Smart but Safe: How Industrial AI Challenges Existing Occupational Safety Regulations

Dagmar Gesmann-Nuissl[1,*], Stefanie Meyer[1,*]

[1]Professorship for Private Law and Intellectual Property Rights, Chemnitz University of Technology, Germany

Abstract

Increasing automation and the use of AI-controlled robot systems in industry are boosting efficiency, but they also pose new risks to occupational safety. Interacting with adaptive machines in atypical situations such as maintenance or conversion work, where both in-house employees and contractors are potentially at risk, is particularly problematic. This article analyzes the existing occupational safety framework and identifies gaps, particularly with regard to the dynamic hazards posed by adaptive AI systems. It discusses the role of "AI literacy" as defined in Article 4 of the EU AI Act, which requires the qualified involvement of all users, including external service providers. Existing national laws and regulations currently provide insufficient tools to meet the specific requirements of adaptive systems. To strengthen the protection of all workers in AI-supported work environments, a combination of continuous risk assessment, targeted training, and organizational measures is therefore recommended. The integration of AI literacy requirements into national occupational safety and health regulations could be an important contribution in the future.

Keywords

industrial AI, adaptive AI systems, occupational safety regulations, AI literacy

"An ounce of prevention is worth a pound of cure"
Benjamin Franklin, 1735

1. Introduction

As robotics and artificial intelligence (AI) become increasingly integrated into industrial processes, companies and legislators are facing new challenges. While automation and intelligent machines contribute to greater efficiency[1][2], they also pose significant risks to occupational safety – especially in situations that occur beyond the scope of regular operations. This is particularly relevant in the context of external companies: Not only a company's own employees, but also, increasingly, external service providers in the areas of maintenance, repair, or technical installation come into contact with adaptive machines – and are exposed to particular hazards. A striking example is the fatal accident involving an employee of an external company at the Volkswagen plant in Baunatal in 2015. The technician was setting up a robot inside a protective fence when the machine caught him and pressed him against a metal plate[3]. The robot, which was originally programmed for a specific, defined work process, had acted unexpectedly due to a configuration error. The case makes it clear that it is not enough to assign responsibility for safety risks to the manufacturer alone – rather, an integrative occupational safety framework is needed that also addresses new technologies and their dynamic behavior. The aim of this contribution is therefore to examine the occupational safety framework for the use of AI-controlled robot systems and to identify existing gaps. Particular attention is paid to the role of third parties and the challenges in atypical work situations, such as malfunctions, maintenance, or conversions[4][5]. The central question is whether and how the new "AI literacy" requirement under Article 4 of the Regulation (EU) 2024/1689 (AI Act) – i.e., the ability to safely and effectively interact with AI systems – needs to be integrated into existing occupational safety regulations. Alternatively, it should be examined whether recourse to manufacturer responsibility within the scope of the Machinery

BEHAIV-2025: AI for understanding human behavior in professional settings, 25 October 2025, Bologna, Italy.
*Corresponding author.
dagmar.gesmann@wiwi.tu-chemnitz.de (D. Gesmann-Nuissl); stefanie.meyer@wiwi.tu-chemnitz.de (S. Meyer)
0000-0003-0092-7845 (D. Gesmann-Nuissl); 0000-0001-9988-9564 (S. Meyer)

Regulation (in particular through risk-based design and ergonomic requirements[6]) is sufficient to ensure an adequate level of protection for employees of external companies as well.

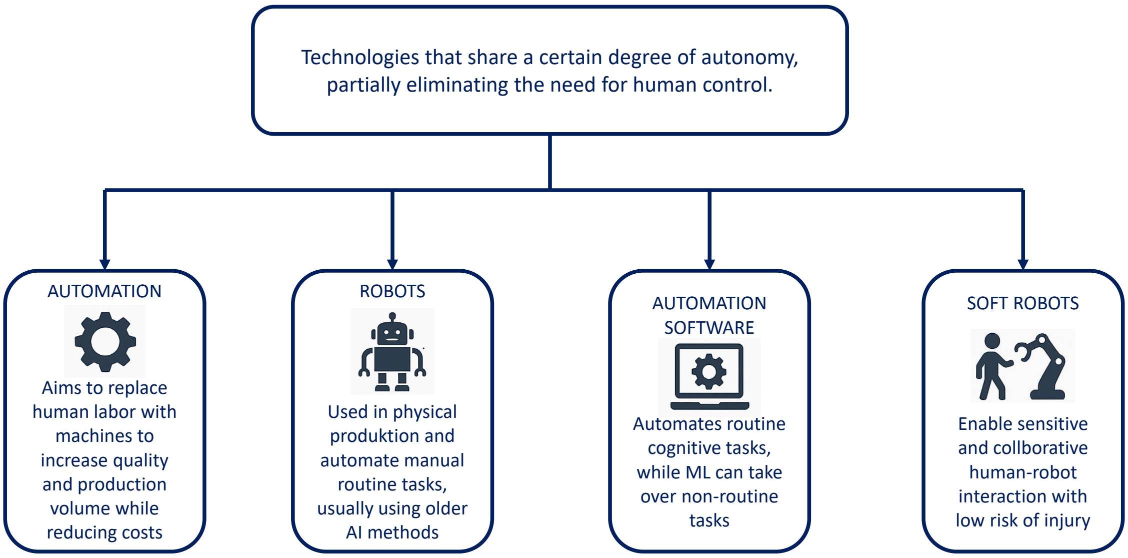

Figure 1: Types of Automation Technologies.

2. Technological Background

The terms "automation," "robotics," and 'digitalization' are often used interchangeably in scientific literature to refer to "AI," even though there are clear differences between them (Figure 1)[7][2]. What these technologies have in common is a degree of autonomy that partially eliminates the need for human control. Automation aims to replace human labor with machines in order to increase quality and production volume while reducing costs[8]. Robots are primarily used in physical production and automate manual routine tasks, mostly using older AI methods[9]. Automation software, such as robot process automation (RPA), automates routine cognitive tasks, while machine learning (ML) can also take over non-routine tasks through independent problem solving[10][11]. Industrial robotics has evolved: "soft robots" enable sensitive and collaborative human-robot interaction with a low risk of injury[12]. Cobots, which work with humans without protective barriers, are an example of this development[4]. While the term robotics is widely established in an industrial context, the definition of AI remains heterogeneous. In a technical and legal sense, AI encompasses programmed systems with their own scope for selection and decision-making, whereby a distinction is made between weak AI, which is limited to specific problem solutions, and strong AI, which is supposed to possess independent consciousness or creativity[13][14][15][16]. AI is manifested in a wide variety of as specified in recitals 4 and 103 of the AI Act: it can take the shape of physically acting robots or purely digital algorithms[17]. A characteristic feature of AI systems is that, despite their programmable foundations, they have a certain degree of autonomy and independent decision-making[17][18]. Modern information technologies not only perform automated functions, but also increasingly fulfill complex information-processing tasks, thereby contributing significantly to the management of multi-layered industrial processes[6].

Examples of such complex information-processing tasks include:

- Real-time object detection and quality control in manufacturing using computer vision;
- Predictive maintenance, where AI analyzes vibration and temperature data from industrial machinery to anticipate failures before they occur;
- Adaptive process control systems that continuously adjust production parameters based on sensor feedback to optimize output;
- Human-machine interaction via natural language processing, such as voice-controlled operator interfaces in control rooms;
- AI-based scheduling and logistics planning systems that coordinate resources across dynamic supply chains.

In industrial applications, AI systems are used in particular in the shape of collaborative robots (cobots), which take over or support monotonous, physically demanding, or cognitively challenging tasks, thereby reducing the workload on human workers[19][20]. They are also used in a wide variety of areas such as quality control, sensor technology, assistance systems, and automated and autonomous processes – for example in the field of driving or production control[21][22]. The interaction between humans and machines is becoming increasingly intuitive and efficient, which contributes to the optimization of operational processes[21].

Examples of intuitive human-machine interaction include:

- Gesture-controlled collaborative robots (cobots), which recognize and respond to human hand movements to coordinate shared tasks without the need for physical interfaces;
- Wearable devices that monitor biometric data such as fatigue or stress levels, dynamically adjusting task assignments or break intervals to prevent overload;
- Augmented reality (AR) systems that project real-time instructions into the worker's field of vision, guiding maintenance or assembly steps interactively and hands-free.

These technologies foster more natural communication between humans and machines, improve operational reliability, and enhance occupational safety in AI-supported workplaces.

Accordingly, the AI Act also refers in Recital 47 to autonomous robots as an example of AI applications, particularly in industrial manufacturing and care. From a legal and technical perspective, it is important to distinguish between classically programmed robots and autonomous AI-driven robots. Classical robots follow pre-defined instructions within fixed parameters and do not adapt their behavior beyond what was explicitly coded. In contrast, autonomous robots – as addressed in the AI Act and Machinery Regulation (see below) – are capable of making decisions or adapting their behavior based on environmental inputs or learned experience. This includes the ability to modify task execution paths, prioritize actions dynamically, or even suspend operations in response to unexpected conditions. These adaptive behaviors shift parts of the control logic from the human operator to the machine itself, which raises new legal challenges in terms of transparency, traceability, and safety obligations. The risks associated with the use of AI include, in particular, inadequate system specification and faulty formulation of the algorithm, as well as risks arising from incorrect use or misuse of the systems[21]. In addition, there are specific risks arising from the nature of AI-based systems, such as unpredictable behavior and the characteristics of self-learning algorithms, whose decision-making processes and adaptations develop dynamically and are sometimes opaque. These special features make it difficult to fully control and evaluate the systems in an occupational safety context. It should also be noted that the risk situation for a company's own employees may differ from that of external contractors, for example due to different instructions, access regulations, or liability issues. Cobots, which are used in close human-robot collaboration, raise complex occupational safety issues concerning the protection of employees and responsibilities in the event of damage or injury[4].

Key risks associated with adaptive AI systems include:

- Unpredictable system behavior due to non-deterministic learning processes;
- Lack of transparency in decision-making (so-called "black box" effects);
- Difficulty in predefining all possible system states or reactions;
- Potential for unintended system adaptation during operation;
- Challenges in assigning responsibility in case of harm or malfunction;
- Insufficient user understanding of dynamic system behavior, especially among external staff;
- Delayed or inadequate human intervention due to overreliance on system autonomy.

3. Legal Framework: Occupational Safety and Product Safety Regulations

Occupational health and safety are closely linked to the Machinery Directive and the upcoming Machinery Regulation. Together, they provide the legal basis for ensuring that machinery is designed safely and can be used safely in the workplace. While the Machinery Regulation – the currently applicable Directive 2006/42/EC is soon to be replaced by Regulation (EU) 2023/1230 – specifies the essential safety requirements for the design and construction of machinery, occupational safety regulations aim to continuously improve working conditions during the operation of such machinery and minimize risks in the workplace. The basis for safety and health at work is provided by Framewokr Directive 89/391/EEC, which has been transposed into national law in all EU member states. This directive establishes minimum requirements for the protection of safety and health, leaving it up to individual countries to adopt or maintain stricter regulations. Against this backdrop, the legal framework for occupational safety and health has so far been shaped primarily at the national level. The following section therefore focuses on the current occupational safety and health requirements in Germany (an overview can be found in Table 1) and examines their applicability to AI-supported systems. Technical diversity and automation make occupational health and safety considerably more difficult, as existing regulations such as the German Occupational Safety and Health Act (ArbSchG), the Industrial Safety Regulation (BetrSichV) and the Workplace Ordinance (ArbStättV) reach their limits when it comes to dynamically learning AI systems [9]. In addition, the complexity of the systems requires transparent design so that employees can understand their tasks and intervene appropriately in the event of malfunctions[6]. According to Sections 618 and 241 (2) of the German Civil Code (BGB), employers are obliged to ensure the safety and health of their employees. In particular, when using industrial robots and AI systems, Section 3 of the BetrSichV requires a comprehensive risk assessment to be carried out before commissioning, taking into account physical and psychological stress as well as ergonomic aspects[20][23]. This risk assessment should ideally be carried out before the work equipment is selected and procured and is to be reviewed and adapted on a regular basis (Section 3 (7) BetrSichV). The use of robots may even be mandatory under occupational safety and health law if they ensure greater safety than traditional methods (Sections 2, 3 ArbSchG)[20]. In addition to technical protective measures, the qualification of employees through regular and comprehensible instruction is of central importance to ensure safe handling[24]. In the case of collaborative robots and AI systems, special requirements have to be met in terms of technical safety, transparency

Legal Source / Norm	Scope / Content
German Civil Code (BGB) – §§ 618, 241(2)	General duty of care and protection by employers
Occupational Safety and Health Act (ArbSchG)	Core German law for workplace safety; mandates comprehensive risk assessments and protective measures
Industrial Safety Regulation (BetrSichV)	Regulates technical safety and mandatory risk assessments before use of equipment; includes psychological stress
Workplace Ordinance (ArbStättV)	Governs ergonomic, technical, and organizational workplace design in digital/flexible environments
Framework Directive 89/391/EEC	EU-wide directive for occupational safety; provides minimum standards to be implemented nationally
AI Act – Regulation (EU) 2024/1689	Regulates AI systems in various risk classes; becomes fully binding in 2026
– Art. 3 No. 4 AI Act	Defines "operator" as responsible entity for deployment and risk management of AI
– Art. 4 AI Act	Introduces obligation to ensure sufficient "AI literacy" for users and third-party workers
Machinery Directive 2006/42/EC	Current directive on machine product safety; includes requirements for safe design and operation
Machinery Regulation (EU) 2023/1230	Successor regulation, in force from 2027; explicitly addresses autonomous and adaptive machine behavior
– Annex I and III, Recitals 12, 32, 43, 54	Covers autonomy, self-learning behavior, and risk of self-modifying logic
DGUV Requirements (2021)	German Social Accident Insurance rules for AI safety: prohibit safety-critical decisions by learning systems
IEC 62443 / DIN EN IEC 62443-4-2	Industrial IT security standards for automation and AI in critical systems

Table 1

of system decisions, and employee training in order to minimize the risk of accidents[4][21]. In addition, the requirements of the ArbStättV are relevant in the context of digitalization and flexible forms of work. These also require a risk assessment and appropriate protective measures (Section 5 ArbSchG)[25]. Corresponding provisions of Framework Directive 89/391/EEC can also be found in other Member States, such as the Loi de Vigilance in France or the Arbetsmiljölagen in Sweden, which stipulate a general obligation to carry out risk assessments and systematic occupational health and safety measures.[1] The practical implementation of these occupational health and safety requirements when using digital and automated systems is a challenge, but remains essential for the

[1]République Française. Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre. Journal Officiel de la République Française, 2017; Kingdom of Sweden. Arbetsmiljölagen (1977:1160) – Swedish Work Environment Act. Swedish Code of Statutes, 1977.

protection of employees. With regard to the industrial robots used, employers are obliged to use only machines that comply with the applicable safety requirements. This is primarily based on product safety regulations aimed at manufacturers of robot systems, in particular the Machinery Directive, which will be replaced by the Machinery Regulation in 2027. This standardizes the requirements for designing, operating, and modifying machines (Section 3 (1), (2) of the Machinery Ordinance – 9. ProdSV; Annex I Directive 2006/42/EC).[2] At the same time (as the other side of the coin), employers have to make sure that machines – including their software components – are safe, ergonomic, and healthy when first used and during operation[26]. The risk assessment requirement also applies to software-based control systems, in particular adaptive systems whose behavior may change during operation[6]. If systems are modified in the context of occupational safety law, the employer may become the manufacturer themselves – with the obligation (now derived from the Machinery Regulation) to carry out a conformity assessment (Art. 3 No. 16, Art. 18 Machinery Regulation)[27]. The increased use of intelligent, adaptive systems – for example in robotics and automation – is giving rise to new challenges. The German Social Accident Prevention Institution (DGUV) has already formulated specific requirements for AI systems in occupational safety and health in 2021[21]: Continuously learning systems hast to be designed in such a way that they cannot make safety-critical decisions.

Technically, this requirement can be implemented by several means, such as:

- Safety envelopes: Defining strict operational boundaries within which the system's decisions are allowed, preventing any action outside safe parameters.
- Hierarchical control architectures: Separating the learning algorithm from the real-time control loop, so that only decisions passing through a safety validation layer can affect critical functions.
- Human-in-the-loop mechanisms: Ensuring that a human operator can monitor, intervene, or override decisions before they lead to safety-critical actions.
- Fail-safe fallback modes: Automatically switching to a predefined safe state or control mode if the learning system's outputs are uncertain or exceed risk thresholds.
- Formal verification and validation: Applying rigorous testing and model checking to verify that learning components cannot produce unsafe outcomes.

The control system has to ensure that the operating state always maintains an acceptable risk for humans. Safety functions have priority over sequence controls, and the system limits – in particular the limits of safe functioning – have to be recognizable to the user. The simulation of non-existent safety need to be avoided. Technically, reference should be made here to the IEC 62443 series of standards on IT security (DGUV Test GS-IFA-M24; DIN EN IEC 62443-4-2), among others. The Machinery Regulation also responds to these technological developments, but without using the term "artificial intelligence"; instead, it refers – for example in recitals 12, 32, and 43 and in Annex III, Part B, No. 1 – to machines with different degrees of autonomy or autonomous behavior. In addition, it addresses the challenges of self-developing behavior (rec. 54 et seq., Annex I Part A No. 5, Annex II No. 19, Annex III Part B No. 1) and self-developing logic (ibid.) in several provisions in order to cover safety-related risks of adaptive systems under product law. These basic principles are also incorporated into the AI Act, which will be directly applicable from 2026. Employers who integrate AI systems into work processes – for example, to control machines or assist in decision-making – are considered operators according to Art. 3 No. 4 AI Act if they use them on their own account and at their own risk[28]. The decisive factor is whether the system has a certain degree of autonomy and

[2]Comparable regulations can be found in other European countries, such as Sweden: Swedish Work Environment Authority. AFS 2008:3 – Maskiner. Stockholm, 2008. (Repealed); Swedish Work Environment Authority. AFS 2023:4 – Produkter – Maskiner. Stockholm, 2023. These regulations emphasize the implementation of systematic occupational health and safety measures — including risk assessments, user instructions, protective devices, and maintenance protocols — to ensure safe machine use and reduce workplace hazards.

is capable of adapting its behavior independently based on experience (Recital 12, p. 11 AI Act)[29]. Conventional software that operates purely on the basis of rules does not fall under the term AI system[30]. The legal obligations for employers – now as operators – arise directly from the AI Act: According to Art. 4, they need to ensure that all persons involved in development, operation, and use have sufficient AI literacy. This applies not only to their own personnel, but also to third parties, such as external service providers, temporary workers, or processors[31][32]. The requirements vary depending on the context of use – from basic training to specialized training on risk, technical application, and evaluation of AI outputs[31][33]. The aim is to ensure that AI is used competently, that risks are identified at an early stage, that malfunctions are avoided, and that employees are protected at all times, including from manipulative or non-transparent system effects. This does not relativize the classic duty of care of employers in the AI-based world of work, but rather gives it new concrete form.

4. Peculiarities when employing external company personnel

The increasing use of external employees, for example in the context of work contracts or temporary employment, leads to complex occupational health and safety challenges in the context of AI-supported industrial robotics. In a work contract, the external company remains primarily responsible for occupational health and safety, and the client is only liable for hazards arising from its working environment (Section 8 ArbSchG)[24]. However, due to the adaptive and sometimes unpredictable behavior of AI systems, the contracting company has a special obligation to take appropriate protective measures and make risks transparent, even for employees of external companies. According to Section 5 ArbSchG, a risk assessment is to be carried out; if different employers are working at the same time, Section 8 ArbSchG stipulates that coordination is required. One-off assessments are often insufficient, particularly in the case of AI systems, as risk situations can change dynamically due to system behavior. Employees of external companies are particularly at risk here, as they often lack the necessary understanding of the system or knowledge of specific operational risks. This necessitates continuously updated assessments and clearly defined responsibilities between the companies involved. In addition, Section 12 ArbSchG requires that all employees be instructed, which in a multi-employer context also includes external staff pursuant to Section 8 ArbSchG. However, the special feature of AI-based systems is that not all hazards can be predicted and communicated in an understandable manner. In addition, external employees often do not have the necessary qualifications to use the technology employed. Art. 4 of the AI Act makes it clear that external users of AI systems also require special protection. Responsibility for safe use therefore lies not only with the manufacturer, but also with the operator, who need to ensure that all parties involved have adequate AI literacy.

5. Critical Analysis: Is the existing legal framework sufficient?

With the increased use of adaptive AI systems in industrial production, the question arises as to whether current occupational safety and health legislation adequately addresses the new risks that arise from this—especially when not only a company's own employees but also employees from external companies are involved in work processes. The current understanding of risk is still based on the older Framework Directive 89/391/EEC, which assumed that all risks are identifiable and predictable. However, AI-supported systems, in particular adaptive and self-modifying industrial robots, undermine this paradigm. They exhibit context-dependent behavior that is not necessarily deterministic or consistent, and thus elude traditional forms of risk assessment. Instead of selective assessments, continuous, dynamic risk assessment would be necessary, for which there is currently no explicit legal basis. There are also still gaps in product/product safety legislation: Although the Machinery Regulation addresses systems with self-developing behavior or self-developing logic, it does not contain any conclusive requirements for ongoing conformity assessment in the event of system updates or self-modifying behavior, as is typical for adaptive systems. At the same time, traditional protection obligations, in particular pursuant to Section 12 ArbSchG, are reaching their practical limits. Providing instruction on hazards is made more difficult when risks cannot be described conclusively due to the system logic. In addition, employees of external companies are not usually integrated into internal training systems, which results in a protection gap with regard to risks that are difficult to calculate. This in turn raises questions of liability if unforeseeable system behavior leads to damage—for example, if external employees are injured by autonomous decisions made by a robot system. Employer liability according to Section 3 ArbSchG, which has so far been focused on clearly identifiable hazards, is not readily applicable to such constellations. The distinction from manufacturer liability also remains unclear, as the actual risk exposure lies in the operational context of use. In this context, Article 4 AI Act takes on central importance. The obligation it imposes to ensure sufficient AI literacy within the organization marks a qualitative transition in the structure of responsibility under occupational safety and health law. Unlike product law regulations, which primarily focus on technical safety, the AI Act explicitly requires organizational precautions for the competent handling of high-risk AI systems. This obligation applies not only to IT departments or system administrators, but also to those areas of the company where humans and AI physically interact. AI literacy thus becomes an element of operational safety organization, comparable to operating competence for conventional machines. A purely functional understanding of the system is not sufficient—rather, a fundamental understanding of the decision-making logic, adaptability, and limitations of the respective system is required in order to be able to assess and prevent risk constellations in advance. This literacy requirement cannot be limited to permanent employees. Since Article 4(1) AI Act expressly includes "other persons" who interact with the system, it can be assumed that this also covers employees of external companies. This means that operator organizations are also obliged to integrate these groups of people into the safety architecture through appropriate measures, such as training, instruction, and technical protection concepts. The current structure of labor law – in particular the ArbSchG, BetrSichV, and ArbStättV – does not adequately address this requirement, as it does not yet treat technological competencies as an independent protective component. This raises the question of whether a systematic addition to occupational safety regulations is necessary in order to normatively anchor AI literacy as an operational prerequisite for protection—for example, in the form of a specific obligation to provide training, to document AI-related instruction, or to continuously maintain competence in organizations that operate high-risk AI systems. Until this transition is complete, a structural gap will remain between safe technology and safe interaction.

6. Legal and operational requirements for the safe use of adaptive AI systems

To address occupational safety challenges associated with the use of AI-supported industrial robots, particularly when working with employees from other companies, companies can consider various practical measures. One possible approach is to supplement the classic risk assessment with a dynamic system that is reviewed and, if necessary, adapted when significant software or AI updates are made. The use of specialized tools for risk assessment of adaptive systems, for example through simulations of possible AI behaviors under different environmental conditions, can contribute to a better assessment. In addition, continuous validation of the actual system responses appears to be useful in order to continuously assess the effectiveness of protective measures. Furthermore, specific training concepts should be developed that reflect the particular characteristics of adaptive AI systems and their inherent unpredictability. Particular attention should be paid to employees from external companies, as they often have less relevant prior knowledge. Regular updating and documentation of these instructions can help to maintain the level of information among employees at an appropriate level. In addition, extended documentation requirements could be introduced to systematically record changes to the AI system – such as updates or new training data – and integrate them into the occupational safety organization. Consistent change management that ensures that every adjustment is reviewed for potential occupational safety implications appears to be an appropriate approach here. Storing system logs and error messages could also be useful for informed accident analysis. On the legislative level, it can be argued that further regulation in several areas could be helpful in better reflecting the specific risks of adaptive AI systems. For example, it could be discussed to what extent the introduction of continuous risk assessments for AI systems could be a useful addition to existing regulations in order to take account of the dynamic and changing risk situation. In addition, specific requirements for fail-safe mechanisms in AI robots, such as mandatory emergency shutdown functions in the event of unpredictable behavior, could contribute to increased safety. The promotion of standards in the field of "explainable AI" could improve the traceability of decisions made by adaptive systems and thus increase transparency for employees. In this context, it seems appropriate to develop industry-specific guidelines on "AI safety organization" that provide specific guidance comparable to existing requirements for machine instruction. The integration of the obligation to ensure sufficient AI competence within operator organizations, as formulated in Article 4 AI Act, into the occupational health and safety framework also appears to be of particular relevance. The inclusion of this competence requirement as an operational obligation within the meaning of the ArbSchG could help to structure responsibilities more clearly. An amendment to existing regulations such as the ArbStättV and the BetrSichV to specify specific requirements for AI-related training, dynamic risk assessments, and the integration of external company employees could also be considered. The structural gap between technical system safety and safe interaction suggests that supplementary requirements to ensure AI competence – such as training obligations or documentation requirements – should not be seen as innovation-inhibiting overregulation, but rather as a logical extension of existing regulatory mechanisms. Workplace regulations such as the ArbStättV and BetrSichV already regulate technical, ergonomic, and organizational safety aspects in great detail, from minimum lighting requirements and computer workstations to the maintenance of complex machines. Against this backdrop, it does not seem far-fetched to standardize specific requirements for the competent handling of highly complex, adaptive systems as part of safety-relevant operational organization. The establishment of AI competence requirements would thus not only consistently implement Article 4 AI Act at the national level, but would also fit systematically into the existing structure of occupational safety and health standards. Finally, it will be necessary to discuss whether the creation of a separate hazard category for AI-related risks within the meaning of the ArbSchG could be helpful in order to better take into account the special features of adaptive systems in occupational safety and health law. Overall, it seems sensible to carefully develop the legal provisions further, taking into account technical, organizational, and personnel aspects, in order to strengthen the protection of workers in increasingly AI-supported manufacturing processes.

In light of rapid technological developments, the importance of adaptive systems is continuing to grow — not only because of their technical potential, but also due to their increasing integration into complex, interdependent industrial environments. Unlike conventional automation systems, adaptive AI can modify its behavior based on new data, environmental changes, or altered task requirements. This ability introduces a layer of unpredictability and autonomy that challenges established occupational safety paradigms. In dynamic production environments, these systems may interact in unforeseen ways with machinery, software infrastructure, or human workers. Therefore, adaptive AI does not merely represent a variation of existing systems, but a fundamental shift in how systems behave and evolve during operation. Addressing this requires a proactive safety culture that includes scenario planning, predictive monitoring, and flexible risk control measures. The adaptive nature of such systems also makes them more susceptible to long-term drift, bias accumulation, or unintended emergent behaviors, all of which demand continuous oversight. As these systems become more prevalent in human-machine collaboration, especially across organizational boundaries, it is essential to recognize their role as a driver of systemic change — and to reflect this with appropriate technical, organizational, and legal frameworks.

7. Conclusion

The increasing integration of adaptive AI systems into industrial work processes poses new and unpredictable risks that challenge existing occupational safety regulations. Gaps in protection are particularly evident when external contractors are involved, as they are often not adequately trained in the use of these technologies. A comprehensive and dynamic risk assessment, supplemented by continuous training and a strengthening of AI skills of all those involved, can be an effective solution for minimizing these risks. The AI literacy requirement provided for in the European legal framework (Art. 4 AI Act) offers a promising approach in this regard, which should also be seen as a supplement and further development of traditional occupational safety regulations. While the product safety regulations address the issue of machine autonomy and impose obligations on manufacturers, the mandatory occupational safety framework remains at the level of the 1989 Framework Directive. Careful adaptation of existing regulations and greater consideration of organizational and personnel protection measures appear advisable in order to ensure the safe use of adaptive AI systems in the long term.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] A. Goldfarb, B. Taska, F. Teodoridis, Could machine learning be a general purpose technology? a comparison of emerging technologies using data from online job postings, Research Policy 52 (2023) 104653. doi:10.1016/j.respol.2022.104653.

[2] G. Zimmermann, § 6 d., in: C. K. K. J. Chibanguza, H. Steege (Eds.), Künstliche Intelligenz: Recht und Praxis automatisierter und autonomer Systeme, Nomos, 2022.

[3] W. Eckl-Dorna, Unglück in VW-Werk: Roboter tötet Arbeiter, https://www.manager-magazin.de/magazin/artikel/unglueck-in-vw-werk-roboter-toetet-arbeiter-a-1041739.html, 2015. Manager Magazin, 2. Juli 2015.

[4] J. Hensiek, Mensch-Roboter-Kollaboration: Gefährdungen, Schutzmaßnahmen und Rechtsrisiken, Arbeitsschutz in Recht und Praxis (ARP) (2022) 236–242.

[5] I. Wildhaber, Robotik am Arbeitsplatz: Robo-Kollegen und Robo-Bosse, Zeitschrift für Schweizerisches Recht (ZSR) 135 (2016) 315–351.

[6] K. Kohte, Arbeitsschutz in der digitalen Arbeitswelt, Neue Zeitschrift für Arbeitsrecht (NZA) (2015) 1417–1425.

[7] Y. Lu, Y. Zhou, A short review on the economics of artificial intelligence, CAMA Working Paper No. 54/2019, 2019. https://ssrn.com/abstract=3433527.

[8] M. Muro, R. Maxim, J. Whiton, Automation and artificial intelligence: How machines are affecting people and places, Brookings Institution, 2019. https://www.brookings.edu/articles/automation-and-artificial-intelligence-how-machines-affect-people-and-places/.

[9] E. Ernst, R. Merola, D. Samaan, Economics of artificial intelligence: Implications for the future of work, IZA Journal of Labor Policy 9 (2019) 1–35. doi:10.2478/izajolp-2019-0004.

[10] A. Agrawal, J. S. Gans, A. Goldfarb, Artificial intelligence: The ambiguous labor market impact of automating prediction, Journal of Economic Perspectives 33 (2019) 31–50. doi:10.1257/jep.33.2.31.

[11] M. Webb, The impact of artificial intelligence on the labor market, Working Paper, Stanford University, 2020. https://www.michaelwebb.co/webb_ai.pdf.

[12] M. Haddadin, A. Knobbe, Künstliche Intelligenz und Robotik, in: In: J. Ebers, T. Heinze, and J. Steinrötter (eds.), Nomos, 2020.

[13] R. Hauck, B. Cevc, Patentschutz für Systeme Künstlicher Intelligenz?, Zeitschrift für Geistiges Eigentum / Intellectual Property Journal (ZGE/IPJ) 11 (2019) 135–169.
[14] M. Hennemann, Datenschutzrechtliche Herausforderungen bei Künstlicher Intelligenz, Zeitschrift für Wirtschaftsrecht (ZWR) (2018) 161–164.
[15] F.-U. Pieper, Künstliche Intelligenz: Im Spannungsfeld von Recht und Technik, InTeR – Zeitschrift für Innovations- und Technikrecht (2018) 9–15.
[16] M. Pils, A. Rektorschek, § 24, in: T. K. J. Ebers, T. Heinze, J. Steinrötter (Eds.), Künstliche Intelligenz und Robotik, Nomos, 2020.
[17] M. Denga, Deliktische Haftung für künstliche Intelligenz: Warum die Verschuldenshaftung des BGB auch künftig die bessere Schadensausgleichsordnung bedeutet, Computer und Recht 34 (2018) 69–78. doi:10.9785/cr-2018-0203.
[18] S. J. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, 3rd ed., Pearson Education Limited, Malaysia, 2016.
[19] M. Gajo, Studie zur Automatisierung der Arbeitswelt, GmbH-Rundschau (GmbHR) (2019) R239–R240.
[20] J. Günther, M. Böglmüller, Künstliche Intelligenz und Roboter in der Arbeitswelt, Betriebs-Berater (BB) 72 (2017) 53–58.
[21] J. Hensiek, Künstliche Intelligenz: Digitaler Wandel im betrieblichen Arbeitsschutz, Arbeitsschutz in Recht und Praxis (ARP) (2023) 354–360.
[22] P. Huchler, Kriterien für die Mensch-Maschine-Interaktion bei KI. Ansätze für die menschengerechte Gestaltung in der Arbeitswelt, Die Plattform für Künstliche Intelligenz, 2020.
[23] B. Wiebauer, Arbeitsschutz und Digitalisierung, Neue Zeitschrift für Arbeitsrecht (NZA) (2016) 1430–1436.
[24] P. Pöhls, Unterweisungen im Betrieb – Die praxisorientierte Durchführung, Arbeitsschutz in Recht und Praxis (ARP) (2021) 11–14.
[25] R. Neighbour, § 8, in: M. Sassenberg, M. Faber (Eds.), Rechtshandbuch Industrie 4.0 / Internet of Things, C.H. Beck, 2020.
[26] S. Nebe, § 178, in: Münchener Handbuch Arbeitsrecht, Band 2: Arbeitsvertrag und betriebliche Arbeitsgestaltung, C.H. Beck, 2022.
[27] M. Kittelmann, T. Mössner, Die neue Europäische Maschinenverordnung, Arbeitsschutz in Recht und Praxis (ARP) (2023) 324–328.
[28] C. Wendehorst, Kommentar zu Art. 4 Rn. 4, in: M. Martini, C. Wendehorst (Eds.), KI-VO: Verordnung über Künstliche Intelligenz. Kommentar, C.H. Beck, München, 2024.
[29] K. J. Chibanguza, H. Steege, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, Neue Juristische Wochenschrift (NJW) (2024) 1769–1775.
[30] M. Heine, M. Köhler, Die ersten Schritte der KI-Verordnung im Arbeitsrecht, Neue Zeitschrift für Arbeitsrecht (NZA) (2025) 521–526.
[31] T. Fleck, AI Literacy als Rechtsbegriff, Künstliche Intelligenz und Recht (KIR) (2024) 99–104.
[32] T. Kaufmann, Kommentierung zu Art. 4, in: S. Schefzig, M. Kilian (Eds.), BeckOK KI-Recht, C.H. Beck, München, 2025.
[33] R. Schippel, Trainingsvorgaben: Wie kann man KI-Kompetenz nach Art. 4 KI-VO vermitteln? Strategievorschlag zur effektiven Vermittlung, Künstliche Intelligenz und Recht (KIR) (2025) 119–124.