cecimo
European Association of Manufacturing Technologies

THE CRA COMPLEXITIES FOR THE MACHINE TOOL INDUSTRY

CECIMO POSITION PAPER

October 2025

www.cecimo.eu

The machine tool industry is the pillar of Europe's manufacturing capacity as they are critical in the supply chains of various downstream industries ranging from automotive and aerospace to defence, precision engineering, and optical equipment etc. In 2024, the European machine tool industry generated over €25.5 billion in production, representing around 1,500 industrial enterprises and employing more than 150,000 people directly. Yet the industry's significance goes well beyond these jobs and turnover. The European machine tool industry is a constant source of innovation, positioning the sector among the most advanced in Europe.

Modern machine tools are highly sophisticated and increasingly digitalised. A single machine tool may incorporate numerous components, often sourced from several specialised suppliers. Under the Cyber Resilience Act (CRA), each of these components must meet cybersecurity requirements before the final product declared compliant with the regulation and placed on the market. This dependency on intricate, multilayered supply chains highlights both the industry's systemic relevance and the considerable difficulty of rapid compliance, particularly for small and medium-sized enterprises.

CECIMO, representing the European manufacturing technology industry, supports the CRA as a necessary regulatory step to raise the level of cybersecurity for all products with digital elements and create a level playing field especially for SMEs. As industrial systems become ever more connected, the CRA is rightly designed to protect supply chains, production facilities, and end-users from growing cyber risks. Stronger cybersecurity is a matter of digital safety and an economic security for Europe. **The principles of security by design, alongside clear liability and warranty obligations for software producers, address long-standing gaps that the CRA appropriately seeks to resolve**.

Nevertheless, CECIMO fears that the current implementation timeline of the CRA risks creating disproportionate burdens for machinery producers and their suppliers. The short timeframe foreseen to establish compliance does not reflect the complexity of industrial supply chains and may prevent companies from adapting all components and systems in time. Without a phased approach and clear, practical guidance, manufacturers may be forced to pause product development, postpone investment, and delay delivery, ultimately weakening Europe's industrial competitiveness. In the longer term, such pressures could create unnecessary uncertainty for businesses and employment loss.

1.MACHINE TOOLS MATTER

Machine tools occupy a unique position in Europe's industrial ecosystem. They are not neither consumer products nor standalone devices but highly develop manufacturing equipment, enabling the production of almost every other advanced good such as cars, aircraft, medical equipment, renewable energy technologies, and more. These machines are designed to cut, shape and refine materials such as steel, aluminium and non-ferrous materials with high precision and efficiency.

Over the past decades, digitalisation has transformed the industry. Computer numerical control (CNC), software integration and digital workflows have made machine tools smarter, more connected, and more productive. Today, machine tools are highly digitalised production systems, embedded in global supply chains and integrated with industrial software. This underscores the importance of cybersecurity, but also exposes the challenges faced by the sector when new regulations apply universally to "all products with digital elements", without considering the sector's inherent complexity and interdependencies.

2.CONCERNS AND RECOMMENDATIONS

Under the current provisions of the CRA, all products with digital elements placed on the EU market must comply by December 12, 2027. This deadline applies immediately, without any transition period or "grandfathering" for existing products. While the timeline was intended to give industry time to adapt, it remains insufficient for highly complex sectors such as machine tools, where long development cycles and multi-tiered supply chains make implementation particularly challenging.

2.1 Complex supply chains and timing constraints

Machine tool builders are system integrators operating within complex, multi-level supply chains. They do not produce every part themselves but rely on specialised suppliers for critical components, assemblies and subsystems such as controllers, drives, industrial robots, cooling devices, or sensors. Many of these components qualify as "products with digital elements" under the CRA, meaning each must achieve individual compliance before the final machine tool can be declared compliant.

This interdependence creates a major timing challenge. If component manufacturers use most of the transition period to redesign and certify their products, machine tool builders will have very limited time left to adapt and validate their own machines. Unlike mass-market electronics, machine tools are typically custom-built. This means that design, or customer-specific adaptations begin only after an order is placed. Procurement of compliant components, assemblies and systems must happen well before a machine is assembled and delivered. Integrating compliant components and validating the final machines can take more than 12 months and, in some cases, up to 18 or even 24 months.

To realistically meet the 2027 deadline, compliant components would need to be available on the market by 2026 at the latest. Without this sequencing, manufacturers risk facing a compliance bottleneck that could leave them unable to deliver CRA-compliant machines within the prescribed timeframe.

Policy Recommendations

- **Distinguish between component manufacturers and system integrators.** It is essential to recognise that the compliance timeline for integrators depends on the readiness of their suppliers. Component manufacturers must therefore achieve compliance first, allowing sufficient time for machine tool builders to integrate and test compliant parts within complete systems.

- **Introduce a phased transition period.** Given the sector's dependence on suppliers and its long development cycles, CECIMO recommends maintaining the 2027 deadline for component manufacturers while extending the transition period for system integrators (machine tool builders) until the end of 2029. This two-year extension would give companies the time needed to embed and validate compliant components in complex assemblies. Such an approach would also account for the considerable workload expected of accredited certification bodies and the current shortage of qualified experts. Without a sequenced and realistic transition, the industry faces the risk of being required to comply before it is technically feasible to do so.

2.2 Interplay between CRA and Machinery Regulation

Both the Machinery Regulation (MR) and the Cyber Resilience Act introduce cybersecurity provisions for machinery. However, the CRA will take effect less than a year after the MR, creating overlapping and potentially conflicting compliance obligations. Manufacturers would first have to meet the MR cybersecurity provisions, notably EHSR 1.1.9 (Protection against corruption) and EHSR 1.2.1 (Safety and reliability of control systems) and then adapt again for the CRA, which is a duplicative and burdensome process.

Furthermore, the relevant harmonised standards underpinning these requirements are unlikely to be published before late 2026, leaving insufficient time for manufacturers to adapt their designs and processes before the MR's application date in January 2027. As previously noted, misaligned implementation timelines risk forcing companies to re-assess products twice within a short period, increasing costs and complexity. If manufacturers first implement MR-cyber requirements and then have to redo everything for the CRA, this would mean double work, more audits, more revalidation and additional documentation.

Policy Recommendations

- **Postponing the implementation of the cybersecurity-related provisions in the Machinery Regulation until the CRA requirements and the related harmonised standards are finalised and published.** Ideally, this should be aligned with **December 2027**. Such alignment would ensure coherence, prevent duplication, and give industry sufficient time and clarity to implement effective cybersecurity measures.

2.3 Delayed harmonised standards

For companies to comply with the CRA in a consistent and effective manner, harmonised standards are essential. They provide clear frameworks that simplify the declaration of conformity and ensure a level playing field across the Single Market. As many of these standards are still under development, businesses face uncertainty regarding their future compliance pathways.

The process of developing harmonised standards is inherently complex process, requiring close cooperation among public authorities, standardisation bodies, and industry. Currently, much of this work is driven by IT experts whose perspectives may not always reflect the realities of industrial production. Meanwhile, traditional manufacturing sectors, such as the machine tool industry, often struggle to allocate the specialised personnel or resources needed for standardisation activities. Even when the expertise exists, it is often focused on operational priorities rather than standard-setting efforts.

Larger companies can often participate in these processes, but smaller firm, especially SMEs, face additional constraints. As a result, some industrial perspectives risk being under-represented, despite the sector's commitment to high safety and security standards.

Policy Recommendations

- **Allow sufficient time and support for implementation.** Once harmonised standards are published, companies need time to assess their implications, train staff, and adapt governance systems accordingly.

- **Provide targeted assistance.** Explanatory materials, sector-specific training, and outreach initiatives would help ensure consistent and efficient implementation across the industry.

2.4 Delayed implementation guidelines

Many companies, especially SMEs, remain uncertain about how to begin applying the CRA in practice. They often lack in-house legal or cybersecurity expertise to interpret complex regulatory requirements. Facing multiple and sometimes overlapping digital regulations, businesses may struggle to understand how these frameworks interact and what concrete actions are required. Without clear, practical guidance, it is difficult to determine whether products fall within the CRA's scope, what actions are necessary for compliance, or how to integrate requirements into daily operations. This lack of clarity risks creating bottlenecks, slowing down compliance efforts, and increasing administrative burdens, especially for resource-limited organisations.

Policy Recommendations

- **Accelerate the development of practical implementation guidelines.** Guidelines should be developed in close coordination with industry stakeholders covering both technical and operational dimension. A comprehensive guide, similar to the Guide for the application of the Machinery Directive, would support consistent interpretation and application across industrial sectors.

2.5 Interplay between CRA and NIS2 Directive

Parallel reporting requirements in CRA and NIS2 create unnecessary administrative burdens, legal uncertainty, and delays in incident response. When a cybersecurity incident affects both connected products and network systems, companies are often required to notify multiple authorities using different platforms, templates, and procedures — frequently submitting the same information several times.

Current inconsistencies between the two legislations further complicate implementation. The terms “significant incidents” (NIS2) and “serious incidents” (CRA) differ despite addressing comparable risks. Reporting thresholds, timelines, and competent authorities also vary. Moreover, diverging national implementations of NIS2, such as the inclusion of additional sectors, differing deadlines, or non-aligned audit systems, create an uneven regulatory landscape across the EU.

A fragmented reporting system undermines Europe's overall cybersecurity resilience and diverts resources from incident management to bureaucracy. The proposed one-stop-shop reporting platform would enable manufacturers to submit a single report automatically forwarded to the relevant national authorities, with ENISA acting solely as a technical intermediary. This system should also facilitate secure follow-up communication between competent authorities, reducing redundant requests and ensuring consistency.

Policy Recommendations

- **Harmonise incident reporting obligations through a "one-stop-shop" reporting platform** under Article 16 of the CRA, with a single reporting template and authority, creating a single EU-level mechanism.

- **Align the NIS2 implementation across Member States** ensuring mutual recognition of audit systems and consistency in reporting deadlines. Alignment between the CRA and NIS2 frameworks would strengthen governance, reduce administrative burden, and allow manufacturers to focus on prevention, mitigation, and recovery.

3.BROADER IMPLICATIONS FOR INDUSTRY

Tight deadlines, complex supply chains, incomplete standards, and limited guidance are already placing significant financial and operational pressure on manufacturers. The additional costs of compliance, particularly during the early stages of product redesign and conformity assessment, represent a heavy burden for SMEs that often lack the financial and human resources to absorb such demands. For some, these pressures could reduce competitiveness, slow innovation, or even force market withdrawal, especially when competing with larger global players that benefit from greater economies of scale.

Simultaneously, the ongoing shortage of skilled cybersecurity specialists across Europe further hinders companies' capacity to adapt. Many companies struggle to recruit specialists capable of managing digital security within industrial settings. When combined with economic uncertainty, trade barriers, and global competition, this skills gap further weakens Europe's ability to remain an attractive hub for industrial investment and technological development.

CECIMO believes that the current CRA implementation timeline is neither realistic nor proportionate for complex industrial equipment. The mismatch between three factors — (1) the time needed to comply with harmonised standards once available, (2) the lead time suppliers require to deliver compliant components, and (3) the time integrators need to assemble finished machines (integrate CRA-compliant components into the end product, the machine tool), creates an unsustainable situation. If the current implementation deadline remains unchanged, manufacturers will face both technical and economic risks, with SMEs disproportionately affected. This could undermine competitiveness and erode Europe's industrial base.

That being said, for highly technical equipment such as machine tools, the CRA timeline must therefore be reconsidered. CECIMO calls for a longer transition period for system integrators, sufficient time to for adoption of harmonised standards once published, and accelerated development of practical implementation guidelines.

FOR MORE INFORMATION, PLEASE CONTACT:

Olha HUNCHAK

Digital and Technical Policy Manager

olha.hunchak@cecimo.eu

About CECIMO:

CECIMO is the European Association of Manufacturing Technologies. With a primary focus on machine tools and additive manufacturing technologies, we bring together 15 national associations representing approximately 1500 industrial enterprises in Europe (EU + UK+ EFTA + Türkiye), over 80% of which are SMEs. CECIMO covers 97% of the total machine tool production in Europe and about 1/3worldwide. It accounts for approximately 150,000 employees and a turnover of around 25.8 billion euros in 2024.

CECIMO Members

Austria: Metaltechnology Austria
Die MetalltechnischeIndustrie

Germany: VDW
Verein Deutscher Werkzeugmaschinenfabriken e.V.

Sweden: MTAS
Machine and Tool Association of Sweden

Belgium: AGORIA
The Federation of Technology Industry

Italy: UCIMU
Associazione dei costruttori Italiani di macchine utensili robot e automazione

Switzerland: SWISSMEM
Die Schweizer Maschinen-, Elektro- und Metall-Industrie

Czech Republic: SST
Svazu Strojírenské Technologie

Netherlands: FPT-VIMAG
FederatieProductieTechnologie / Sectie VIMAG

Türkiye: MIB Makina Imalatcilari Birligi

Denmark: The Manufacturing Industry
a part of the Confederation of Danish Industry

Portugal: AIMMAP
Associacão dos Industriais Metalúrgicos, Metalomecânicos e Afins de Portugal

United Kingdom: MTA
The Manufacturing Technologies Association

Finland: Technology Industries of Finland

Spain: AFM Cluster
Asociación española de fabricantes de máquinas-herramienta, accesorios, componentes y herramientas

France: Evolis
Organisation professionnelle des biens d'équipement