UNECE WP.6
Project on CRA for products with embedded AI
Draft for Public Review as of: 12 Apr. 2024

A common regulatory arrangement for the regulatory compliance of products and/or services with embedded AI or other digital technologies

Disclaimer

ECE draws attention to the possibility that the practice or implementation of its deliverables (which include but are not limited to standards, recommendations, norms, guidelines and technical specifications) may involve the use of a claimed intellectual property right. Each output is based on the contributions of participants in the ECE Working Party 6 (WP.6) deliverable development process, who have acknowledged that all new intellectual property rights generated belong to ECE and have also agreed to waive enforcement of their existing intellectual property rights used in the WP.6 deliverables against any party using the outputs.

ECE takes no position concerning the evidence, validity or applicability of any claimed intellectual property right or any other right that might be claimed by any third parties related to the implementation of its outputs. ECE makes no representation that it has made any investigation or effort to evaluate any such rights.

Acknowledgement

(This will be on the "publication" version; not on the version for the annual session)

This publication was designed and edited under the supervision of Lance Thompson, Economic Affairs Officer and Secretary to the UNECE Working Party on Regulatory Cooperation and Standardization Policies (WP.6) assisted by Alec Fischbein. The content was authored and coordinated by Markus Krebsz, project leader, with contributions from: Heidi Lund, Emily McIntyre, Valentin Nikonov, Lucy Salt and Paul Taylor. The final draft was reviewed by Ariel Ivanier.
The UNECE WP.6 expresses its gratitude to all those who contributed to the development of this publication.

Introduction

Products and/or services making use of embedded artificial intelligence (AI) or other digital technologies are used widely, yet without universally agreed or accepted definitions and under varying regulatory frameworks. Relevant standards are under development aiming at international harmonization. Functional safety and cybersecurity of such products are essential elements for economic competitiveness and product regulations. However, breakthroughs and innovations are moving considerably faster that standards and regulations.

A common regulatory arrangement (CRA) as outlined in the UNECE WP.6 *Recommendation L on the International Model for Transnational Regulatory cooperation based on Good Regulatory Practice*[1] provides a voluntary framework for regulatory cooperation that facilitates market access through the use of good regulatory practice and the establishment of sectoral and/or product-specific arrangements between interested UN member States.

This CRA can be used in relation to products and/or services with embedded AI systems or other digital technologies as a basis for:

- Setting legitimate regulatory objectives
- Identifying and assessing risks
- Identifying relevant international standards for the development of regulations
- Establishing mutually recognizable conformity assessment procedures
- Establishing market surveillance and other enforcement mechanisms

[1] See: https://unece.org/DAM/trade/wp6/Recommendations/Recommendation_L_en.pdf

Product regulation is often managed in a siloed approach, whereas embedded technologies are more of a horizontal nature. This may result, in some economies, in a disparity of regulations at the national level where requirements on AI or other embedded technologies might be interpreted or tested differently. This CRA can be used at a national level to promote convergence of national technical regulations among agencies currently in place or yet to be put in place.

This CRA provides an overall approach to products and/or services with embedded AI or other digital technologies. It is proposed that use cases be developed to demonstrate how the CRA could be used in different sectors.

This CRA builds upon the paper developed within WP.6 for the November 2023 Annual Session, *"Regulatory compliance of products with embedded artificial intelligence or other digital technologies" (ECE/CTCS/WP.6/2023/9)*[2]*,* and has taken into consideration the *"Interim Report: Governing AI for Humanity" December 2023* developed by the United Nations Advisory Board on Artificial Intelligence[3]. In this perspective, it supports the use of AI as a potential means to achieve all 17 Sustainable Development Goals and sustainable development in its three dimensions – economic, social and environmental.

Due to the technologies' continuous evolution, it will likely be necessary to periodically review this CRA and update as necessary. References to this document are encouraged to clearly indicate the version number.

1. Scope

Products and/or services covered by this CRA include:

- Artificial intelligence (AI) system: engineered system that generates outputs such as content, predictions, recommendations or decisions for a given set of human-defined objectives (as for example, covered by the *International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 22989 on AI concepts and terminology*).[4]
- Generative artificial intelligence (GenAI): an AI system which can produce a variety of data such as images, videos, 3-D models or audio files. These systems may be embedded into a device or be made available as a Software as a Service (SaaS).
- Product: a product is an item produced and given or sold, often as a result of a manufacturing process, that may change or be re-purposed after entering the market or following a software update (and can include software / SaaS in itself).
- Product and/or services with embedded digital technologies: a product and/or service with an embedded, upgradeable (remotely, offline or by other means) AI system or with integrated, upgradeable software or with a combination of both, that operates with varying levels of autonomy and directs its operation and can make decisions influencing physical or virtual environments in a way that is generally intended to further human-defined objectives.

Where not otherwise indicated in the text, the terminology used is based on definitions of the World Trade Organization's (WTO) Agreement on Technical Barriers to Trade (TBT), Annex 1[5].

[2] See: https://unece.org/sites/default/files/2023-10/ECE_CTCS_WP6_2023_09_E.pdf
[3] See: https://www.un.org/en/ai-advisory-body
[4] See: https://www.iso.org/standard/74296.html
[5] See: https://www.wto.org/english/docs_e/legal_e/17-tbt.pdf

This CRA does not intend to cover autonomous wheeled vehicles[6] or autonomous weapons[7]. Both of these are directly covered by other national or international arrangements. However, the guidance in this document may provide useful for these product categories as well.

2. Product and/or services requirements

Regulatory objectives and assessing the level of risk

Setting regulatory objectives should be based on the acknowledgement that zero risk is not achievable. Determining the tolerable level of risk and risk appetite should be performed as described in UNECE WP.6 *Recommendation R on Managing Risk in Regulatory Frameworks*[8].

Certain products with embedded AI or other digital technologies have an intrinsically high risk, where there is a potential to have direct negative impact on health and safety or fundamental rights of people. Limited risk (or medium risk) is that which could impact safety issues. Low risk AI is that which does not use personal data and/or influence human beings. Governments will need to assess what level each risk is and choose the appropriate conformity assessment methods accordingly.

Certain sectors have an intrinsically higher severity, where the stakes for life and health are particularly high. Certain medical equipment in hospitals, for example, have sophisticated diagnostic systems using embedded AI. Even if the medical equipment could generate algorithmic decision-making, given liability issues and the potential risk for patients, it is suggested that human decision-making be included wherever possible. Some industrial machinery where humans work alongside programmed robots piloted by AI could also merit obligatory human oversight and intervention. AI systems should not be able to override human control.

Technology embedded within products is often difficult to assess or to know the actual content; this phenomenon is called “black box” (e.g., we do not know what is inside). This is true of products with embedded AI or other digital technologies, perhaps even more so as the system itself may react in an unexpected way because of the information it is learning from other sources. This unknown parameter of technology is usually balanced by a series of robust testing of the system within various parameters; this may not be sufficient to discover every unknown of the system, so a certain level of residual risk will remain. Regulators and distributors of such products need to ensure that these residual risks are tolerable.

For example, further guidance has been developed in the *National Institute of Standards and Technology (NIST) - Artificial Intelligence Risk Management Framework (AI RMF1.0)*[9].

Regulatory objectives and societal impact

The embedded system has been conceived in a way to mitigate bias in the AI system itself and within the AI-aided decision making. This includes human cognitive bias, data bias and bias introduced by engineered decisions. These are outlined in the *ISO/IEC TR 24027 on Bias in AI systems and AI aided decision making*[10].

---

[6] Self-driving cars and autonomous wheeled vehicles are covered under separate United Nations committees. In contrast to autonomous wheeled vehicles, aerial and submarine vehicles as well as robots are within the scope of this CRA. See: https://unece.org/wp29-introduction

[7] The deployment of autonomous weapons and defence products and/or services with embedded AI system and other digital technologies falls within national defence and national security strategies and hence are out of scope of this CRA.

[8] See: https://unece.org/fileadmin/DAM/trade/wp6/Recommendations/Recommendation_R_en.pdf

[9] See: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj6gda824CFAxUURKQEHXqzB70QFnoECBcQAQ&url=https%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2Fai%2Fnist.ai.100-1.pdf&usg=AOvVaw2VNmSoibzEJI-lKBXBIYTw&opi=89978449

[10] See: https://www.iso.org/standard/77607.html

The embedded system will not result in the loss of individual freedom or of human autonomy.

The embedded system will not negatively impact individual mental wellbeing or wider societal impacts. This includes safeguarding children's vulnerabilities and children's rights on education, home, media and gamification/play. These are outlined in the *United Nations Convention on the Rights of the Child (UNCRC)*[11], further elaborated in the *Convention's General Comment No 25 (2021) on children's rights in relation to the digital environment*[12].

The embedded system will not further widen the digital divide as outlined in the *United Nations resolution on "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development" (A/78/L.49)*. [13]Products with embedded AI or other digital technologies should be fully functional in emerging economies. They should further aim to not create barriers for emerging economies to trade in these products or to enter into such markets.

Regulatory objectives and digital considerations

The embedded system has been designed in such a way as to ensure trustworthiness. This would include safeguards against AI-specific security threats, AI-specific privacy threats, unpredictability, opaqueness and challenges in the implementation and use of AI systems. These are outlined in the *ISO/IEC TR24028 on Overview of trustworthiness in artificial intelligence*[14]. Specific concerns on loss or unauthorized access to data is developed for example in the *European Union (EU) General Data Protection Regulation (GDPR)*[15], the *EU AI Act*[16] and other data regulations.

The embedded systems should foresee a robust system to protect against cyber-attacks. Data drift, concept drift, reward hacking algorithms and safe exploration should be safeguarded within these systems. This is outlined in *ISO/IEC TR5469 on functional safety and AI systems*[17]. For instance, see also the *NIST Adversarial Machine Learning, Taxonomy and Terminology of Attacks and Mitigations (NIST AI 100-2e2023)*[18] and the *NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP.29)*[19].

Likewise, measures should be taken to ensure that the embedded technology cannot be used for illicit activities (such as unauthorized or illegal control or monitoring, slander, or libel).

3. Reference to international standards

Beyond the standards listed in the previous section, there are a number of standards which can assist in designing and regulating products or services with embedded AI or other digital technologies.

As outlined in the WTO TBT Agreement, article 2.4: "Where technical regulations are required and relevant international standards exist or their completion is imminent, Members shall use them, or the relevant parts of them, as a basis for their technical regulations except when such international standards or relevant parts would be an ineffective or inappropriate means for the fulfilment of the

---

[11] See: https://www.unicef.org.uk/what-we-do/un-convention-child-rights/
[12] See: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[13] See: http://www.undocs.org/A/78/L.49
[14] See: https://www.iso.org/standard/77608.html
[15] See: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[16] See: https://artificialintelligenceact.eu/
[17] See: https://www.iso.org/standard/81283.html
[18] See: https://csrc.nist.gov/pubs/ai/100/2/e2023/final
[19] See: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjD7YeY3ICFAxWoVKQEHWMpCokQFnoECBMQAQ&url=https%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2FCSWP%2FNIST.CSWP.29.pdf&usg=AOvVaw2G2k0cNmqcbku2eve_gYVU&opi=89978449

legitimate objectives pursued, for instance because of fundamental climatic or geographical factors or fundamental technological problems."

The following international standards may be applied in relation to products and/or services with embedded digital technologies.

- *ISO/IEC 42001 series of standards on AI management systems*[20]
- *ISO/IEC 23894:2023 series of standards on AI – Guidance on Risk Management*[21]
- *ISO/IEC TR 22100-5 series of standards on the implications of AI machine learning*[22]
- *IEC 62443 series of standards on industrial automation and control systems (IACS)*[23]
- *IEEE 7001-2021 series of standards for transparency of autonomous systems*[24]
- *Organisation for Economic Co-operation and Development (OECD) Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449)*[25]
- *United Nations Educational, Scientific and Cultural Organization (UNESCO) Recommendation on the Ethics of Artificial Intelligence (SHS/BIO/PI/2021/1)*[26]
- *World Health Organization (WHO) Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models*[27]

4. Conformity assessment

Current regulatory practices for conformity assessment follow sector-specific mandates while compliance of products and/or services with embedded AI or other digital technologies is of a horizonal nature, requiring new expertise. Horizontal regulatory collaboration as a multi-disciplinary approach is needed to both identify and address risks, vulnerabilities and cyberthreats and increase operational resilience. This necessitates the development of horizontal regulatory capabilities beyond sectoral mandates, that are cutting across mandated procedural silos and are both supportive of the dynamic nature of digital innovation and conducive of enforcement strategies demanded by a digital market.

Beyond checking the conformity of the product which is under the supervision of a specific agencies, a product with embedded AI or other digital technology will need to be verified against the AI-specific technical aspects of the product. As noted above, the risk is that each national agency may take a different approach to AI in relation to the products it traditionally oversees. This may result in multiple compliance rules on AI within a single economy. It is suggested to avoid such an approach.

There may be a different approach based on the risk analysis. As with the example above under product regulation, there could be considered three levels of risk: high, limited (or medium) and low. For those products of low risk, governments might consider no specific conformity assessment process, or at most a supplier's declaration of conformity. For those of limited risk, governments might consider a supplier's declaration of conformity. And for those of high risk, governments might consider third party conformity assessment.

---

[20] See: https://www.iso.org/standard/81230.html
[21] See: https://www.iso.org/standard/77304.html
[22] See: https://www.iso.org/standard/80778.html
[23] See: https://www.iec.ch/blog/understanding-iec-62443
[24] See: https://ieeexplore.ieee.org/document/9726144
[25] See: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjgxvXX3ICFAxVyVKQEHXRyBlUQFnoECBMQAQ&url=https%3A%2F%2Flegalinstruments.oecd.org%2Fapi%2Fprint%3Fids%3D648%26lang%3Den&usg=AOvVaw3bU62HpvCxeAcd6gxRGeJ6&opi=89978449
[26] See: https://unesdoc.unesco.org/ark:/48223/pf0000381137
[27] See: https://www.who.int/publications/i/item/9789240084759

Supplier's declaration of conformity

A supplier's declaration of conformity may be considered for products or services with embedded AI or other digital technologies of limited risk, and eventually also for those of low risk.

Such a declaration should outline that the supplier recognizes the importance of the principles in the product requirements section and that the product or service complies with the relevant international standards. For example, the supplier declaration could usefully reference the *ISO/IEC TR5469 on functional safety and AI systems*[28] and the *Organisation for Economic Co-operation and Development (OECD) Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449)*[29].

Third-party conformity assessment

A third-party conformity assessment would likely be preferred for products or services with embedded AI or other digital technologies that are considered of high risk. For the AI-related technical aspects of the product or service, such an assessment should outline conformity with the principles in the product requirements section and that the product or service complies with the relevant international standards. The referenced standards may vary depending on the type of product. For medical equipment, it would likely be the *World Health Organization (WHO) Ethics and governance of artificial intelligence for health: Guidance on large multi-modal models*[30], for example.

By adopting this CRA, government agencies would signify their acceptance of third-party conformity assessment on the AI-related aspects of the product or service based on the principle of this CRA. This could be within or beyond pre-existing mutual recognition agreements. In both cases, there would need to be reference to the principles within this CRA for the AI-related aspects.

5. Market surveillance

One of the major defining aspects and key regulatory challenges of products or services with embedded AI or other digital technologies is that they may be linked to a remote server that will provide regular updates. The challenge is therefore how to ensure continuous compliance of these products once they have been put onto the market, which may not allow physical follow-up, inspection or verification of changes in product/service properties.

Market surveillance authorities will need to integrate methods for continuous compliance into their workflows. This will include regular mandatory independent audits to assure compliance to binary (compliant/non-compliant) government-approved criteria of products or services already on the market and to test their conformity to the principles and standards initially required for entry onto the market (hopefully based upon the principles within this CRA). These audits will be of particular importance for products or services that had been identified as high risk.

Products or services that no longer comply to the principles and standards required of such products to enter the market should be promptly called back and taken off the market. In case of critical non-conformity, an international alert should be put in place to inform other economies.

[28] Op.cit.
[29] Op.cit.
[30] Op.cit.