g. laboratory values) and calculates a risk-scoring of a possible disease or determines the most prone treatment recommendation for review by healthcare professionals. Note: those systems, are on the market since the late 70s and under certain conditions exempt from pre-market controls in the USA. According to Art. 6(1), this device would be classified as 'high-risk' AI, which we consider to be an inappropriate classification and resulting regulatory treatment.
5.	Medical diagnosis system	a) Supervised learning systems, b) Expert systems	A. 11. Product	Computerized systems often include AI algorithms to automate workflows, to facilitate speech-to-text or visualize and present information that is to be checked for plausibility by a physician. We are questioning that such non-autonomously acting systems shall be classified as high-risk AI system, because AI is not taking any decision, just making the workflow more efficient.
6.	Rule-based control of individual hardware components (e.g. automatic gear shifts, electric energy deployment)	(b) Expert system	B. 2./3./6. Safety component	Many individual hardware components require specific control software. The software controls the behavior using fixed logic based on clearly defined rules that are designed by experts. Such software is already used for quite some time in most individual hardware components integrated into vehicles operating on public roads and cleared by regulatory bodies. We are questioning if classifying such logic-based expert systems (where the control roles are simple and

				clearly defined) as AI systems is the intention of the AI Act.
7.	Filter techniques to limit sensor uncertainty from statistical noise	(c) Statistical approaches	B. 2./3./6. Safety component	Kalman filtering is used on many occasions to more accurately estimate a system state under noisy measurements. When operating a sensor under real conditions all measurements include statistical noise or other inaccuracies. The reliability of sensor data can be improved by incorporating knowledge of previous time frames instead of only using the current sensor reading. The rules for the estimation are clearly defined before-hand by experts and such filter are in-use for a long period of time in both complex systems (spacecrafts, etc.) and for uncritical, comfort tasks (wheel rotation, localization for map service etc.).
8.	A Radar Transceiver as a component in a car filters signals from outside the car to enable e.g. an automated cruise control or an automatic emergency stop. - An AI-based algorithm is used in this component to pre-filter radar signals and do a first plausibility assessment of the received data.	(b) Inference	B. 6. Safety component	The Radar Transceiver itself does not trigger the brake, it provides pre-processed data e.g. to a tier-one product doing so in the final OEM product / car. It is not clear whether the Radar Transceiver company (Tier 2) is regarded as producer, manufacturer or third party of a high-risk AI system. If it was to be seen as a provider of high-risk AI, the obligation of post-market monitoring could not be fulfilled since field-data do not flow back to Tier 2. Potential risk can arise rather in the design of the full car, depending on how the pre-processed radar signals are being processed and integrated in the car system. This is beyond the reach of Tier 2. Also, the deterministic functionality of the algorithm in this safety context makes us question if capturing such use cases is the AI Acts intention. A clear differentiation to high-risk systems which are still learning in the field would be needed.

Annex III

	Example	Listed in Annex I	Listed in Annex III	Explanation
9.	Automated systems that set temporary speed limits in order	ALL. (a), (b), (c)	2. (a) AI systems to be used as	Although such systems are supposed to increase safety levels, there is no obvious substantial risk involved in malfunctions (especially compared to

	to optimize traffic flows		safety components in the management and operation of road traffic [...]	not having such systems or using less evolved ones). Furthermore, fairness or explainability are not required; adversial attacks are extremely unlikely and associated with potentially minor consequences.
10.	Predictive Maintenance for Network Assets	(a) Machine learning approaches	2. (a) AI systems intended to be used as safety components in the management and operation of [...] electricity.	Predictive Maintenance uses machine learning to predict if an asset of the electrical network is likely to fail in the near future. With this information, we optimise the asset replacement strategy to minimise the occurrence of failures. This helps spend the budget allocated by the Distribution System Operators (DSOs) for their asset replacement effectively. With our algorithms, we help to select assets with the highest risk of failure, on one hand, and components that would have the worst consequences in the case of failure, on the other hand. In this sense we understand it to fulfil a safety function but would question the classification as high risk.
11.	Vegetation Management along Power Lines	(a) Machine learning approaches	2. (a) AI systems intended to be used as safety components in the management and operation of [...] electricity.	Management of vegetation in power distribution is a mandatory operation to ensure a reliable supply of electricity and public safety. Trees that are too close to the power lines represent a significant hazard, putting human life and the environment in danger and are a leading cause for power outages. Each operator develops its own tree trimming management plan in compliance with legal requirements. Legacy approach of assets inspections is slow, resource intensive mostly with visual inspections and ground field surveys and often based on fixed annual cycles. A new digital vegetation management process via cloud-based artificial intelligence and machine-learning algorithms can make this process more efficient. The AI helps to structure the data coming from a variety of data sources (ground inspection, aerial imagery, drones, LiDAR, satellite) and to extract insights by turning raw data

				into actionable intelligence based on current status as well as on forecasts and predictions of vegetation (tree species, weather data, historical patterns, etc.). The use of AI enables to optimize planning of trimming on a condition-based approach built on predictive models which detect potential hazards before they occur. While we consider it to fulfil a safety function, we would question the classification as high risk if it only complements the existing vegetation management.
12.	Task-routing tools. Among other functions, these tools allow the automatic routing of calls from a German number to a German-speaking customer service agent.	(a) Machine-learning approaches	4. (b) AI intended to be used for [...] task allocation	Task-routing tools would be captured by the scope set out in Annex I. However, they cannot alter the tasks for which they have been set up and, in our understanding, do not pose any risk of the dimension that is to be addressed by the AI Act.
13.	AI-based allocation of logistic routes to individual trucks / truck drivers	ALL. (a), (b), (c) – mostly optimization and/or machine learning	4. (b) AI intended to be used for [..] task allocation	The risk involved for the subjects is in our view limited, and the chance of biased, unfair allocations would be significantly higher as a result of manual processes due to the inherent mathematical complexity of logistics use cases.
14.	Automated claims handling (e.g. in travel or insurance).	ALL. (a), (b), (c) – mostly optimization and/or machine learning	4. (b) AI intended to be used for [..] task allocation	Those solutions' sole purpose is process optimization and customer convenience. If a claim cannot automatically be handled to the extent a customer wants it to, it is automatically allocated to an employee who then deals with the claim in the traditional way. The associated risk in the sense of the AI Act is in our view limited.
15.	Models used in online shops in order to determine eligibility to use different payment methods	(a) Machine learning	5. (b) AI systems intended to be used to evaluate the creditworthiness of natural persons	The risk to sell on credit is mainly with the seller whereas the customer has a comparably small potential disadvantage of less convenient payment methods as long as he is not denied business. Thus, a "high risk" categorization can be questioned.

Bitkom represents more than 2,700 companies of the digital economy, including 2,000 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.