

European standardization in support of the European Artificial Intelligence regulation

Presentation by Patrick Bezombes

Vice-chair of CEN-CENELEC JTC 21 (European AI standardization)

AI « horizontal » EU standardization environment

- The European Commission (+ OECD and UN influence)
 - AI Act: safety, security, health and protection of human rights (fairness...)
 - AI liability directive:
 - “allowing compensation for damage when products like robots, drones or smart-home systems are made unsafe by software updates, AI or digital services that are needed to operate the product, as well as when manufacturers fail to address cybersecurity vulnerabilities.”
 - A future set of Harmonized Standards - Standardization request (draft received, official request expected by end 2022)
- CEN-CENELEC/JTC 21 (Artificial Intelligence)
 - Created in May 2021; four Working Groups; first focus on the AI Act, but will cover broader concerns (Green AI, NLP, AI nudging...)
 - Adoption/adaptation of ISO-IEC standards or homegrown standards
- ISO-IEC/SC 42 (Artificial Intelligence)
 - Very active: More than 35 standards developed or launched, and a lot more to come
 - Terminology, AI management systems, AI risk management, Trustworthiness characteristics, data quality, use cases....
 - JWG 3 on Health informatics
- Sectorial considerations
 - Aeronautics:
 - SAE/EUROCAE G34/WG114 (under EASA supervision in the EU)
 - ISO TC 20 – Aircraft and space vehicles
 - Automobile:
 - SAE (J3016 – Taxonomy and definition)
 - ISO TC22 Road vehicles
 - ISO TC 204 Intelligent transport systems
 - UN regulations/standards
 - ITU-T, IEEE...
 - Health: ...
- Insurance – reinsurance
 - AI risk assessment based on standards before insuring products and organizations

Findings:

- A legislative, societal and insurance environment generating a need for clear and comprehensive standards
- A horizontal and sectoral proliferation of standards without terminology and concepts alignment

Request for standardization to support the AI act

Standardization request (draft)

1. risk management system for AI systems
2. governance and quality of datasets used to build AI systems
3. record keeping: built-in logging capabilities in AI systems
4. transparency and information to the users of AI systems
5. human oversight of AI systems
6. accuracy specifications for AI systems
7. robustness specifications for AI systems
8. cybersecurity specifications for AI systems
9. quality management system for providers of AI system
10. conformity assessment for AI systems

Quote: “We need a horizontal approach to unleash the potential of artificial intelligence in all areas. *A cross-cutting technology can only be effectively regulated by horizontal rules that provide solutions to common challenges.*” - Commissioner Thierry Breton

Criteria for EU/JTC 21 homegrown standards

- General principle: Use as much as possible ISO-IEC standards as long as it fits requirements
- General context set by the European Commission in its standardization strategy:
 - EU should be a global standard setter not just a standard taker
- European specificities and requirements:
 - EU values and principles
 - EU AI Act, with its timeline
 - Risk scope: Safety, health and fundamental rights... (+ environment ?)
 - Strong horizontal approach → interconnection with sectorial standardization, e.g. “explainability” concept is domain-agnostic/horizontal, “level of explainability” is domain-specific/context dependent
- Further requirement
 - Innovation and SMEs friendly

Standards considered for harmonization by JTC 21

- Terminology
 - ISO/IEC 22989:2022 Artificial intelligence concepts and terminology (published)
 - ISO/IEC 23053:2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (published)
 - ISO/IEC 5259 - part 1 Data quality for analytics and machine learning (ML) Overview, terminology, and examples (in development)
- AI management system & Risk management
 - ISO/IEC 42001 AI management system (in development)
 - ISO/IEC 27001:2013 Information security management systems (published)
 - ISO/IEC 23894 AI Risk Management (in development)
 - CEN-CENELEC AI Risk catalogue (in development)
- AI & Data
 - CEN-CENELEC AI trustworthiness characterisation (in development)
 - ISO/IEC 5259 - part 2 Data quality for analytics and machine learning (ML) Data quality measures (in development)

- ISO/IEC 5259 - part 3 Data quality for analytics and machine learning (ML) Data quality management requirements and guidelines (in development)
- ISO/IEC 5259 - part 4 Data quality for analytics and machine learning (ML) Data quality process framework (in development)

Horizontal requirements & vertical specificities

Base line: Strong horizontal/transversal foundations in AI

- Horizontal requirements
 - Terminology/taxonomy/ontology and concepts
 - Technical requirements frameworks (trustworthiness, metrics, control...) on AI components
 - Risk management framework, risk catalogue (not exhaustive)
- Vertical specificities
 - Operational domain
 - Risk assessment, domain specific risks
 - Technical requirements on AI systems (and components)
 - Conformity assessment schemes

Articulation between horizontal and sectorial standardization layers

Sectoral standards (automobile, health, aeronautics etc.) to be aligned with horizontal standards potentially from 2022

Timeframe for horizontal harmonized standards development

2021:

- First draft AI Act

2022:

- Standardization request (draft? official?), standardization work programme 2023
- AI Act publication (?)

2023/2024:

- Development of harmonised standards (Develop homegrown standards; Adopt/adapt ISO-IEC/SC 42 standards)
- 2nd standardization request

2023-2025:

- Development of conformity assessment schemes
- Designation of notified bodies

2025:

- Entry into application of AI Act

Challenges forward

- *Coherency between horizontal standardization and sectorial standardization*
 - Common terminology on AI, Machine Learning and AI trustworthiness characteristics
- *Getting ready in time for the AI Act*

- Anticipate mandatory conformity assessment and AI trustworthiness labelling
- *Competencies of evaluation, verification, testing, audit and certification bodies*
 - For AI systems
 - For AI management system
- *Making sure that the relevant EU stakeholders are contributing to AI standardization*
 - Consumer associations, Trade Unions, SMEs association, accreditation and certification bodies...