What can be expected from standardization regarding artificial intelligence?

Standardization regarding artificial intelligence: implications and expectations for French industry

by Franck GAMBELLI,
Health, Safety, CSR and Environment Director, UIMM The Factory of the Future[1]

In general, the end user of artificial intelligence (AI) can expect standardization to provide an **impartial view** of this fashionable phenomenon. Clearly, AI arouses emotions, and stimulates the imagination, hopes and fears. It fascinates or horrifies. The new draft regulations on AI clearly seem to give some credit to the transhumanist myths of consciousness emerging from matter. These regulations would make null and void the whole current legislative framework on the safety of machinery. Regarding AI, enterprises often receive mediatized injunctions and are stigmatized because they appear to be lagging behind.

- Firstly, we can recommend that standardization organizations should not give in to the temptation to do business with this theme by artificially stimulating the market for certification and training.
- Secondly, specific standardization for digital technology is perfectly desirable and legitimate, although a clear distinction should be made between the development of standards **regarding the core AI system** which is clearly a matter for AI specialists, and the development of standards for industrial applications. In the field of occupational safety, the issue of AI will therefore have to be approached in light of the expertise of the mechanics and machinery risk preventers.
- Thirdly, for the machinery standardizer, the recommendation would be to address the issue with the engineer's rigor and neutrality by calling on the acquired skills from their experience as preventers over the past thirty years.

As an employer located downstream of the value chain, i.e. as an end user, the standardizer should be reminded that there exists in the European Union a robust framework for managing occupational health risks.

- **The first European framework** is that governing occupational risk prevention for the end user. It is based on Article 153 of the Treaty on the Functioning of the European Union, the cornerstone of which is the **framework directive of 12 June 1989 on workplace health.** One of its daughter directives is Directive 2009/104/EC of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work. Whatever is done with regard to AI will therefore mandatorily have to comply with this framework. The end users should be encouraged to organize in order to better contribute to the standardization work,

1 https://uimm.lafabriquedelavenir.fr/industrie/

which is not easy for most of them; moreover, the European legislative framework gives them no incentive to do so.

The social aspect of the European legislation does not refer to the technical standards. This legislation is a minimal legislation that the Member States are entitled to reinforce. This therefore seems in conflict with standardization work, which aims rather to harmonize practices when a machine is placed on the market. Accordingly, the employees' trade unions complain, not without reason, that it is hard to obtain experience feedback from employees as an end user of the machines. This is also the case for companies as end users, and not just for SMEs.

It is very significant that the draft AI Regulation completely disregards the European framework for occupational safety in the workplace. In violation of the very principles of the New Legislative Framework of European technical harmonization and the famous "Blue Guide" which is the Commission's reference manual in this area, the draft regulates the end user. But, according to the Treaty, it is not up to the legislation on the free circulation of products to define employers' obligations in the field of occupational safety.

The purpose of this digression is to say to the standardizers *"Put yourselves in the place of the end user, like you do for any risk analysis, consider their viewpoint and not just that of the digital technology professionals."* Indeed, it is in the workplaces that all the safety issues will arise, because it is in this real-world environment of places, spaces, movements, flows, human beings, practical and economic issues that these technologies will operate. It is undoubtedly possible to create standards for methods to help SMEs conduct an IA implementation project rigorously. Moreover, there already exist guides, and in particular the remarkable French guide of the Centre Technique des Industries Mécaniques, which assist companies in the careful and rational conduct of a robotics project.

- **The second European framework** is that of the New Approach, i.e. the world of placing on the market products and in particular machinery, with of course the Machinery Directive 2006/42/EC and its series of harmonized standards. This is the natural environment of historical machinery standardizers.

On the other hand, this framework seems practically unknown to digital technology specialists and standardizers. It is therefore essential that digital standardization should be incarnated in machinery standardization with the support of experts having a good knowledge of the industry from the viewpoints of both the design and use of machinery. Digital concepts must be translated into the language and methods of the engineering offices designing machinery and the OSH experts.

The very principles of the New Approach are not only still relevant for dealing with the issue of AI, but, what's more, they should be an essential requirement for AI.

- **A first principle is the risk analysis requirement.** This principle is found for the end user with the framework directive on workplace health, but it also applies upstream to the entire value chain which performs systems integration, manufactures the hardware and designs the software. This principle does not exist in the draft AI Regulation. **And yet, risk analysis is the basis for targeting the essential requirements that will make it possible to control risk by adopting effective and proportionate preventive measures.**

What may seem striking, therefore, is the binary (0-1), absolute, abstract and authoritarian nature of the requirements of the AI Regulation, without nuance and without a hierarchy, which in no way resembles the risk analysis dynamic and the iterative approach of a risk analysis. The expressions of the AI Regulation and standards are therefore hard to exploit directly for an industrial design office, let alone for the end users.

- **A second principle is technological neutrality.** It doesn't matter whether the machine is a machine which operates manually with pulleys or gears, with hard-wired logic, programmable logic controllers, fixed software or software with algorithms. Only the result counts: **the risk must be controlled and the function ensured**. This principle is very important for the employer as end user, because it is he who will incur civil and penal liability of the first order in the event of an accident. It is also he who will be faced with the system with all the economic and technical issues that will arise. Obviously, the end user will demand that their machine operate predictably from the viewpoint of both its functionality and safety. Who would want to buy a machine that does whatever it likes? The standardizer must therefore conserve technological neutrality by principle in their prevention work. There is no sense in defaming or extolling conventional machinery and equally machinery with on-board AI. Once again, **all eyes must be focused on the end result, not on the technology which remains merely a means**.
- **A third principle is the clarity of concepts.** Admittedly, standardization is not a beautifully manicured garden, but with artificial intelligence confusion is reaching summits. Standardization must create definitions, introduce order, distinctions and hierarchies.

Compare the definitions of the ethics guide, the draft AI Regulation, and the draft Machinery Regulation. There is no room for slack legislation, confused legislation, or media-attracting legislation especially when there are threats of penal sanctions and prohibitions at stake.

  - AI can be **strong** AI, that of the transhumanist ambitions. In this case, the algorithm produces the algorithm and the machine lives its life by itself. In that case it must be given papers and an insurance policy, because the machine is an unruly adolescent and there is no knowing what it is capable of. The acquirer of the system and their lawyers, for their part, will remember, when the time comes, that behind every AI lurk several natural intelligences, in flesh and blood.
  - AI can also be systems which perform **complex tasks**, which already exist. This is called **medium or moderate AI.**
  - It can also include **conventional automatic learning systems**.
  - It can cover anything that operates with information technology.

The priority of standardization is therefore to clarify the holdall concept of AI. The standardizer must define functional safety classes according to the desired level of determinism. We should stop including all software in AI. In the rationale of the Machinery Directive, standards should make it possible to assess the impacts of automatic learning on machines. The standardizers recall that a machine can never go beyond its limits, that these limits well and truly exist and are objectivized in the risk analysis approach.

In the end, and if we have correctly understood the scientific discussions on AI, it is an unfortunate anthropomorphism, because in it there is not one ounce of intelligence, and especially of will, which is the highest faculty of the human soul. Co-legislators and standardizers would be well advised to say so.

Therefore, the standardizer, for digital technology and for machinery, must be concrete. The digital universe developed first in the world of services, especially in finance and insurance where, apparently, algorithms did wonders. It has to become acclimatized to the industrial ecosystem, but it must be recognized that the complexity of the AI value chain does not make this an easy task.

- Let's start with the **end user, still too invisible to the standardizer:** it is an enterprise, often industrial, which works on material, with its company manager, its engineers and technicians, its operators and its control and maintenance specialists. They have expertise and experience. The new system, whether it be robotization, artificial vision or digital twin design, must **preserve the company's expertise and provide real value added from both the economic and human viewpoints**. This value added is not acquired immediately.

- **The system integrator** interfaces with **the machine manufacturer** and with the **software supplier.** This is where **strict discipline** is essential for the user company to tame the AI.
  The CETIM guide mentioned above suggests building a robotization approach by scrutinizing and evaluating all aspects from the start. It is normal for suppliers' sales personnel to sell some dreams, but it is essential to "set the pressure gauges to zero" before deciding. Is this indeed the right technique? What would be the impact on the company's flows? Can we be sure that the traditional operator does not in the end work faster and better than the future system? Do I have the capacity to cope with the system in the long run? What new competencies? Will it impact the corporate hierarchy? Will it destroy know-how? Will the company become completely dependent on the software supplier and the data manager? Will they siphon off all the know-how and reduce the company to the state of a mere subcontractor? It is here that **the involvement of the company's actors** is crucial, because they possess the practices, the knowledge and the information that are not necessarily expressed formally a priori.
  For safety purposes, AI must be double-screened by risk analysis of the system's installation location and analysis according to the Machinery Directive. Conventional risks such as the risk of being impacted or burned must be identified and addressed, as well as less obvious risks relating to ergonomics.

For example, adaptation of the machine's movement to that of the operator, and not the reverse. **Cognitive aspects for the operator** related, for example, to the speed of the machine, must also be taken into consideration. Psychological aspects such as the fear of being impacted should be dealt with by appropriate preventive measures. This must be done in advance, because afterwards it will be too late.

However, the AI Regulation seems to be superimposed on the draft "Machinery" Regulation. It must not crush it. The predominance of digital technology over the mechanic's art is a risk in itself. AI must be introduced at the mechanics' pace. Studies mainly concern partial subjects such as artificial vision or the use of AI ahead of a control system. The studies also concern the use of AI to ensure that the machine adapts to a new product range safely.

To conclude, here are a few points to watch and bear in mind. Preservation of safety expertise and industrial expertise is crucial. For example, **in digital twin design**, it is completely illusory to imagine that the software will replace the intelligence and natural will of the mechanic. Admittedly, the software will be able, by itself, to increment the feedback coming from outside data, but only the mechanic's eye will be able to discern whether the process underway remains appropriate.

More fundamentally, the giants of the digital economy could be powerful enough to reduce manufacturing industry to the role of "commodities", as happened for the music industry and electricity (until the crisis for the latter). This is valid for manufacturing machinery, but equally for the end user, their workshops and personnel. Commodities refer to a generic, banal, accessory activity, with low value added. It is our conviction that industrial genius, the men and women forming the industry, but also its production facilities, its expertise, its disciplines with regard to production and occupational safety, must not become the accessory of a principal reality consisting of AI. AI must serve them, and not the reverse.