Siemens Energy Position and Recommendations on European Commission's proposal for an EU regulation on AI 21 April 2021

Introduction

We, at Siemens Energy, welcome the work the European Commission has done in the past few years aiming at creating the world's first AI regulation, which resulted in the proposal of the AI Act published on 21st of April 2021. We appreciate the time taken by the European Commission in consulting the various stakeholders, and, specifically, appropriately listening to the industry, the key strength of Europe, in creating the proposal. Nevertheless, from our Industrial AI point of view, in particular for the energy domain, the proposal can be improved on few aspects.

In the following paragraphs, we describe our position and few recommendations:

On the horizontal approach

Whereas a horizontal approach is helping in having harmonized rules across Europe, we need to ensure that these regulatory aspects will not hinder the speed of development in EU. This is key to create expertise in EU, develop the economy and employment, and add value to Europe, leverage the strength of EU to contribute to the global targets.
In a discussion mostly dominated by Business-to-Consumer (B2C) narrative and global competition, Europe has an absolute key differentiator with the Industrial AI combined with Business-to-Business (B2B) domains, built on top of more than 20 years of knowledge. AI applications as crucial part of the Internet-of-Energy presents vast opportunities that can contribute to resolving major challenges facing society in the energy transition. To leverage this strength of Europe and contribute to the ambitious global climate targets, Europe should aim at speeding up the development of AI solutions in the EU. As relevant example, of key importance for the energy sector, AI not only plays an essential role in the decarbonization of energy eco-systems, but also enables the consumers', operators' and OEMs' autonomous decision making to access reliable, low-cost, sustainable energy.

On the risk-based approach

We welcome the risk-based approach since there is no "one-size-fits-all" solution. Having a list of high-risk use cases is significant in giving focus and clarity to the legislation. However, the list should be under continuous assessment, with a clear procedure, making sure that accidental inclusion of non-critical or insignificant, harmless, AI systems are avoided.

Furthermore, the use of real-time biometric recognition systems as high-risk use case should not be horizontal; we advise to assess its industrial use in AI systems case-by-case.

We also advise not to consider AI in critical infrastructure *automatically* as high-risk, but only when health, safety & security are at risk.

The proposal to ensure accuracy, robustness, and cybersecurity of high-risk AI systems "throughout their lifecycle" is an unrealistic request, under many aspects: technical (algorithms that change constantly), timeline for checkpoints varying for each and every algorithm, application or use case, etc. The potential consequences of such an unrealistic concept would imply major limitations to the development and implementation of European 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. Further elaboration of such concept should be done in close collaboration with all stakeholders, especially with industry.

On data sets

As required now in the proposal, the data sets must be free of errors and complete, is unrealistic in real life. Whereas we always aim at high-quality of data fed in our algorithms, achieving such perfection in data sets is an immense challenge. Instead of having an absolute

requirement, the legislation should include an assessment set of rules and criteria for the data to fulfill (such as: error definition, testing procedure, including data input order, training criteria for algorithms, references to standardization of data sets, etc.)

Concretely we propose to enforce data traceability and data monitoring components in all the AI systems subject to this legislation. Ensuring that the data of the AI system is stable over time or in case it changes we can understand why, and we can relate changes in the created models and predictions with this data distribution shift.

On best practices and procedures

Besides datasets monitoring we propose that the legislation enforce a standard workflow procedure for ensuring the right design of AI system independently of the risk level. We believe that standards as CRIPS-DM are no longer sufficient, and we propose the creation of a new one where model monitoring and model explainability come in to place.

Moreover, we think that the European Commission should ensure that the explainability of these models matches the underlying physical mechanism that the AI system is trying to make predictions for or that it is in line to what the SME of the domain where the AI system is working believe to be correct.

Finally, we are convinced that every AI system, and especially the high-risk ones should be fair and robust. Meaning that these systems should be protected against biases presented in the data as well as malicious manipulations, e.g., adversarial attacks against classification models for detecting failures in component manufacturing.

Alignment with existing legislation and conformity assessment procedures

We welcome the fact that the AI Act is a New Legislative Framework (NLF)-based proposal. Although the proposal, through its *AI system* definition extends the NLF scope, Europe should consistently assess whether divergence from existing legislation is really needed, and furthermore, make sure not to deviate from existing conformity assessment procedures, widely established in industry, as well as the existing standards.

Additionally, European Commission should ensure that the scope is kept (as it seems so far) narrow to AI systems, avoid including conventional algorithms or statistical methods in the scope.

On sandboxes

For a fast and precise development of new regulation in the industrial AI domain, Europe must also be considerably more active in supporting the implementation of solutions for cutting red tape, by regulatory sandboxing, as described in the proposal. This would enable us to generate timely the requisite innovation surge and carry European industry back to global competitiveness in the AI field.

Frequently, use cases fail to succeed due to outdated or missing regulation, therefore the regulation should include a clear procedure on how the results of the regulatory sandboxes are taken into account and translated into the regulation, through amendments and updates.

On governance

Europe should ensure a balanced stakeholders' representation in the envisaged European AI Board, with industry (manufacturers and operators) and industry associations having an appreciable role, as an appropriate mirroring of the market and deployment of AI systems in Europe.