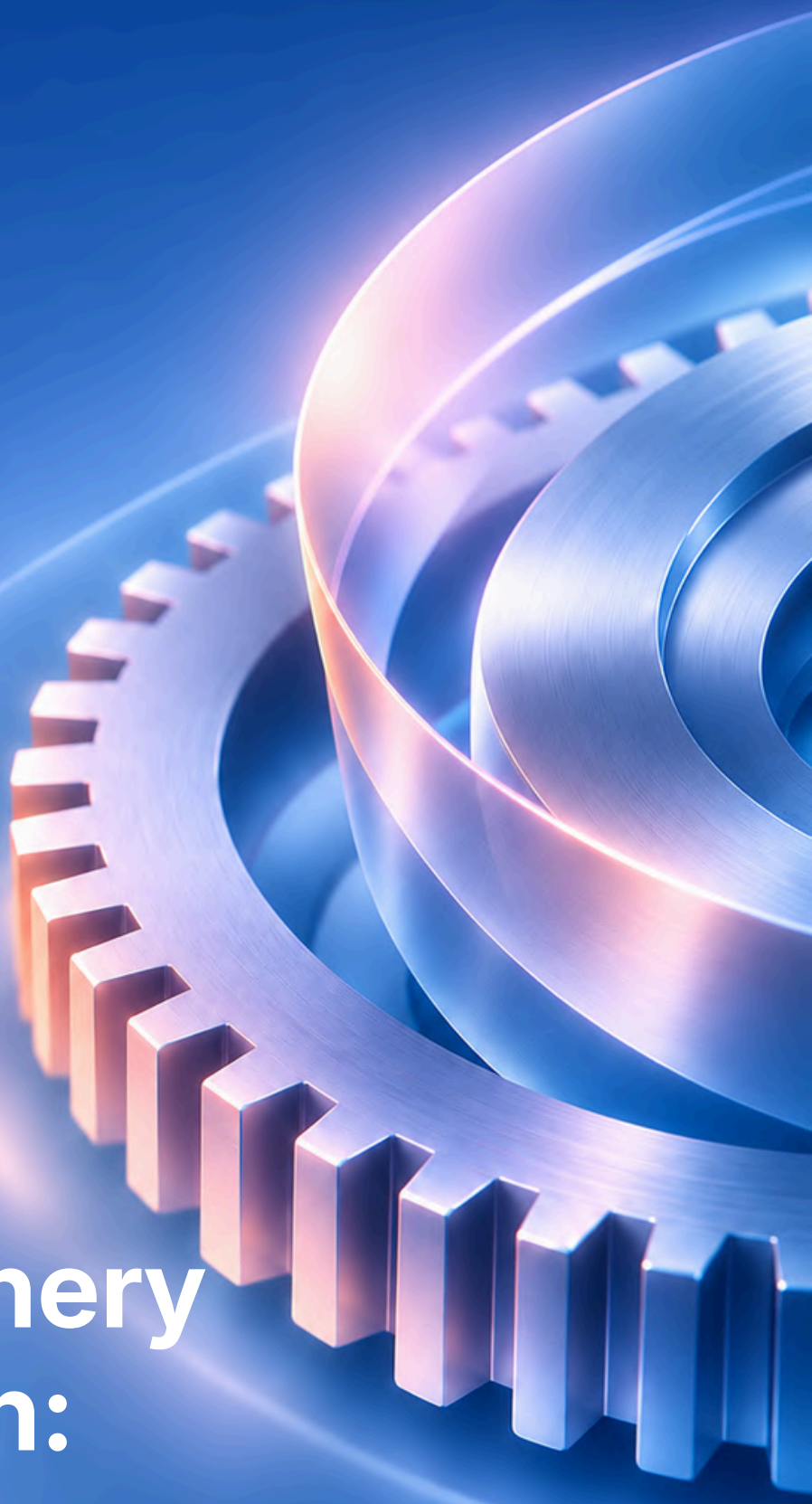
Nemko Digital



EU Machinery Regulation:

Why Digital Safety Is Now Machinery Safety

When Software Becomes a Safety Function

Machinery safety has traditionally been associated with physical hazards: moving parts, electrical faults, uncontrolled motion and the protective measures that keep people safe. Yet a machine's behaviour can also depend on software, connected control systems and artificial intelligence. A digital failure can therefore become a physical safety failure.

This is the central challenge behind the EU Machinery Regulation: manufacturers need to understand how a machine operates and how its digital functions can fail, be manipulated or behave outside their intended limits.

For manufacturers, now the practical question is how to demonstrate that the complete product remains safe when hardware, software, connectivity and AI interact.

From the Machinery Directive to a Digital Safety Framework

The Machinery Regulation (EU) 2023/1230 replaces the Machinery Directive 2006/42/EC. Its scope includes machinery, safety components, other specified related products and Partly Completed Machinery (PCM). The shift from a directive to a regulation provides a directly applicable European framework rather than one dependent on national transposition.

The underlying purpose remains the protection of health and safety. What is new is the explicit attention to digital technologies and the ways in which software and control-system integrity influence safe operation.

Digital assurance should form part of the machinery safety process and the evidence supporting the product's design, risk reduction and conformity.

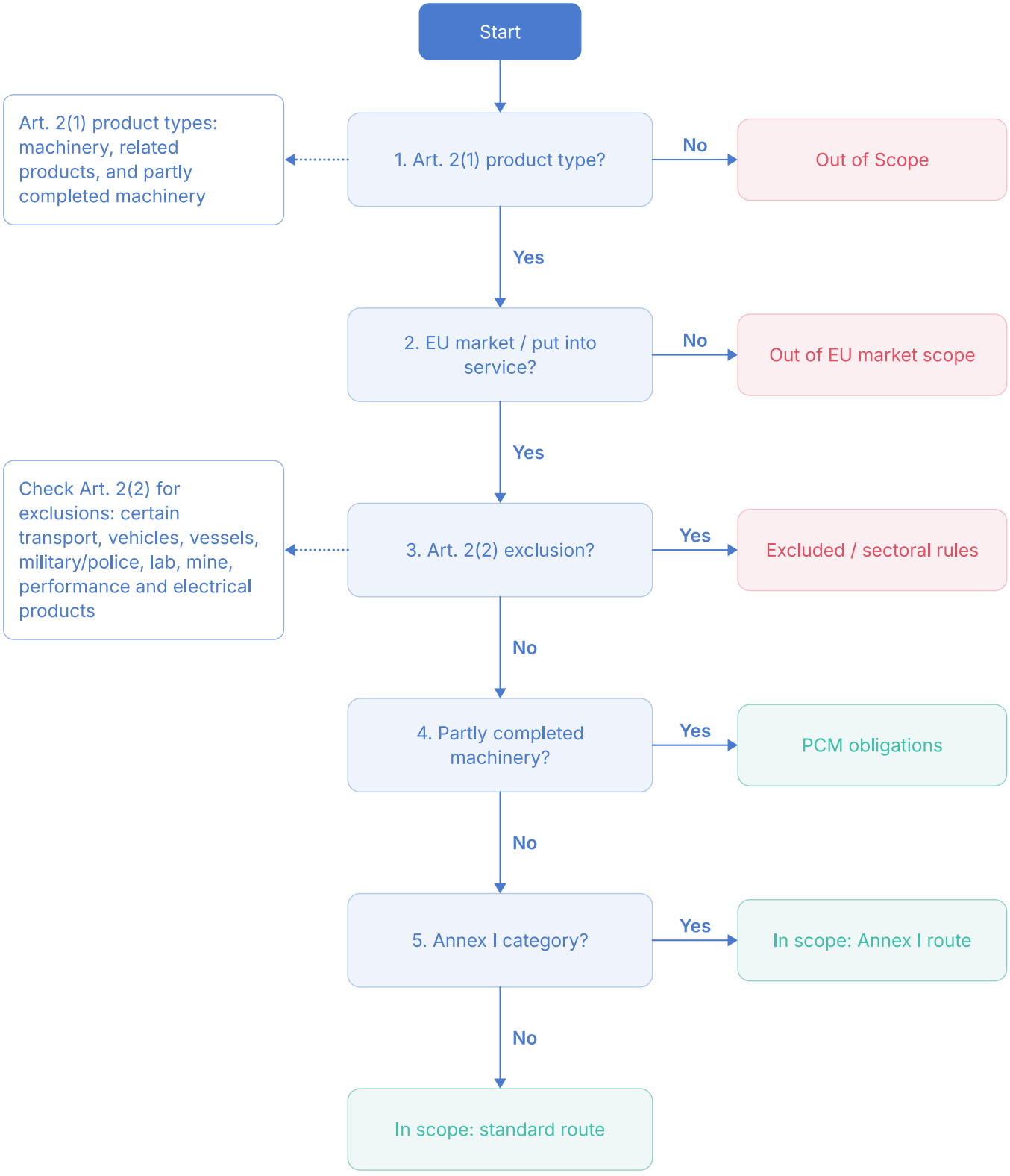


Figure 1: Machinery Regulation Applicability Decision Tree

Digital Safety Under the Machinery Regulation: Three Dimensions

Digital safety in machinery involves three connected dimensions: software and control-system integrity, cybersecurity, and AI-enabled behaviour. Each can affect how a machine behaves and the hazards it creates. The Machinery Regulation provides the safety framework; the sections below explain how cybersecurity and AI-related risks interact with the Cyber Resilience Act (CRA) and AI Act.

Before looking at the technicalities, it is important to determine the MR product category and applicable assessment route. This establishes how conformity must be demonstrated; the technical assessment then examines the digital elements affecting safe operation.

Partly completed machinery has its own documentation and incorporation obligations, distinct from the CE-marking route for a complete machine. Certain machine-learning-based safety components and embedded safety systems are listed in Annex I, Part A, for assessment involving a notified body.

For the machine's intended use and reasonably foreseeable misuse, the technical risk assessment covers three dimensions:

- **Software and control-system integrity:** Identify the software, data and control functions that influence safe operation. Examine failure modes, operator interaction and the conditions for safe intervention.
- **Cybersecurity:** Examine how unauthorised changes to software, data, interfaces or control logic could create dangerous situations. Connect protection against manipulation to the safety functions it supports.
- **AI-enabled behaviour:** Evaluate operating limits, foreseeable errors and safeguards when model outputs influence safety. Learning-based functions can also change through concept or data drift, even without malicious interference.

Across all three dimensions, technical documentation should connect identified hazards to design decisions, protective measures and verification evidence. Manufacturers need a traceable explanation of why the safeguards are appropriate for the machine and its operating conditions.

When it comes to software and control-system integrity, Annex III addresses protection against corruption and the safety and reliability of control systems. These provisions cover the integrity of safety-relevant hardware, software and data. The assessment should examine how interfaces, remote connections and changes to control logic could create dangerous situations, including failure modes, operator interaction and the conditions for safe intervention.

Cybersecurity and Safety: Different Questions, Shared Evidence

The Machinery Regulation and the Cyber Resilience Act (CRA) address related but distinct concerns. The Machinery Regulation focuses on machinery safety, including cybersecurity risks that can affect safe behaviour. The CRA addresses the cybersecurity of products with digital elements, including secure design, vulnerability handling and ongoing support.

Connected or software-driven machinery can fall within both frameworks. Where both apply, manufacturers must meet both sets of requirements and follow the applicable conformity-assessment procedures. Evidence may be reusable, but an overlap in controls is not an automatic equivalence in compliance.

A useful distinction is:

- **Machinery Regulation:** Could a software failure, compromised control system or manipulated input cause hazardous machinery behaviour?
- **CRA:** Is the product designed, maintained and supported to address its cybersecurity risks?

Consider an illustrative connected production machine with remote maintenance. An unauthorised change to a safety-relevant parameter raises a machinery safety concern. The access controls, update mechanisms and vulnerability-handling processes surrounding that interface also raise CRA questions.

Cybersecurity measures can support machinery safety. Manufacturers should show how those measures protect safety functions and build a coordinated body of evidence for both assessments.

From a Cyberattack to a Machinery Hazard: A cybersecurity finding becomes a machinery safety concern when it can be connected to hazardous behaviour. The risk chain is relatively straightforward, e.g., remote access or a network connection → manipulation of control logic or a safety function → hazardous machine behaviour → risk of injury or property damage.

For the connected production machine described above, the assessment should follow the path from the exposed interface to the affected control function and its possible physical consequences. Could unauthorised interference undermine the measures keeping the machine safe?

Recital 25 of the Machinery Regulation frames this in terms of proportionate measures against risks caused by malicious third parties where those risks affect product safety. Annex III, sections 1.1.9 and 1.2.1, bring that concern into the requirements for protection against corruption and the safety and reliability of control systems.

This gives cybersecurity evidence a clear purpose within the machinery assessment: demonstrate how identified attack paths are controlled and how the associated safety functions remain effective. General enterprise IT controls may contribute, but a standalone IT checklist is far from explaining the machine-specific safety consequences.

AI-Enabled Behaviour: Machinery Safety and the AI Act

AI-enabled machinery needs evidence that its behaviour remains within validated safety boundaries throughout its intended lifecycle. Recital 12 recognises the challenge posed by machinery that can learn, adapt, process real-time information and operate with greater autonomy in unstructured environments. The safety assessment needs to consider initial performance and the changes anticipated during use.

The following illustrative industrial-automation scenarios show where that assessment becomes concrete:

- **Machine vision misclassification:** An AI-based vision system misclassifies a person or object near a moving machine. The assessment should examine how that error affects detection and the protective response, rather than relying on overall model accuracy alone.
- **Adaptive control outside the safety envelope:** An adaptive controller changes machine behaviour beyond the conditions validated as safe. The engineering question is how permissible adaptations are bounded and how unsafe changes are prevented or detected.
- **Predictive logic influencing motion:** AI-generated decisions affect speed, force, direction or stopping behaviour. Their safety significance depends on the consequences of an incorrect decision and the safeguards that constrain the resulting action.
- **Model updates or drift after deployment:** An updated model, or a change in its performance as operating conditions evolve, alters safety-related behaviour. Evidence from the original validation may no longer be sufficient to explain performance under the changed conditions.

These scenarios point to a lifecycle assessment rather than a one-time model test. The risk assessment should account for future software updates or developments foreseen when the machine is placed on the market or put into service, as well as risks arising from an intended evolution of behaviour and varying levels of autonomy.

For manufacturers, the practical task is to connect operating limits, foreseeable changes and validation evidence. A defensible safety argument should explain what behaviour has been validated, which changes remain within that boundary and when a change calls for renewed assessment. Any adaptation must remain compatible with safe operation.

The AI Act Connection (The Sectoral Route): The relationship between the Machinery Regulation and the AI Act requires careful qualification. The July 2026 Digital Omnibus on AI moved machinery to Section B of Annex I to the AI Act, shifting the product-safety approach towards sectoral legislation.

Under the amended Article 2(2), the AI Act has limited direct application to high-risk AI systems related to products covered by Section B. This is not the same as saying that AI-enabled machinery is unregulated or that manufacturers can disregard AI-related safety risks. The Machinery Regulation remains the central product-safety framework.

The UK Government's explanatory memorandum on the amendment describes the power to introduce AI-related essential health and safety requirements into the Machinery Regulation, with the relevant additions to apply by 2 August 2028. Manufacturers should distinguish the legal framework already adopted from the detailed requirements to be introduced through delegated acts.

For the machinery-related high-risk systems covered by this sectoral route, a separate AI Act conformity-assessment procedure is not the applicable channel. That conclusion should not be extended automatically to every AI system used in a factory or offered alongside a machine: the function, product scope and classification still matter.

The AI Act Articles 8–15, 17, 19, 72 and 73 offer a useful preparation lens: risk management, data governance, documentation, logging, transparency, oversight, robustness, quality management, monitoring and incident reporting.

The table below connects some of these AI assurance themes to the machinery safety questions illustrated above. Data quality, logging, oversight and robustness evidence can help explain how AI-related hazards are controlled. The table is a preparation aid; whether an AI Act obligation applies directly depends on the system's scope and classification.

AI Act reference	Assurance theme	Indicative preparation for AI-enabled machinery
Art. 9	**Risk management**	Identify AI-specific hazards, foreseeable misuse and failure modes; connect them to lifecycle risk controls.
Art. 10	**Data and data governance**	Assess whether training, validation and test data cover the operating conditions, with documented quality and governance.
Art. 11	**Technical documentation**	Document the AI function, intended purpose, architecture, limitations, testing and safety controls.
Art. 12	**Record-keeping / logging**	Plan logging and traceability that support investigation of safety-relevant operation and events.
Art. 13	**Transparency and information**	Explain capabilities, limitations and correct use so operators can understand the AI function in context.
Art. 14	**Human oversight**	Define appropriate supervision, intervention and override mechanisms for safe operation.
Art. 15	**Accuracy, robustness and cybersecurity**	Validate performance and resilience against foreseeable errors, failures, manipulation and cyber threats.

ISA/IEC 62443 and the Emerging EN 40000 Family: Complementary Approaches

Manufacturers also need to translate legal requirements into development practices and technical evidence. Two standards families support this work: ISA/IEC 62443 and the emerging EN 40000 family.

The ISA/IEC 62443 series addresses cybersecurity across industrial automation and control systems, with responsibilities spanning product suppliers, integrators, service providers and asset owners. Within that family, IEC 62443-4-1 addresses secure product development lifecycle processes, while IEC 62443-4-2 addresses technical security requirements for industrial control-system components.

The EN 40000 family is being developed around CRA-oriented product cybersecurity. Part 1-2 addresses cybersecurity principles, product risk management and lifecycle activities. Its focus differs from the industrial-system perspective of ISA/IEC 62443, even where the two approaches support similar engineering practices.

They should therefore be treated as complementary rather than competing: a manufacturer can use industrial cybersecurity processes and controls as evidence within a broader CRA compliance approach.

An emerging draft is not a final harmonised standard, and applying a standard does not automatically demonstrate compliance with every obligation under either the CRA or the Machinery Regulation.

Dimension	ISA/IEC 62443	EN 40000 family (emerging)
Purpose	Cybersecurity framework for industrial automation and control systems (IACS)	CRA-oriented product cybersecurity framework under development
Geographic orientation	International	European
Primary scope	Industrial automation/control products, systems, integrators, service providers and asset owners	Horizontal product cybersecurity approach, supplemented by applicable product-category standards
Regulatory origin	Industry cybersecurity standardization	European standardisation work supporting CRA implementation
Core perspective	IACS security across product suppliers, integrators, service providers and asset owners	Product risk management and lifecycle evidence supporting manufacturer compliance

Supporting Guidance for Cyber-Safety and AI

prEN 50742, Safety of machinery — Protection against corruption, addresses the link between unauthorised interference and machinery safety, particularly the requirements in Annex III, sections 1.1.9 and 1.2.1. It complements the broader standards discussion by focusing on the integrity of machinery control and safety functions. Its applicable edition, publication status and any Official Journal citation should be verified before it is used to support a formal conformity claim.

For AI, ISO/IEC TR 5469:2024, Artificial intelligence — Functional safety and AI systems, provides technical-report guidance on risk factors, methods and processes where AI is used within safety-related functions, where non-AI safety functions protect AI-controlled equipment, or where AI supports the design of safety-related functions. It offers a useful lens for structuring the engineering discussion, not an automatic route to Machinery Regulation conformity.

The common thread is evidence tied to the actual safety function: what can fail or be manipulated, how the resulting hazard is controlled, and why those controls remain appropriate as the product changes.

The Timeline: Different Obligations, Different Dates

The Machinery Regulation applies generally from **20 January 2027**. The CRA's main obligations apply from **11 December 2027**, while its reporting obligations have applied since 11 September 2026.

The AI-related sectoral additions described above follow a further timetable, with application by **2 August 2028**. Manufacturers should keep that process distinct from the Machinery Regulation's existing digital safety provisions and the CRA obligations already in application. In short: for products with AI components covered by this route, 2028 is an additional AI-related milestone and not a postponement of the existing Machinery Regulation or CRA duties.

For product teams, the implication is straightforward: preparation should be organised around the product configuration, the applicable legislation and the date of market placement.

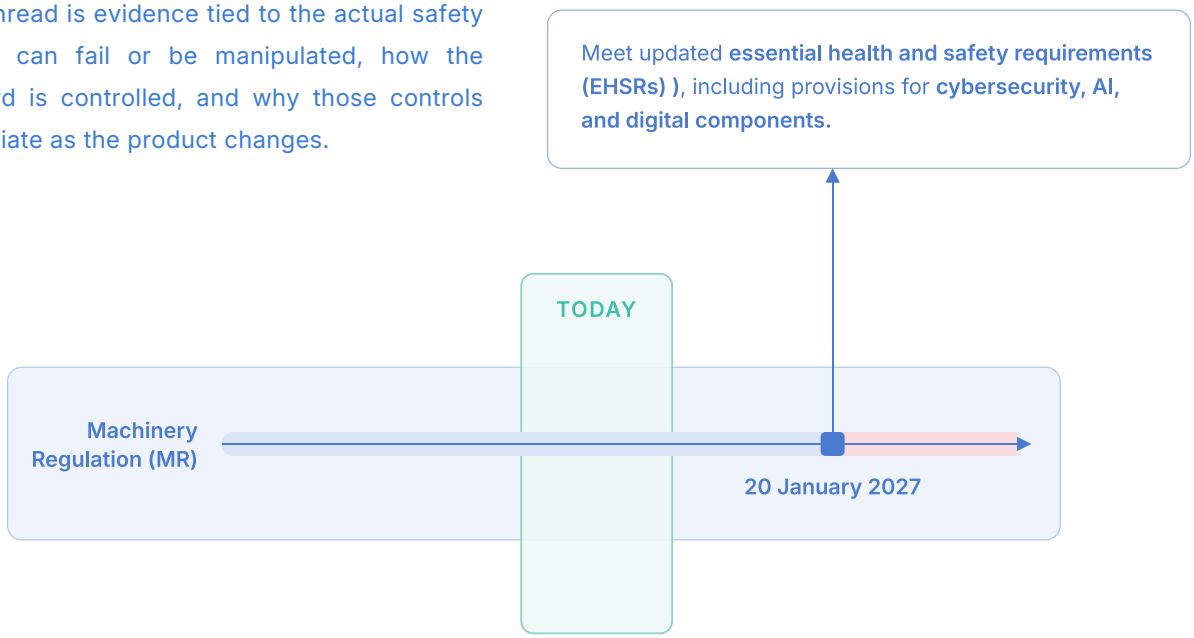


Figure 2: Machinery Regulation Timeline

A New Operating Model for Machinery Assurance

The most important organisational change is the need to bring machinery safety, software engineering, cybersecurity and AI assurance into the same product conversation.

A practical preparation programme should include:

- **Map the product:** Identify machinery functions, digital interfaces, AI components and the suppliers responsible for them.
- **Connect security to safety:** Link credible digital failures and manipulation scenarios to the hazards they could create.
- **Build traceable evidence:** Align risk assessments, design decisions, test results and technical documentation.
- **Clarify lifecycle responsibilities:** Agree who manages updates, vulnerabilities, safety-relevant changes and incidents.
- **Review the regulatory route:** Confirm product scope, conformity-assessment requirements and the status of applicable standards.
- **Plan for change:** Revisit assumptions when software, AI behaviour, connectivity or operating conditions change.

These are preparation priorities rather than a substitute for a product-specific legal and technical assessment. Their value lies in making responsibilities and evidence visible before a conformity assessment exposes the gaps.

Ultimately, digital safety is machinery safety whenever software, connectivity or AI can influence how a machine behaves. Nemko Digital support manufacturers when it comes to identifying requirements and implementing controls, ensuring efficient consideration of all three: MR, CRA and AI Act. Join us live in our next webinar EU Machinery Regulation Compliance Webinar | Nemko Digital or watch it offline.

About the author



Gustavo Sánchez, PhD

Expert Consultant AI Trust, Nemko Digital.

Gustavo brings strong expertise at the intersection of AI security, trustworthy AI, and assurance for high-stakes systems. With a research-driven mindset and hands-on experience tackling real-world challenges — from adversarial ML to critical infrastructure contexts — Gustavo helps customers build AI systems that are not only innovative, but also secure, reliable, and demonstrably trustworthy.

Nemko Digital