

FROM THE DIRECTIVE TO THE MACHINERY REGULATION: IMPLICATIONS, CHALLENGES AND IMPACTS OF DIGITALISATION, AI AND SAFETY IN EUROPEAN INDUSTRY

Adriano A. Santos^{1,2}[0000-0001-8991-6768], Gonalo Pinho¹, Filipe Pereira^{1,2}[0000-0001-7809-5554], Ant3nio F. da Silva^{1,2}[0000-0003-2067-7601], Paulo J. Silva³[0000-0002-9879-8414], Margarida Pinto¹[0009-0004-2688-0752], Carlos Felgueiras³[0000-0002-4202-5551]

¹ISEP, Polytechnic of Porto, rua Dr. Ant3nio Bernardino de Almeida, 4249-015 Porto, Portugal

²INEGI, Institute of Science and Innovation in Mechanical Engineering and Industrial Engineering,
rua. Dr. Roberto Frias, 4200-465 Porto, Portugal

³CIETI, ISEP, Polytechnic of Porto, rua Dr. Ant3nio Bernardino de Almeida, 4249-015 Porto, Portugal

E-mail(s): ads@isep.ipp.pt , 1240113@isep.ipp.pt, fal@isep.ipp.pt,
afs@isep.ipp.pt, 1190053@isep.ipp.pt, mcf@isep.ipp.pt

Abstract - The current industrial paradigm, commonly referred to as Industry 4.0, is characterized by the interconnection of cyber-physical systems (CPS), artificial intelligence and connectivity on the shop floor. This technological evolution brings benefits in terms of efficiency and flexibility, but at the same time introduces security challenges that existing regulatory frameworks do not anticipate. The recent publication of Regulation from European Union (EU) 2023/1230, which replaces the current Directive 2006/42/EC, represents the legislative response to these new challenges by imposing new requirements in the areas of cybersecurity, safety-critical software and machine learning systems. The main aim of this paper is to carry out a comparative analysis between Directive 2006/42/EC and the new EU Regulation 2023/1230 given the recent shifts in the industrial paradigm, particularly due to the emergence of Industry 4.0 and 5.0, which are manifesting themselves in the areas of industrial automation, cyber-physical systems, digitalization and artificial intelligence, technical challenges have arisen that are reflected in the gaps in the current Machinery Directive (2006/427/EC). This article aims to analyze emerging technological challenges, with a particular focus on the risks associated with collaborative robotics, cybersecurity and machine learning systems, by systematizing the necessary knowledge and highlighting the gaps in the current directive, thereby demonstrating how the new regulation aims to address these new security challenges.

Keywords: Machinery Directive, Machinery Regulation, Industry 4.0 and 5.0, Industrial Automation, Collaborative Robotics, Cybersecurity.

1. Introduction

Throughout history, humanity has reinvented itself whilst simultaneously refining its industrial capabilities, driven by the emergence of new resources and technologies. The development of automation systems and control techniques has played a crucial role in this process, helping to create a more stable and efficient world [1].

The industrial revolutions forced humanity to adapt to make the most of technological advances [2], using them efficiently and safely. In this context, the evolution of industrial automation is directly linked to the industrial revolutions, each of which is

characterized by technological leaps that led to paradigm shifts in production systems. The First Industrial Revolution was marked by mechanization, the Second by the intensive use of electricity and mass production, and the Third by digitization and electronics-based automation [3]. However, recent developments in industrial automation have not been limited to increased efficiency but have also brought about a structural shift in the way production systems are designed and operated. This transition is characterized by two complementary paradigms: Industry 4.0, which focuses on digitization and interconnectivity, and Industry 5.0, which shifts the technological focus toward

sustainability, resilience, and human-centeredness. *Figure 1* illustrates the transformations across paradigms, according to key stakeholders and industry segments, to achieve the best industrial results from the following perspectives: people, organization, and technology.

An analysis of *Figure 1* shows that the role of the operator has undergone a clear transition, evolving from a mere performer of manual or assisted tasks to a worker who operates using augmented reality and collaborative systems in an era supported by cyber-physical systems. According to Zizic et al. [4] this transformation becomes more evident when comparing the shift toward smart factories and the decentralization of information-based decision-making (Industry 4.0) with the reintegration of the human factor into the process (Industry 5.0). In this new context, technology is no longer merely a tool for automation but has become a collaborative element, where skilled workers operate side by side with autonomous systems and augmented technologies, requiring a new approach to safety that goes beyond simple physical segregation.

1.1 Paradigms of Industry 5.0

The European Commission [5], officially defined the Industry 5.0 (I5.0) paradigm based on three fundamental pillars: a human-centered approach, sustainability, and resilience. This definition proposes a more humane, sustainable, and resilient vision by recognizing industry's role in promoting social and environmental goals, placing worker well-being at the center of the production process, and encouraging respect for the planet's limits.

This new concept also emerges as a response to recent challenges, such as the need to make supply chains more resilient, adopt circular economy models,

and reduce dependence on non-renewable resources, aligning with the European Green Deal and the lessons of the COVID-19 pandemic [6].

Technology should enhance capabilities rather than replace them, and promote safer, more ergonomic and more satisfying working environments [7] where operators work alongside collaborative systems, with robots performing repetitive, physically demanding, or dangerous tasks, while humans focus on activities that require dexterity, perception, and decision-making [8]. Technologies such as digital twins, artificial intelligence, and cyber-physical systems - already present in Industry 4.0 (I4.0) - are being repurposed to address sustainability goals, such as optimizing energy consumption, predicting failures, and customizing products to avoid overproduction [7]. On the other hand, organizations must adapt to disruptions such as economic crises, pandemics, supply chain disruptions, or extreme weather events, and make their systems resilient by combining system flexibility with human creativity in problem-solving [5], [6].

This paradigm shift has direct implications for the European regulatory framework, particularly the Machinery Directive. The new Regulation (EU) 2023/1230 brings this vision to fruition by introducing and strengthening specific safety requirements that protect not only physical integrity but also the psychological and cognitive well-being of operators in collaborative environments, such as human-robot collaboration (HRC), thereby aligning the law with the principles of Industry 5.0 [9].

This article is structured as follows: Section 2 outlines the importance of regulation, focusing on the evolution of the legislation, the challenges involved, and the transition to the new regulation. Section 3 provides the conclusion of the paper.

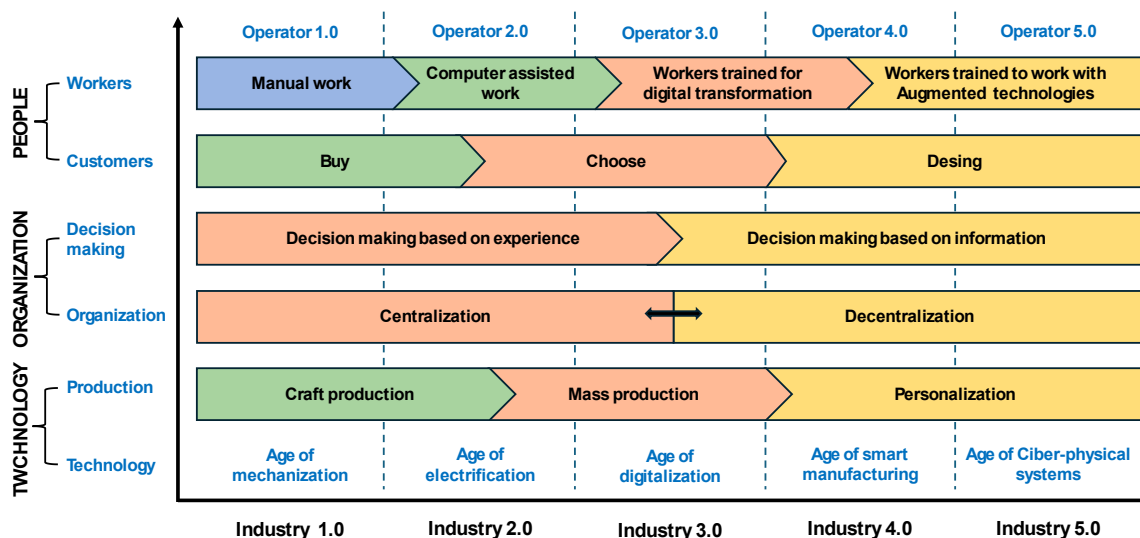


Figure 1: The Evolution of Industry, adapted from [4]

2. The Importance of Machinery Regulation

The pillars underpinning Industry 5.0 have direct implications for the regulatory framework governing the design, manufacture, and marketing of machinery in the European market. The digitization, connectivity, and autonomy of systems raise new challenges regarding worker safety and well-being, which must be addressed in new legislation, as existing legal frameworks do not account for such systems as cyber-physical systems and artificial intelligence. The following sections will analyze regulatory developments, with a particular focus on the requirements applicable to control and safety systems in industrial automation environments.

2.1 Development of Legislation

The European Machinery Safety Regulation originated in the 1980s, when the strategy known as the “New Approach” was adopted, establishing innovative principles for technical harmonization within the European Union (EU) market [10]. This approach introduced a model for technical harmonization that is characterized by three fundamental principles defined by the European Commission [11]:

- **Essential requirements**

They define only the Essential Health and Safety Requirements (EHSR), which are formulated as objectives to be achieved, without specifying particular technical solutions. This approach provides flexibility to accommodate different technologies and allows for innovation without the need for constant legislative revisions.

- **Harmonized Standards**

They delegate the detailed technical specifications to harmonized European standards developed by standardization bodies, such as the European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC), and European Telecommunications Standards Institute (ETSI). Compliance with these standards is voluntary and helps establish a presumption that the requirements are being met, thereby simplifying the evaluation process.

- **Conformity Assessment**

It establishes risk-based conformity assessment procedures. Once these procedures are successfully completed, the product receives the CE marking, which allows it to circulate freely and be marketed within the European market.

Directive 89/392/EEC, published on June 14, 1989, established for the first time a harmonized

regulatory framework for machinery at the European level. This directive defined essential safety requirements applicable to the design and manufacture of machinery, introducing concepts such as mandatory risk assessment, the hierarchy of protective measures, and the procedures for CE marking compliance.

Directive 98/37/EC, which entered into force in 1995, consolidated the original directive by broadening its scope and clarifying definitions. This directive introduced more explicit requirements for lifting equipment, safety components, and machinery presenting specific risks.

However, Directive 2006/42/EC, which has been in force since 2009, represented a significant change from its predecessors by clarifying its scope, introducing the concept of “quasi-machine”, strengthening the assessment procedures for high-risk machinery, and updating the requirements considering technological developments in the 1990s [12]. It remained in effect for 15 years, a period during which the industry underwent profound changes associated with Industry 4.0.

The European Commission’s Regulatory Fitness and Performance (REFIT) evaluation (2018–2019) concludes that, despite technological developments in recent years, the directive’s objectives and principles remained valid, but gaps had emerged regarding digitization and software, connectivity and cybersecurity [17], artificial intelligence, and autonomy [13]. This assessment led to the adoption of EU Regulation 2023/1230, which was published in June 2023 and will take effect in January 2027 [9]. As such, the transition from a directive to a regulation represents a shift in legislative instruments, whereby regulations are directly applicable in all member states without the need for national transposition, ensuring complete uniformity in their application.

2.2 New Challenges

The transition to Industry 4.0 has exposed significant limitations in the regulatory framework for machinery, which was designed in an era when machines were predominantly mechanical and electromechanical systems. These limitations are defined at the level of:

Software and programmable systems

The growing reliance on software for critical safety functions represents a paradigm shift. Programmable Logic Controllers (PLCs), embedded systems, human-machine interfaces (HMIs), SCADA systems, and fault-tolerant systems [14], perform functions that directly affect user safety. Directive 2006/42/EC refers to programmable systems only in general terms, without establishing specific

requirements for the development, validation, and updating of safety software [12]. However, while harmonized standards such as EN ISO 13849-1 and EN IEC 62061 already include requirements for safety software, their application is not mandatory under the directive. The REFIT evaluation identified this gap as a priority area for review [13].

Connectivity and Cybersecurity

The integration of machines into industrial networks and their connection to the internet have introduced new potential points of vulnerability that did not exist in conventional and isolated machines. In this context, Humayed et al. [15] identified a number of specific vulnerabilities associated with industrial environments, such as: industrial communication protocols lacking robust authentication mechanisms; the use of obsolete systems designed in a pre-connectivity era that are unable to receive security updates; and the growing convergence between field technology networks and information technology networks—which are used for corporate functions—exposing systems to threats. In turn, Yaacoub et al. [16] have shown that attacks on industrial control systems can have direct physical consequences, extending beyond the traditional realm of cybersecurity and directly affecting the safety of people and equipment [17]. They also state that among the various types of attacks are *spoofing*—that is, masking the identity of sensors or controllers and sending false data, leading to the manipulation or physical destruction of components—and service *disruption*, resulting from physical or digital tampering with devices that causes operational shutdowns, as well as *tracking*, which exploits physical access to devices in order to track or tamper with them.

Directive 2006/42/EC does not address cybersecurity risks, reflecting an era when machines operated in isolation or on closed proprietary networks. This gap was explicitly identified in the REFIT evaluation as a priority area for revision [13].

Artificial intelligence

The integration of artificial intelligence (AI) systems and the use of machine learning algorithms in industrial machinery pose one of the most complex challenges for the existing regulatory framework [18][19]. Unlike traditional programmable systems, whose behavior is deterministic and predictable, AI-based systems can autonomously modify their operating parameters, introducing adaptive behaviors that will not be fully predictable at the time of conformity assessment. This leads to a lack of transparency in the algorithms and makes it impossible to predict all possible states of a system that evolves as new data is added, thereby compromising the ability to ensure ongoing compliance after the system goes live [20].

Collaborative robotics

Collaborative robotics has brought about a paradigm shift in industrial safety, moving from physical segregation to interaction management. This proximity eliminates traditional protective barriers, exposing the operator to new risks of mechanical contact that require rigorous validation. In this context, collision management emerges as the central challenge of collaborative safety and, as such, requires real-time control capable of limiting kinetic energy and impact force to levels tolerable by the human body, as technically defined in the ISO/TS 15066 standard. However, the variability of human behavior makes it difficult to model all possible interactions, requiring advanced perception systems that not only detect presence but also predict the operator's intended movement to avoid accidental contact [21]. In this situation, rather than physical segregation between the operator and hazardous movements, the collaborative cell is based on the controlled coexistence of the operator and the robot, achieved through dynamic management of the robot's behavior.

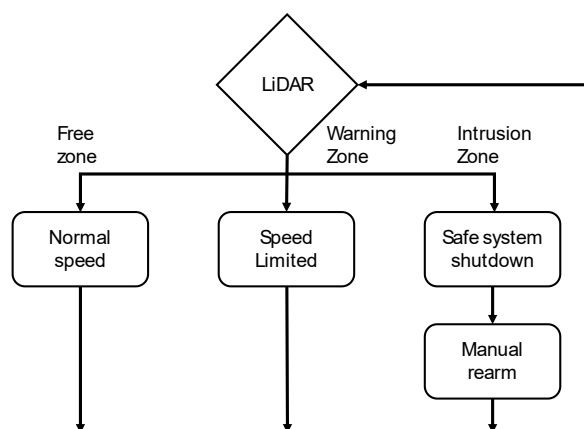


Figure 2: LiDAR action Flowchart

The robot must detect human presence, reduce its speed, and, if necessary, come to a controlled stop before any unauthorized approach. The diagram shown in Figure 2 illustrates the cell's various behaviors. Adjustments may include reducing speed, restricting the trajectory, or bringing the cell to a safe stop, depending on the configuration adopted. Therefore, the human presence-monitored stop function is designed to place the robot in a safe state when the operator's presence is detected in a situation that is incompatible with the robot's current movement. This function activates when the LiDAR (Light Detection and Ranging) sensors detect a person entering the defined intrusion zones and operates according to the diagram shown in Figure 2. Figure 3 shows a possible implementation diagram for LiDAR sensors.

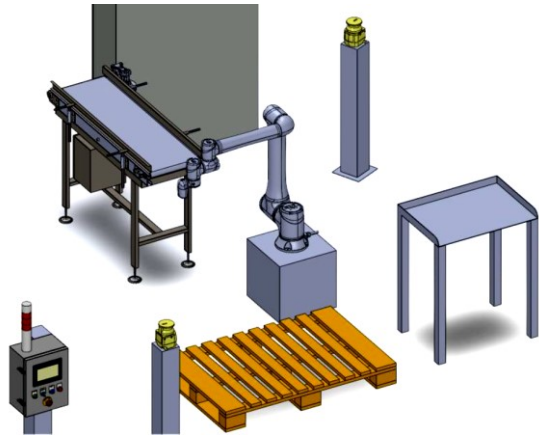


Figure 3: Lidar Sensor Position.

2.3 Transition to the Regulation

The transition from Directive 2006/42/EC to the new Regulation (EU) 2023/1230 represents not merely a technical update, but a fundamental shift in the philosophy of oversight and compliance.

The Directive, which has been in force since 2009, sets out the essential health and safety requirements applicable to the design and manufacture of machinery, safety components, lifting accessories, transmission components, removable mechanical transmission equipment, quasi-machines [12]. This model, based on essential generic requirements supplemented by harmonized technical standards, makes a significant contribution to reducing the number of accidents and the social cost of accidents and damage to health [22]. On the other hand, the technical principles set out in Annexes I and II of the Directive, in particular the requirements concerning the reliability of control systems, emergency stop devices and the priority of safety functions over operational functions, remain conceptually valid and form the basis of modern safety engineering [11]. These safety function techniques involve the selection and integration of appropriate devices; the compliance of the solution depends on the individual compliance of the components, the functional consistency of the adopted architecture, and its ability to maintain a safe state in the face of foreseeable failures [23]. Figure 4 shows one possible configuration for containing hazardous zones, ensured by fixed perimeter guards and access points controlled by interlocking devices. This functionality introduces a connectivity aspect that must be considered from a safety perspective, particularly regarding protection against unauthorized access, as addressed in the new Regulation (EU) 2023/1230.

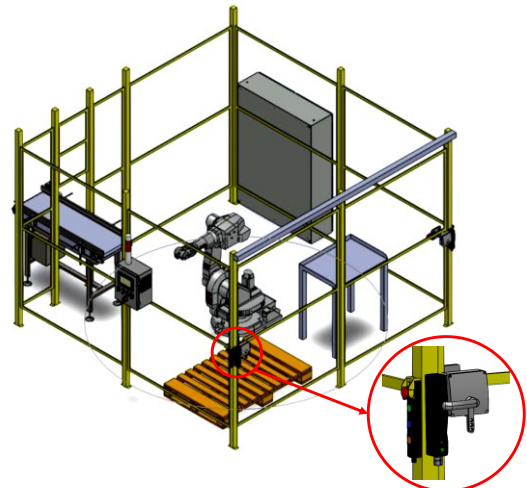


Figure 4: Fixed perimeter barriers and a close-up of the delayed-action latch.

Although the safety provisions were validated, the European Commission's REFIT review confirmed that, whilst the structure of the Directive remained adequate for traditional mechanical risks, there were critical gaps in addressing emerging risks. The legal uncertainty surrounding the status of security software, the lack of explicit cybersecurity requirements, and the difficulty in regulating autonomous systems have been identified as barriers to innovation and potential risks to users, highlighting the need for legislative reform [13], no with respect to the risk assessment covering automatic operation, transient states, and reasonably foreseeable misuse scenarios [24].

The change from a directive to a regulation aims to ensure uniform application across all Member States by eliminating the variations resulting from the transposition of the directive into national law, thereby addressing the identified shortcomings [9].

In the field of software, the Regulation introduces a structural change by classifying, in Annex I [9], explicitly defines software that performs safety functions as a 'safety component'. This means that the computer code is now subject to the same conformity assessment and CE marking requirements as physical components and must be developed in accordance with the state of the art in functional safety.

Regarding cybersecurity, the new essential requirement 1.1.9 "Protection against corruption" in Annex III [9] fills the previous legislative gap. This requirement obliges manufacturers to design machinery in such a way that connection to other devices or networks does not compromise safety functions.

It is therefore essential to implement measures to prevent unauthorized access and to ensure that any data intrusion or corruption, whether accidental or intentional, does not lead to dangerous situations. However, for systems that are fully or partially self-evolving, the regulation stipulates that data relating to decision-making by safety functions must be retained for a period of one year following their collection, solely for the purpose of demonstrating compliance to the competent authorities.

Legislative framework

Directive 2006/42/EC consists of 29 articles, supplemented by 12 technical annexes. The introductory articles define the scope and terms, whilst the core regulatory provisions set out the fundamental obligations for placing machinery on the market, focusing on the essential health and safety requirements, the design and manufacture of machinery, conformity assessment procedures and the requirements for notified bodies [12], neglecting importers and distributors.

The regulation introduced, as a structural innovation, dynamic updating mechanisms that give the European Commission the ability to adapt specific technical requirements without the need for a full legislative review [9].

Scope of application

Directive 2006/42/EC applies to machinery, interchangeable equipment, safety components, lifting accessories, chains, ropes, belts, removable mechanical transmission devices and quasi-machines. Articles 1 and 2 exclude from their scope various categories of products that are already covered by specific sectoral legislation [12]. However, the transition to Regulation (EU) 2023/1230 retained the scope of application, preserving the main exclusions set out in the directive. Nevertheless, the regulation clarifies borderline cases that had given rise to differing interpretations among Member States. By treating security software as a product subject to CE marking, and by explicitly including machines with autonomous mobility and connectivity, the Regulation removes the interpretative uncertainties that exist among Member States regarding the applicability of the law to these new technologies [9].

Key definitions

The transition to Regulation (EU) 2023/1230 has retained most of the definitions from the Directive, such as the definition of a machine, which, according to [12], is defined as: *'an assembly equipped with, or intended to be equipped with, a drive system other than directly applied human or animal power, consisting of parts or components connected to one*

another, at least one of which is movable'. The concept of a quasi-machine has also remained unchanged and is defined as an *"assembly that constitutes a partly completed machine but which, on its own, cannot perform a specific function"* [9].

The definition of a safety component also remains unchanged, namely *"a component that is not an interchangeable part"* [9], which the manufacturer places on the market with the intention that it should perform a safety function during use, and whose failure or malfunction endangers the safety of users. To address this issue of safety, the Regulation introduces a new legal definition of *'substantial modification'*, thereby clarifying the legal uncertainty surrounding modified machinery and the need for a new CE marking. With this new definition, the Regulation clarifies that a *"modification is substantial when it creates hazards or leads to an increase in existing risks, affecting safety, thereby necessitating new protective measures"*; consequently, this new definition requires the modifier to assume the obligations of a manufacturer [9].

A new definition clarifies, for the first time, the concept of *'safety-related software'*, the operation or failure of which may directly affect the safety of persons exposed to the risks posed by the machinery, thereby removing the ambiguity in the Directive, which previously contained only generic references to *'logic software (programming)'* [12], without establishing clear identification criteria or specific requirements. The introduction of this definition will have practical implications, as it will make it mandatory to explicitly identify safety-related software in the technical documentation (clearly distinguishing software that performs safety functions from auxiliary software that has no impact on safety) and, at the same time, requires that the software be developed in accordance with the state of the art.

Machine learning is a system which, based on data analysis during operation, can autonomously modify its operating parameters or behavior [9]. This definition becomes crucial when new monitoring requirements and decision thresholds are introduced, ensuring that the development of machine intelligence never exceeds the safety limits initially validated.

Regarding cybersecurity, the regulation does not introduce a formal definition, but its articles and annexes incorporate concepts relating to protection against accidental or intentional corruption of safety functions, covering vulnerabilities introduced by the connectivity of machinery to industrial networks. This requirement stipulates that machinery must be designed and manufactured in such a way that [9]:

- Access to security functions is protected against unauthorized access;
- As interfaces de communication do not compromise the integrity of security functions;
- It should be possible to collect data when there is a “legitimate or illegitimate” interference with a connection or access to software.

Whereas the behavior of the machine must always be predictable when controlled by self-adaptive systems. Classifying these machines as high-risk and requiring that their validation be carried out by notified bodies.

2.4 Human-Machine Interaction

The Regulation marks a paradigm shift from the Directive regarding human-machine interaction. The Directive focused on preventing access to hazardous areas, whereas the Regulation recognizes human-machine interaction and the need to adapt risk prevention measures without relying entirely on physical isolation, if safety is guaranteed [16]. This includes the prevention of psychological stress that may result from human-machine interaction and from autonomous or partially autonomous systems, requiring the manufacturer to consider risk assessment not only physical harm, but also the cognitive stress and anxiety that the proximity of an autonomous machine may cause to the human operator. Regarding autonomous mobile machines, the regulation stipulates that these machines must be able to move around safely, requiring the technical capability to detect people or obstacles in their path and to come to a halt autonomously to avoid collisions [9].

The Regulation has introduced stricter new risk classification criteria by limiting manufacturers' autonomy in validating compliance.

2.5 Summary of the Transition

Table 1 provides an overview of the transition from Directive 2006/42/EC to Regulation (EU) 2023/1230. This highlights the responses to the ambiguities identified previously and is supplemented by the new risks associated with the digital dimension. In Figure 5, although it presents a bibliometric analysis of keyword co-occurrence using VOSviewer software, the co-occurrence network illustrates two main groups, Industry 4.0 and Industry 5.0, which reflect this transition to the new regulation.

An analysis of the previous figure shows that the green cluster focuses on Industry 4.0 and the technologies associated with it, whilst the red cluster links the industrial revolution to Industry 5.0 and incorporates aspects of automation and digitalization.

Also noteworthy, in a smaller branch, collaborative robotics is associated with risk assessment, which highlights that the introduction of cobots into shared environments is a key safety concern. It is also worth noting the key points of the transition between Industry 4.0 and Industry 5.0, shown in yellow.

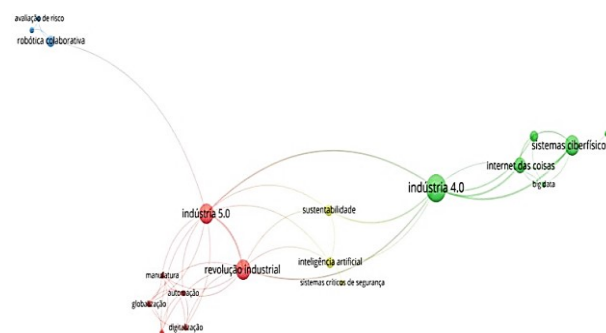


Figure 5: Co-occurrence analysis

3. Conclusions

A comprehensive analysis of the European regulatory framework reveals that the current regulatory safety model is outdated. Directive 2006/42/EC was designed for a static world, in which a machine, once certified, is assumed to maintain its behavior unchanged throughout its service life. The integration of autonomous systems and machine learning challenges this assumption. It follows, therefore, that security ceases to be a static property and becomes a dynamic one, limiting the degree of autonomy in machine learning.

The distinction between functional safety and information security has become inseparable in the era of Industry 4.0. However, the regulation's new legal framework demonstrates that, in a CPS environment, a digital attack can have direct physical consequences, thereby compromising safety. Furthermore, the regulation's new essential requirement, 'Protection against corruption', establishes that there can be no legal compliance without digital integrity.

The introduction of mandatory validation by notified bodies for high-risk devices category which includes new technologies where self-assessment is not feasible, reflects legislative recognition of the complexity of these technologies.

The transition to Regulation (EU) 2023/1230 is not merely a bureaucratic update, but the necessary response to a new paradigm in which machines are connected, intelligent and capable of evolving.

Table 1. A comparative analysis of the Directive and the Regulation

Tema	Directive 2006/42/CE	Regulations 2023/1230	What changes in practice
Legal nature	Transposition into the law of each country. This may give rise to differences in interpretation.	Direct application in all EU Member States, ensuring complete uniformity.	Uniform rules across the EU, with no national variations.
Cybersecurity	Not explicitly addressed, focusing solely on functional safety.	Essential and mandatory requirement.	Connected machines must prevent unauthorized access and manipulation.
Software and AI	No explicit reference, limited references.	Specific rules regarding AI, autonomy and remote updates.	Enhanced risk assessment for smart systems.
High-risk machinery	Old self-assessment checklist based on harmonized standards.	Updated list and mandatory assessment by a certified body.	Some equipment will now require external certification.
Documentation	Paper manual required.	Digital manual available (paper version on request).	Cost reduction and document modernization. Requirement for source code or programmed logic.
Quasi-machines	Less clear requirements	More detailed rules and enhanced technical documentation	More secure and traceable integration in the final assembly.
Responsibilities of economic operators	Less detailed, with a focus on the manufacturer's obligations.	Extended obligations for manufacturers, importers and distributors.	Greater traceability, control and legal accountability.
Software updates	Unregulated.	They must ensure safety and not introduce new risks	Manufacturers are now responsible for security updates.
Conformity assessment	Based on harmonized standards.	Enhanced for high-risk categories.	Stricter procedures for certain products.
Substantial Change	Concept not legally defined.	Clarification of the concept of modification.	Requires a new CE marking.
Application dates	—	Phased implementation between 2025 and 2028	Transition period to allow the industry to adapt.

An analysis of the current gaps suggests that future work should focus primarily on the technical implementation of the new legal requirements, translating the principles of the new regulation into verifiable engineering procedures on the shop floor. In this way, robust operational plans can be developed to help ensure that legal compliance is aligned with practical reality. Prioritize the development of metrics and mechanisms for the ongoing validation of autonomous and machine-learning systems, as well as the conduct of case studies in a real-world industrial environment to assess the economic and operational impact of the new requirements imposed by the regulation, and to evaluate the actual effectiveness of the proposed measures.

Acknowledgement

The authors acknowledge Fundação para a Ciência e a Tecnologia (FCT) for its financial support to LAETA R&I via the project UID/50022/2025 (<https://doi.org/10.54499/UID/50022/2025>).

References

- [1] P. P. Groumpos (2021). A Critical Historical and Scientific Overview of all Industrial Revolutions. *IFAC-PapersOnLine*, 54(13), 464-471. <https://doi.org/10.1016/j.ifacol.2021.10.492>
- [2] Schwab, K. (2016) The Fourth Industrial Revolution. *World Economic Forum*, https://law.unimelb.edu.au/data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf, accessed on 09 June 2026.
- [3] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann (2014). "Industry 4.0," *Bus. Inf. Syst. Eng.*, 6, 239-242. <https://doi.org/10.1007/s12599-014-0334-4>.
- [4] Zizic, M. C., Mladineo, M., Gjeldum, N., & Celent, L. (2022). From Industry 4.0 towards Industry 5.0: A Review and Analysis of Paradigm Shift for the People, Organization and Technology. *Energies*, 15(14), 5221. <https://doi.org/10.3390/en15145221>
- [5] Directorate-General for Research and Innovation (2021). Industry 5.0 - Towards a sustainable, human-centric and resilient European industry. <https://research-and->

- innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en, accessed on 09 June 2026.
- [6] Xun Xu, Yuqian Lu, Birgit Vogel-Heuser, Lihui Wang (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. *Journal of Manufacturing Systems*, 61, 530-535. <https://doi.org/10.1016/j.jmsy.2021.10.006>.
- [7] Praveen Kumar Reddy Maddikunta et al. (2022). Industry 5.0: A survey on enabling technologies and potential applications. *Journal of Industrial Information Integration*, 26. <https://doi.org/10.1016/j.jii.2021.100257>.
- [8] Nahavandi, S. (2019). Industry 5.0—A Human-Centric Solution. *Sustainability*, 11(16), 4371. <https://doi.org/10.3390/su11164371>.
- [9] European Parliament and Council of the European Union (2023). Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC. *Official Journal of the European Union*, L 165/1, 1-102. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1230>.
- [10] Council of the European Communities (1985). Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards. *Official Journal of the European Communities*. <https://eur-lex.europa.eu/legal-content/mt/LSU/?uri=CELEX%3A31985Y0604%2801%29>, accessed on 10 June 2026.
- [11] European Commission (2022). The 'Blue Guide' on the implementation of EU product rules 2022. *Official Journal of the European Union*, C 247/1. <https://www.ibf-solutions.com/fileadmin/dateidownloads/amtsblaetter/the-blueguide-on-the-implementation-of-eu-products-rules-2022.pdf>, accessed on 10 June 2026.
- [12] European Parliament and Council of the European Union (2026). Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC. *Official Journal of the European Union*, L0042. file:///C:/Users/ads25/Downloads/directive%20200642ec%20of%20the%20european%20parliament%20and-DOC_1.pdf, accessed on 10 June 2026.
- [13] Grow, A. (2018). Evaluation of the Machinery Directive 2006/42/EC. *European Commission*. file:///C:/Users/ads25/Downloads/swd-2018-160_en.pdf, accessed on 10 June 2026.
- [14] A. A. Santos, M. de Sousa (2008). Framework for management of replicated IEC 61499 applications. *2008 IEEE International Conference on Emerging Technologies and Factory Automation*, Hamburg, Germany, pp. 200-206. <https://doi.org/10.1109/ETFA.2008.4638393>.
- [15] A. Humayed, J. Lin, F. Li and B. Luo (2017). Cyber-Physical Systems Security—A Survey. In *IEEE Internet of Things Journal*, 4(6), 1802-1831. <https://doi.org/10.1109/IIOT.2017.2703172>.
- [16] Jean-Paul A. Yaacoub et al. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, 77, 103201. <https://doi.org/10.1016/j.micpro.2020.103201>.
- [17] Kasprzyczak, L., Manowska, A., & Dźwiarek, M. (2025). Cybersecurity Requirements for Industrial Machine Control Systems. *Applied Sciences*, 15(3), 1267. <https://doi.org/10.3390/app15031267>.
- [18] Kaur, R., Kumar, R. & Aggarwal, H (2025). Systematic Review of Artificial Intelligence, Machine Learning, and Deep Learning in Machining Operations: Advancements, Challenges, and Future Directions. *Arch Computat Methods Eng* 32, 4983–5036. <https://doi.org/10.1007/s11831-025-10290-z>.
- [19] Daniel Oliveira Cajueiro, Victor Rafael Rezende Celestino (2026). A comprehensive review of Artificial Intelligence regulation: Weighing ethical principles and innovation. *Journal of Economy and Technology*, 4, 77-91. <https://doi.org/10.1016/j.ject.2025.07.001>.
- [20] Yue Wang, Sai Ho Chung (2021). Artificial intelligence in safety-critical systems: a systematic review. *Industrial Management & Data Systems*, 122(2), 442-470. <https://doi.org/10.1108/IMDS-07-2021-0419>.
- [21] Peter Chemweno, Liliane Pintelon, Wilm Decre (2020). Orienting safety assurance with outcomes of hazard analysis and risk assessment: A review of the ISO 15066 standard for collaborative robot systems. *Safety Science*, 129. <https://doi.org/10.1016/j.ssci.2020.104832>.
- [22] Grow A. (2024). Guide to application of the Machinery Directive 2006/42/EC, Ed. 2.3. *European Commission*. <https://ec.europa.eu/docsroom/documents/60145>.
- [23] International Organization for Standardization. ISO 13849-1:2023 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design. 2023.
- [24] European Parliament and Council of the European Union. Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC. *Off. J. Eur. Union*, L165, pp. 1–102, 2023.