Roberto Sammarchi
Avvocato specialista in diritto dell'informazione, della comunicazione digitale e della protezione dei dati personali, Socio AIAS

ENSHPO
The European Network of Safety and Health Professional Organizations Submission on the Artificial Intelligence Act Guidelines on High Risk Systems

Introduction and Regulatory Context

Implementation of the European Union Artificial Intelligence Act represents a landmark regulatory development in shaping a single market dedicated to trustworthy and human-centric artificial intelligence. However, the true operational impact of the legislation depends entirely on the clarity and precision of the forthcoming classification guidelines. Within the European occupational safety and health landscape, a regulatory tension has emerged: the necessity to safeguard workers from invasive, algorithmically driven performance management must be balanced against the equally vital need to foster digital safety innovations that prevent workplace injuries and save lives. To address the issue, the European Network of Safety and Health Professional Organizations actively participated in the European Commission public consultation procedure on the draft proposal for High Risk AI Systems Guidelines.

Core Definition Versus Traditional Industrial Automation

In industrial plants, high-hazard manufacturing floors, and construction sites, physical risk mitigation relies extensively on digital safety instrumentation. Such safety systems operate strictly on static, pre-defined, and fully predictable deterministic rules. For instance, a conventional presence-sensing safety device or an infrared light curtain halts heavy machinery instantly when a physical object interrupts the geometric path. The function is executed via hardcoded logic gates without any machine learning, autonomous data-driven optimization, or inference from variable datasets. The association warns that if the guidelines do not sharply delineate between deterministic, rule-based automation and advanced computational frameworks, standard safety components risk being misclassified as high-risk systems.
A blanket expansion would trigger a severe, unjustified compliance burden.

High-Risk Classification Under Article 6(1) and Annex I

Article 6(1) classifies systems as high-risk if they are embedded as safety components in products covered by the Union harmonization legislation listed in Annex I and require a third-party conformity assessment. The organization argues that the rationale must remain strictly cumulative: safety impact alone should never trigger a high-risk status if the underlying sectoral rules do not require third-party verification for that product category. Interpretation of a safety component must be tightly bound to prevent administrative overreach regarding non-embedded, diagnostic, and informational workplace software tools. Ensuring standalone risk assessment and diagnostic systems are kept outside Article 6(1) avoids regulatory overlap and excessive compliance pathways that stall asset modernization. Clarifying boundaries ensures software providing informational advice, logging metrics, or monitoring passive risks without autonomously driving irreversible physical control loops is not a high-risk safety component.

Further demanded exclusions encompass systems mapping gas concentrations, microclimate variations, or ambient noise levels, alongside camera software detecting visual obstructions in hazard zones and thermal imaging software monitoring panel overheating.

High-Risk Classification Under Article 6(2) and Annex III

Article 6(2) addresses standalone applications that pose significant risks to safety or fundamental rights within targeted use-case areas. The network pushes for a rigorous, legally sound framework to define the phrase intended to be used. The guidelines must create a clear division based on the functional architecture and purpose of the software, separating structural prevention from individual punitive monitoring. To prevent horizontal definitions from becoming overly broad, the text must specify that a system is only intended to be used for an Annex III use-case if the core operational programming directly impacts workers career trajectories, promotions,

task assignments, or disciplinary terms. Conversely, punitive individual monitoring requires mandatory inclusion.

Evaluation and Long-Term Legislative Amendments

Examining the annual review process mandated under Article 112(1), the submission addresses structural gaps in the text of the Artificial Intelligence Act itself, presenting clear arguments for refining text granularity and closing emerging biometric loopholes.

The current phrasing in Annex III, which covers systems used to monitor and evaluate the performance and behavior of workers, lacks the technical granularity required to separate structural diagnostics from punitive individual surveillance.

Rather than removing use cases entirely, which would create a dangerous regulatory vacuum for truly invasive tools, the association formally advocates for a legislative amendment to explicitly carve out systems intended solely for passive safety diagnostics, ergonomic risk reduction, or environmental hazard mapping that lack the functional capacity for individual productivity sifting. Protecting cognitive liberty requires expanding Article 5 prohibitions. An open regulatory loophole regarding cognitive monitoring exists, prompting the advocacy for an expansion of the prohibited practices list to include compulsory neuro-monitoring in the workplace. Coerced neuro-surveillance represents an unprecedented intrusion into mental privacy that goes far beyond traditional physical monitoring. Explicitly adding the practice to Article 5 is necessary to protect human dignity, cognitive autonomy, and mental integrity under the European Union Charter of Fundamental Rights, ensuring human thought processes are never treated as exploitable performance metrics.

Strategic Conclusions and Operational Pillars

The strategic framework is designed to harmonize regulatory compliance with operational safety. The position rests on three fundamental pillars.

- Clarification of definitions remains imperative to establish a clear legal distinction between deterministic, rule-based industrial automation and advanced technology. Explicitly exempting static safety components such as hardcoded interlocks and presence-sensing devices prevents disproportionate administrative burdens that would otherwise stifle modernization and safety upgrades within small and medium-sized enterprises.

- Risk-based classification requires a rigorous interpretation of Annex I and Annex III. Diagnostic, informational, and passive occupational health tools must be excluded from high-risk categorization, as they function as technical controls rather than mechanisms for performance appraisal or worker surveillance.

- Finally, to ensure the future European workplace remains centered on human dignity, expanding Article 5 to explicitly prohibit compulsory neuro-monitoring guarantees that digital advancement never infringes upon the fundamental privacy of the individual.