Artificial Intelligence: Regulation, Standardisation and Conformity Assesment

Mohammad Mahdi Share Pasand
Electrical Engineering Research Group, Faculty of Technology and Engineering, Standard Research Institute, Karaj, Iran.

Abstract

Artificial Intelligence may be the fastest emerging technology trend the civilization ever experienced. It is also among the most high-risk ones in terms of privacy, security and human right issues. A growing number of products are utilizing artificial inteligence in one way or another on a daily basis. In this situation, it is of vital importance to regulate and standardize this technological sector before it spreads into several application domains without supervisory and regulatory control. In this paper we address the most important regulation issues to be dealt with in this area. The regulation and standardizatin procedures must be able to guarantee a minimim level of trustworthy artifical intelligence which is bound to abide some rules in all circumestances. The first task beforehand regulatory bodies is to determine those rules in a systematic manner based on acquired experience and customer feedback, guidances prepared by expert teams in accordance to existing regulations. The second task is to develop conformity assesment schemes to assess the level of conformance of a product to those regulations. The present paper focuses on the first phase and provides standardization requirements for the generic application of AI-based systems.

Keywords: Artificial Intelligence, Regulation, Standardization, Conformity Assesment.

Introduction

Standardization determines how a newly introduced technology is deployed and scaled-up in different technology sectors. For instance, it may hinder the development of a technology by restricting its application in highly sensitive facets. (e.g. child care, health, etc.). Development of new technological trends in general and Artificial Intelligence (AI) based products specifically, occurs in three phases:

1) Introductory phase in which the first ever prototypes are introduced to the society and industry. The first applications are usually restricted to research and laboratories.

2) Limited application phase in which the new technology is utilized by advances high technological firms for military or cutting-edge industry applications.

3) public application in which the new technology spreads in many societal sections and is widely recognized and used by small, medium and large enterprises as well as people of different factions.

The second phase triggers company standardization process while national and international standardization processes usually start in the third phase. The development of new technologies relies on how the technical, legislative and regulatory institutions react to the earlier evolutions. Standardization forms the new technologies in many aspects. Recent years have witnessed a surge in the utilization of AI in many technical and societal platforms. AI is already in phase 3 of its development. However there are still many challenges to be addressed [1-7]. AI is actively expnading. It demands both reseach and experiment to discover and address all standardization challenges it poses [8-14].

Currently, International standardization institutes including International Standardization Organization (ISO) and International Electrotechnical Commission (IEC), the International Telecommunication Union (ITU) and European standards (EN) are working on new standards AI [8]. ISO./IEC joint technical committee JTC 1 is responsible for developing consensus-based international standards in the field of information technology. Subcommittee JTC1-SC 42 is dedicated to AI. The United Nations Inter-Agency Working Group on AI (IAWG-AI) coordinates these activities. AI for good is another convening platform operated by ITU with 40 UN liason agencies on the subject.

Two different approaches are known in the standardization community for emerging technologies:

1) Top-Down approach: In this approach the standadization organization as well as the regulatory bodies gather all experts together and list all possible hypothetical scenarios in which the emerging technology may require regulation. The result of this appraoch is a horizontal or high-level standard/ guidance or directive which is used by later specific, application oriented standards and law.

2) Bottom-Up approach: In this approach, specific application sectors already have developed their own standards or local regulations. The standadization or regulatory body needs to assess these application oriented standards and extract the common aspects, generalize the requirements and prescribe them to other less-developed fields.

Currently, most of the international standadisation bodies are taking the Top-Down approach, working on new horizontal standards to address the general rules and regulations which are to be implemented in all application areas. ISO and IEC use the term holistic to refer to the Top-Down approach in which a number of horizontal standards are first developed to address common aspects and generic requirements. These horizontal standards are then used in the development of application-oriented standards including sector-specific requirements and specifications as well as product standards [8]. In some cases including intelligent vehicles, defence technologies and education, some requirements have been suggested or even published as international standards [3].

Standadization activities for electronic products have been focused on a number of subjects the most important of which can be named as follows [15]:

1) **Safety:** safety is defined as freedom from risk on health of the user or other people invloved in the operation of a product/ system. By the word operation we mean normal operation, single fault situations and othe foreseable misuses by any effector party. A relevant topic in safety is known as functional safety which refers to functionality of systems dedicated to the safety purpose. AI-based products which have interactions with humans or safety systems shall meet functional safety requirements when they are expected to perform in safety related procedures.

2) **Privacy and Security**:Many electronic and computer products can violate privacy or security of their users. This is one of the most important issues in AI-based products.

3) **Human oversight:** Any auomated system (including AI-based or conventioanly automated) shall have the feature of manual mode in which the user, operator or service personnel can disable automated features and opretae the system in the completely manual mode [15].

4) **Performance:** Any electronic or electrical product/ system shall provide the expected/ declared performance in terms of expected life time, energy efficiency, etc.

5) **Compatibility:** Any electronic or electrical product/ system shall be compatible with other products and the human. This compatibility includes electromagnetic compatibility, backward component compatibility and human compatible interactions.

6) **Environenmet:** Electronic products/ systems shall pose no harm to the environment in their life cycle including the recycling stage. This amounts for energy consumption, carbon footprint and hazardous materials during production, usage and recycling.

Besides the aforementioned generic subjects common in electronic products standardization, there are some novel concepts raised almost exclusively for AI-based systems. In fact, AI has changed the standardization goals. In the following sections we give a brief summary of some generic as well as specific requirements already exisiting in standards, guides and regulations throughout the world. The following requirements are re-phrased and generalized in order to better reflect the concepts.

Generic requirements

The following is a non-exhaustive list of legal requirement for almost any AI based system (See [2], [7] and references therein):

1. **Ethics**: All AI-based decision shall be ethical. The definition of ethics remains relative to the society snd context of the application. However, the general ability of the AI algorithm to consider some ethical rules is a common aspect. We do not expect AI to perform complex decisions in situations of conflicting ethical codes. However, we also do not expect the AI to overtly violate those ethical terms agreed upon in the development of that system. In practice, the involved parties (including at least producer, consumer and regulatory body) should agree upon the ethical codes before testing of the product.

2. **Privacy and security**: AI-based products shall not violate privacy and security. This may be interpreted differently in different countries. However, some common examples of privacy violation include unauthorized acquisition and/ or sharing of private information including but not limited to voice or video of the user or his/her surroundings, data regarding his/ her activities or preferences, etc.

3. **Defined Liability:** If an AI-based product is involved in a criminal case, it is important to determine how much different parties are liable. In AI-based environments, there are several parties including the AI algorithm developer company, the end product supplier, the operator and other effectors.

4. **Avoiding Discrimination or classification**: AI-based products shall not discriminate between people because of their ethnicity, religion, gender, life style, etc. This conforms with ethical codes of many societies in almost all situations. However, it is listed as a separate requirement since in some cases, ethical codes may not address this important issue.

5. **Avoiding subliminal techniques:** AI-based products shall not deploy subliminal techniques beyond a person's consciousness to alter their unconscious including attitude, emotions, etc. [9].

6. **Avoiding exploitation of person's vulnerabilities:** AI-based products shall not exploit any of the vulnerabilities of a specific group of persons including elderly, children or their caregivers, etc. [9].

7. **Avoiding biometric identification:** AI-based products shall not use real-time remote biometric identification in publicly accessible spaces unless required by law enforcement.

8. **Provision of a risk assesment scheme**: In high risk applications, it is essential that the provider of an AI-based product, provides a detailed risk assesment analysis in which all possible undesirable outcomes (including those described above) are identified and their corresponding risk (probability of occurrence combinded with the severity of that outcome) is evaluated. This particularly concerns the risks emerging when young people under the age of consent use the product. The provider shall then implement corrective and preventive actions to mitigate the identified risks down to an acceptable level. Then the provider shall compute the residual risk and demosntrate in what situations it may occur. This shall be informed to the consumer and other relevant parties including the regulatory and standardization sectors.

9. **Assesment of data set:** Any AI-based product uses a data set of training, validation and testing. In high risk applications, these data sets shall be assessed regularly for availability, quantity (including all possible scenarios), suitability and shall be free of errors to the best extent possible [9]. The data set may be assessed by regulatory bodies.

10. **Automatic event recording:** In high risk applications, relevant events shall be recorded for later reference.

11. **Human oversight:** Any AI-based product shall have the feature of human oversight in case the user chose to terminate or temporarily deactivate the AI in the product. To enable the human oversight feature, the product should have an effective human machine interface and shall declare to the user, its biases, limitations and risks. This also includes transparency and interpretability of the AI outcome.

12. **Resilience and cyber security:** AI-based products should be able to achieve and maintain a pre-defined level of accuracy in their main performance characteristics in normal conditions as well as in foreseable undesired situations including changes in the environment, cyber attacks, etc. This is particularly essential because conventional mechanisms intended to ensure robustness and cybersecurity may not be adequate when intervened by AI [3, 16]. In fact, in automated systems, the fail safe or manual mode can be triggered by any event of fault or cyber attack. In AI-based systems, however, this can cause challenges.

13. **Documentation:** Besides conventional documentations mandatory for all electronic products, There are additional data which have to be documented and provided to the user for AI-based products. These data include the intended use, performance characteristics, foreseeable circumstances leading to risk, pre-determined changes and expected lifetime as well as the human oversight mechanisms.

Figure 1 from [9] demonstrates some of the aformentioned requirements (from left to right: items 5, 6, 4 and 7 above).

Figure (1) Prohibited AI activities [9]

Sector specific requirements

There are additional requirements for sector specific applications. For instance in intelligent vehicles [3], health and biomedical applications [17], defence technologies [18-20] and education [21-23].

Results Discussion

In this paper some generic standardization requirements are discussed for the emerging field of AI. AI is a friutful research and applied field which is still developing. In fact, reseach activities in AI has a very high rate [10]. Therefore, one may expect that new standardization issues raise in the course of time. This is emphasized in several research works on AI standardization [11-14]. The provided requirements however illustrates the current insight obtained from several decades of information technology and automated systems standardization combined with practical experiences and knowledge from the AI technology.

Conclusions

In this paper some generic requirements for standardization of AI-based systems and products are discussed. International standardization organizations involved in the development of AI standards are listed. Some general standardization subjects for electronic and automated systems are first discussed. Then existing requirements for AI-based products both from standardization bodies and recent research works are introdiuced in a categorized manner. Research works on the sector-specific subjects are also referred to for further reading.

References

[1] Oveisi, S. , , gholamrezaie, F. , , qajari, N. , , Moein, M. S. , and goodarzi, M. . "Review of Artificial Intelligence-Based Systems: Evaluation, Standards, and Methods", *Advances in the Standards & Applied Sciences*, 2, 2, 2024, 4-29.

[2] Share Pasand, M. M. . "Standardization challenges in the IOT and AI era", *Advances in the Standards & Applied Sciences*, 1, 2, 2023, 1-2.

[3] Heidari, N. , and Share Pasand, M. M. . "Artificial Intelligence in Vehicles: Standardization perspectives", *Advances in the Standards & Applied Sciences*, 3, 1, 2025, 23-29.

[4] Kenarkoohi, K. , , Tamtaji, M. , and Ekrami Kivaj, A. . "The Role of Artificial Intelligence in Establishing Safety and Security Standards in the petroleum Industry", *Advances in the Standards & Applied Sciences*, 2, 4, 2024, 163-171.

[5] Haji Molla Mirzaei, H. , and Azizi Mehmandoost, M. . "Prioritizing AI Standards: Integrating Requirements and Expert Criteria", *Advances in the Standards & Applied Sciences*, 2, 3, 2024, 22-35.

[6] Savari, M. . "Book : Artificial Intelligence Safety and Security", *Advances in the Standards & Applied Sciences*, 3, 1, 2025, 30-33.

[7] Tavakoligolpaygani, S. , Share Pasand, M. M. , and Parand, F. . "Multidisciplinary Perspectives on Artificial Intelligence and the Law", *Advances in the Standards & Applied Sciences*, 2, 4, 2024, 194-197.

[8] https://etech.iec.ch/issue/2020-01/a-holistic-ecosystem-approach-to-ai

[9] Charter, R., "Ethical and trustworthy Artificial Intelligence", British Standards Institute, 2022.

[10] Daniel Zhang, N. M. "The AI Index 2022 Annual Report", AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University, 2022.

[11] Zielke, Thomas. "Is artificial intelligence ready for standardization?." *Systems, Software and Services Process Improvement: 27th European Conference, EuroSPI 2020, Düsseldorf, Germany, September 9–11, 2020, Proceedings 27*. Springer International Publishing, 2020.

[12] Golenkov, Vladimir, et al. "Artificial intelligence standardization is a key challenge for the technologies of the future." *International Conference on Open Semantic Technologies for Intelligent Systems*. Cham: Springer International Publishing, 2020.

[13] Prifti, Kostina, and Eduard Fosch-Villaronga. "Towards experimental standardization for AI governance in the EU." *Computer Law & Security Review* 52 (2024): 105959.

[14] Lund, Brady, et al. "Standards, frameworks, and legislation for artificial intelligence (AI) transparency." *AI and Ethics* (2025): 1-17.

[15] Share Pasand, M., M., "Standard and Standardization in Electrical Engineering", *Standard Research Institute Press*, 2022. (in Persian)

[16] TC260, "Guidelines for the Practice of Cybersecurity Standards - Guidelines for the Prevention of AI Ethical Security Risks". *The National Information Security Standardisation* Technical Committee of China (2021).

[17] WHO, "Ethics and Governance of Artificial Intelligence for Health", *World Health Organization* (2021).

[18] Roberson, Tara, et al. "A method for ethical AI in defence: A case study on developing trustworthy autonomous systems." *Journal of Responsible Technology* 11 (2022).

[19] Blanchard, Alexander, Christopher Thomas, and Mariarosaria Taddeo. "Ethical governance of artificial intelligence for defence: normative tradeoffs for principle to practice guidance." *AI & SOCIETY* (2024): 1-14.

[20] Soare, Simona R. "European military AI: Why regional approaches are lagging behind." *The AI Wave in Defence Innovation*. Routledge (2023): 80-111.

[21] Renz, André. "AI in Education: Educational Technology and AI: Challenges and Requirements for the Educational Technologies of the Future." *Work and AI 2030: Challenges and Strategies for Tomorrow's Work*. Wiesbaden: Springer Fachmedien Wiesbaden, 2023. 353-360.

[22] Chen, Lijia, Pingping Chen, and Zhijian Lin. "Artificial intelligence in education: A review." *IEEE Access* 8 (2020): 75264-75278.

[23] Bhutoria, Aditi. "Personalized education and artificial intelligence in the United States, China, and India: A systematic review using a human-in-the-loop model." *Computers and Education: Artificial Intelligence* 3 (2022): 100068.