SIEMENS

EU's AI Regulation proposal (21/04/2021)
Position & recommendations

Introduction

We recognize the European Commission's effort to propose world's first AI regulation, building on its last year's White Paper and aiming at ensuring that AI systems, introduced on the EU market are safe and respect EU laws and values while at the same time creating legal certainty to facilitate investment and innovation in AI.
On the other side we question whether such a horizontal regulation at this point in time, would not hinder innovation due to overregulation. Innovation using AI may consequently be realized and employed outside of the EU, hence this technology is more likely to advance faster in markets outside of Europe. European SMEs or Startups would also be discouraged from developing AI applications in the EU when the regulatory requirements and obligations are so burdensome.
Since today the development of AI applications is still in an early phase, it is certainly difficult to phrase an appropriate legal framework for all kinds of AI applications, especially in the B2B area.
At Siemens, we have been using AI for many years in a wide variety of technology areas, as illustrated in Fig 1.

Fig 1: Application fields of industrial AI at the Siemens

Since several years, we have been consistently contributing actively to the AI policy discussion via several consultations, expert groups, and discussions with European Commission and European Parliament experts. In a policy field mostly dominated by a Business-to-Consumer (B2C) narrative and global competition, Europe has a great opportunity to become a leading player within the Industrial AI and Business-to-Business (B2B) domains, built on upon Europe's strong industrial base.
At this point we need to underline that the Industrial AI market is posing tremendously different challenges from those in the internet market (Web AI) as we illustrate in Fig 2.
Industrial AI applications present great opportunities that can contribute to resolving major challenges facing society, with clear positive examples in the power and mobility sectors (including autonomous driving), industrial manufacturing, critical infrastructure and building automation.

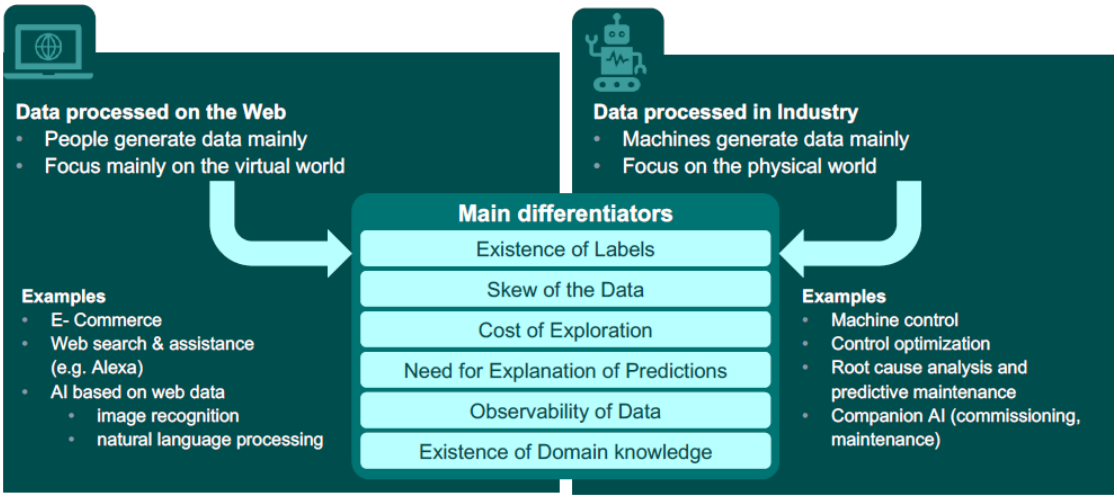

Fig 2: Main differences between Web AI and Industrial AI

At Siemens we are proud of the way we are using trustworthy AI to enhance human capacities, not to replace them but rather supporting, empowering, and augmenting them.
In our view, Data & AI are THE means – instruments or tools - to go to a circular economy and to achieve the twin green and digital transformation of industry for the benefit of people, planet and prosperity.
AI applications in the industrial domains, addressed by Siemens show a very broad variety of application tasks with many grades of complexity and autonomy like e.g.:

- visualizing existing data to make it more understandable (e.g. sales performance, dashboards, trends & spikes, ...)
- detecting or recognizing patterns or objects in data by classifying them (e.g. anomalies, objects, ...)
- predicting future states and events from current and historical data (e.g. weather, system failure, ...)
- recommending actions or decisions to a human operator (e.g., navigation, maintenance schedule, ...)
- autonomously controlling and operating an end-to-end decision process (e.g. collaborative robots, autonomous driving,...)

More examples in many application areas and further Siemens AI news can be found here:
https://new.siemens.com/global/en/company/stories/home/artificial-intelligence.html
https://ecosystem.siemens.com/ailabarea

All these examples illustrate that a risk (and the New legislative Framework - NLF) based approach, as have been taken in this regulation proposal is the right way forward because there is no horizontal "one-size-fits-all" solution for the wide range of AI applications. The risk level should be objectively determined by the criticality of the application itself (and not by sector).

In general, we advise to carefully analyze all potentially unwanted consequences, side-effects, and administrative burden for industry, that specific proposed regulation articles might cause as this could lead to hindering innovation in this fast-evolving technology area and thus putting European industry in a competitive disadvantage compared to our global competitors.
On the following pages we provide our initial feedback for the European Commission's consultation on this AI regulation proposal, while underlining that we will further contribute- also via sector specific feedback and positions- to the upcoming policy discussions during the legislative process in the coming months ahead of us.

Siemens' assessment and main recommendations

Siemens main recommendations

- **We welcome the risk- and NLF-based approach**
- **An additional principal objective of this Regulation must also be to facilitate authorization of AI applications.**
- **Keep the scope "narrow" enough, to real AI systems, avoid including conventional algorithms or statistical methods in the scope that could increase legal uncertainty and harm global competition. A more precise definition what is AI is required and will be key – see our concrete proposal below.**
- **Make use of the already existing quality management system such as defined by ISO 9001, instead of setting up a separate, dedicated AI quality management system**
- **Avoid any unrealistic absolute requirements, like e.g. data sets that need to be free of errors and complete.**
- **No need to deviate from existing NLF conformity assessment procedures, widely established in industry, hence no support for a mandatory registration of certain AI systems (it is not an element of conformity assessment nor is it necessary or proportionate), Also in-house conformity assessment bodies must be allowed to assess the conformity of AI systems/applications. The NLF already provides for the possibility to use in-house bodies for the performance of conformity assessment.**
- **Lessons learned from sandboxes shall be taken into account in amendments and updates of the regulation**
- **Include a balanced industry representation in the envisaged European AI Board**

Detailed assessments and comments

General:
Siemens welcomes the risk- and NLF-based approach taken by the European Commission

Title 1 General Provisions (incl. Annex I):

- The **proposed definition for AI system** (see Art 3 and Annex I)) **is arbitrary and too broad**. In particular, the definition does not support the necessary distinction to be made between AI systems and "conventional" logic units.
    - According to the list of AI techniques and approaches in Annex I, even conventional logic programming and statistical methods will be considered to be AI.

- A rule that filters the entries of an Excel spreadsheet for specific criteria or conventional logical programs used in industrial applications for many years for example would be considered as AI according to that definition.
- Consequently, **many existing software solutions will be considered to be AI systems, which increases legal uncertainty for manufacturers and users** and is harmful in global competition.

- Proposal for a definition of an AI system, partly referring to ISO/IEC DIS 22989, 3.1.2 and 3.1.26:

  "'artificial intelligence system' (AI system) means software that is developed with one or more ~~the techniques and approaches listed in Annex I and~~ methods or automated entities that apply a model, representing a physical, mathematical or otherwise logical representation of a system entity, phenomenon, process or data, so that the system can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."
  Rational for this proposal:
  - It is defined technology-agnostic
  - It is aligned with ongoing international AI standardization activities
  - By highlighting the application of a model which refers to some kind of representation of the real-world, the definition introduces a differentiation from pure software systems as well mentions explicitly one important source of risk / uncertainty
- In addition, because the actual definition of an AI system would also include the broadly used industrial "conventional logic units" (so-called PLCs) without any AI software, unjustifiably burdening these with additional obligations, we propose to exclude such "conventional logic units" (without AI software) expressis verbis from the proposed AI Regulation by including following text added to Article 3:

  "This Regulation does not apply to hard-coded and rule-based software systems that rely solely on human software engineering skills (i.e. not generated by data-based learning techniques), such as logic units with "conventional" (non-AI) embedded and/or application software that ensure safety functions."

- In order to **achieve alignment with the NLF** and avoid overlap with the definition of 'making available on the market' article 3 (11) should be modified as follows:

  "putting into service": means ~~the supply of an AI system for~~ the first use by the intended ~~directly to the~~ user or for own use on the Union market for its intended purpose.

- Also, further considerations are necessary to determine whether the concept of "reasonably foreseeable misuse" (Article 3(13)) such as applied under safety related product legislation, can be transferred 1:1 to the supply of AI systems.

- The definition of the term "safety component" is too broad in its current wording. Safety components should focus on the health and safety of persons but not of property. The AI regulation should be aligned with the machinery directive in this respect, which does not mention property in its definition.
  Therefore, we propose a rephrasing Art 3 (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~~ so that its failure or malfunctioning endangers the health and safety of persons ~~or property;~~*

Title III High risk AI Systems (incl. Annex II - VIII):

- We strongly advise not to consider AI in critical infrastructure automatically as High-Risk but only when health, safety & security are at risk.
- Article 6 (1) classifies an **AI system** that is intended to be used as a safety component of a product, or is itself a product, covered by specific Union harmonization legislation and that product **is required to undergo third-party conformity assessment as high-risk AI system**. It **should be ensured that this does not lead to the overall promotion of third-party conformity assessment** just for the sake of achieving the classification of high-risk AI systems.
- We advise to restrict the Annex III High-Risk applications on education & employment 4 (and 3) to situations without final human decision making (not all automated filtering of CVs is per se high risk). If the EU imposes high-risk regulation requirements on filtering applications so broadly, technology is more likely to advance faster in markets outside of Europe. Hence, companies might be inclined to buy such services from non-EU players since they can develop their software much faster and with more and live data (and then comply to EU-regulation once the system is developed outside). Non-EU players are already well advanced on the topic (e.g., https://eightfold.ai/). European SMEs or Startups would be discouraged from developing such AI applications in the EU when the regulatory requirements and obligations are so burdensome in comparison. Potential threat to Siemens/EU includes development of AI system that detects our key talents via externally available information.
- Chapter 2 defines various requirements for high-risk AI systems. Several of these requirements are still topics of active research and concrete approaches for achieving these requirements might not be available depending on the specific AI technique. Furthermore, the overall expenditure caused by these requirements needs further investigation whether and in how far they are proportionate
- Article 9 requires and defines a **risk management system for high-risk AI** systems. The current **definitions are not specific** on the kind of risk that has to be considered. As the type of risks can be manyfold (e.g. financial risks, risk of delays in development) and many of them are not relevant for this regulation, **a specific** definition of the risks that have to be considered by this risk management system **must be added**.
    - We **advise to amend paragraph 2 (a),** in order to define the concrete risks that shall be considered by the risk management system: *"(a) identification and analysis of the known and foreseeable risks **to the health and safety or fundamental rights of persons** associated with each high-risk AI system."*
    - Furthermore, also to **stay in line with the well-established NLF concept**, it should be **sufficient to require a documented risk analysis and assessment**, rather than a full-blown specific risk management system, which leads to unnecessary additional costs and burden.
- Article 10(2) and 10 (5): bias in its generic meaning as a systematic difference in treatment of certain objects, people, or groups in comparison to others is essential for proper AI system operation (e.g. classification). The critical issue is unwanted bias that effects the output of AI systems in a harmful way resulting for example in unjustified favoritism and discrimination. Considering and avoiding all kind of bias is not necessary and even counterproductive, in particular for machines. Therefore, the more precises term "unwanted and harmful bias" should be used in the regulation.

- Article 10 (3) requires that **data sets shall be free of errors and complete**. These **are unrealistic absolute requirements** which raise many questions and issues, especially in the B2B area; as example, closed loop algorithms are never complete.
    - What would be considered as error for data sets, error in the classification, errors in the data, errors in the correct representation of the intended behavior?
    - The efforts for minimizing errors in the data sets has to be balanced against the actual benefits.
    - For testing and validation, data sets with errors have to be explicitly used.
    - What would be the threshold for completeness of data sets?
    - Training with too much data sets could result in overfitting
    - Requirements for data governance and management practices (for the training, validation and testing data sets) should not be laid down in the Regulation, but should be left to standardization, also to ensure that the relevant requirements keep step with the development of the state of the art.
- In Art 11 the level of technical detail required, seems too excessive. Technical details should be left to standardization. In particular, concerning Annex IV (5): this point should be deleted. The requirement is disproportionate and impractical as it includes "any change to the system" and "through its lifecycle". There is no reason, why this should be required for the technical documentation
- Article 12: record-keeping for High-Risk AI systems will require that a long history of information has to be stored for analysis. Collecting and storing this type and amount of information could get in conflict with the overall goals of increasing energy efficiency and remaining compliant with data privacy. Additional data protection mechanism might be required.
- It is questionable whether the comprehensive and very demanding requirements for human oversight by natural persons as set out in Article 14 do not hinder the objectives and the further development of AI systems
- It is necessary to clarify that the obligations for providers to maintain a specific QMS and risk management system (Articles 17, 9) end when the provider decides to end the service/support of the (high-risk) AI systems concerned. Likewise, it is necessary to clarify that the obligation to carry out corrective action and to ensure accuracy, robustness and cybersecurity (Articles 15, 16) of products already placed on the market ends at the expiry of the products lifetime / support time as defined by the provider.
- The concept of ensuring **accuracy, robustness and cybersecurity** of high-risk AI systems "throughout their lifecycle" is new with regard to the NLF and extends the responsibility – and potential liability – of the provider/manufacturer beyond what is under his control. The possible consequences of such a far-reaching concept would imply major hindrances to the development and supply of AI systems. **We recommend that the obligations should be related and limited to the point in time of placing on the market/putting into service – very critical for us!**
- The **levels of "accuracy, robustness and cybersecurity**" as required for high-risk AI systems under Article 15 **should be made subject to what "can be reasonably expected**" (cf. product safety legislation) as market expectations differ regarding software as opposed to hardware products.

- The requirement in relation to “feedback loops” for high-risk AI systems that continue to learn (Article 15 (3)) covers a very specific aspect of such systems. AI systems that continue to learn after being placed on the market or put into service have various issues in relation to robustness but also to conformity assessment in general. Picking just one specific issue does not cover such systems appropriately in the regulation. In general, more detailed considerations and even further research is required to address continuous learning AI system in an appropriate way, therefore we advise to exclude these at this point in time. Furthermore such technical details should be left to standardization.
- Fulfilment of the obligations placed on "providers" under Article 16 (e.g. Quality Management System, registration obligation,..) is not related and limited to the point in time of placing on the market/putting into service, as is the case for the legislation based on the NLF but appears to extend beyond the placing on the market throughout the entire lifecycle. It **must therefore be ensured that the providers may decide on the end-of life of their products/services to the extent they inform their customers within a reasonable timeframe (prior notice). Only as long as they provide the services, they need to comply with their duties/obligations.** We recommend additional text to clarify that the obligations apply only to the extent that providers actually exercise control over the products/AI systems.
- The detailed requirements for a QMS set down in Article 17 are overly prescriptive as, for high-risk AI systems, these are already inherent in the required risk management system (Article 9) and in the obligatory conformity assessment procedure. There is the risk that this additional Article only leads to need for additional certification without any tangible benefits in terms of safety or protection of other public interest issues (e.g. data protection, privacy).
- The obligation for the provider of high-risk AI systems of **putting in place a quality management system according to Article 17** shall not impose a dedicated AI quality management system but **should be covered by existing quality management system such as defined by ISO 9001.**
- Concerning Article 24, we recommend further clarification that the AI system provider remains responsible for the compliance of his AI system (in addition to the responsibility taken by the product manufacturer)
- Authorized representatives (Article 25 (1): “Appointment of authorized representative by written mandate, if an importer is not available and the provider is outside the EU”. To ensure consistency in the implementation of legislative requirements (from Annex II and this draft Regulation), reference should be made to the Market Surveillance Regulation 2019/1020/EU, rather than introduce a specific Article with slightly deviating contents
- In order to ensure that the harmonized standards (Article 40) are available when the regulation comes into force, standardization requests to the ESOs shall be issued in a timely manner.
- In the exceptional case the **common specifications** are adopted (article 41), **all relevant stakeholders must be consulted and involved** in the development of such common specifications
- Article 41(4) needs to be corrected in line with the NLF (Standards or Specifications are not mandatory!) as follows:
  “Where providers do not comply with the common specifications referred to in paragraph 1, they shall duly justify that they have adopted technical solutions that meet the requirements referred to in Chapter 2 to a level ~~are~~ at least equivalent thereto.”

- Article 44(2) on QMS certificates: The extent of re-assessment needs further clarification. Is it still necessary if the AI system is still in use by the user or is it only necessary if it will be "manufactured" by the provider? Furthermore, it should not be the task of the legislator to provide for a maximum period of validity of certificates. Rather, this should be left to standards and rules of the certifiers, based on the specific risk potential of the products in question.
- Article 44(3) – The provisions in this paragraph are problematic with regard to the detailed requirements in Article 17 concerning the QM-system and the need for it to ensure the requirements of the Regulation throughout the product's lifecycle (Articles 9, 15). It should also be clarified that the termination of production and the ensuing termination of the QMS and risk management system for the AI systems concerned does not invalidate the certificates issued for those systems.
- We **welcome, in principle, the NLF based approach** of chapter 5. However, **we do not support the introduction of an obligation for registration of certain AI systems as foreseen in Article 51**. Such a registration obligation **is neither an element of conformity assessment** under the NLF **nor is it necessary or proportionate**, in particular considering the information that has to be provided together with the registration according to Annex VIII.

Title V Measures in support of innovation

- Art 53-54: The **legal basis for regulatory sandboxes should be** r**epresented by experimentation clauses** in accordance with the Council's communication (11/2020)**, that have already been used by many member states**, to be activated on a case-by-case basis in order to guarantee flexibility.
- Art 55: We welcome the proposed measures for SME's and Startups, but **not only size of the company is important**; in our view **also the impact of the AI system** (on society, environment, and business) **and its market relevance** has to be taken into account.

Title VI Governance

- For the **envisaged European AI Board** according to article 56 to 58 to be successful, it is important that the Board **is a true public-private collaboration and includes industry representatives (or associations)** on an equal footing with public stakeholders

Title VIII: Post-Market monitoring

- Article 61 should be removed or at least significantly reduced, since it implies only additional burden for each provider. Not all AI systems can be monitored, especially if it is a product with an integrated AI system. (e.g. autonomous cars: if there are 1mio cars with embedded AI systems, the provider would have to monitor each of these AI systems, because all AI systems are generating data independently. How should this be feasible?)

Contact:

Dr. Eddy Roelants
Siemens
Government Affairs Office
Montoyer 47 – Floor 6
1000 Brussels
Belgium