AKENATECH

NEW EU MACHINE REGULATION 2023/1230: INTEGRATING CYBERSECURITY INTO INDUSTRIAL COMPLIANCE

The European regulatory landscape is undergoing a major transformation with the adoption of the EU Machine Regulation 2023/1230, which marks a historic turning point in the design and marketing of industrial equipment. For the first time, cybersecurity is becoming an explicit requirement on par with traditional physical security. This evolution responds to the growing threats to connected production systems and requires manufacturers to rethink their development processes. Understanding this new regulatory framework is now essential for any industrial organization wishing to maintain its access to the European market.

What is RM?

A new legal framework for machines

The Machinery Regulation (MR) EU 2023/1230, published in the Official Journal of the European Union on 29 June 2023, replaces the historic Directive 2006/42/EC, which until then governed the safety of machinery in Europe. Unlike a directive, which requires transposition into the national law of each Member State, a European regulation applies directly and uniformly in all 27 countries of the European Union as soon as it enters into force.

This change in legal format is not insignificant: it guarantees a total harmonisation of requirements throughout the European territory, thus eliminating national differences of interpretation that could create complexities for manufacturers exporting to several member countries.

The historical integration of cybersecurity

The real revolution of the Machine Regulation 2023/1230 lies in the explicit integration of cybersecurity requirements. While the old directive focused exclusively on physical and mechanical risks, the new text recognises that modern machines, increasingly connected and driven by digital systems, are exposed to cyber threats that can compromise their physical security.

This evolution reflects the contemporary industrial reality: according to the ANSSI's 2024 annual report, attacks targeting industrial systems have increased significantly in recent years, and connected equipment is a privileged entry point for cybercriminals.

Key dates of application

The Machinery Regulations came into force on 19 July 2023, but their effective date is set for **20 January 2027**. This transition period of more than three years allows manufacturers to adapt their design processes, document systems and production lines to the new requirements. After this date, any machine placed on the European market must comply with the provisions of the new regulation.

What are the objectives of the RM?

Harmonising machine safety in the EU

The primary objective of the Machinery Regulation is to guarantee a high and uniform level of safety for all equipment marketed on European territory. By adopting the format of a regulation rather than a directive, the European Union eliminates variations in interpretation between Member States and simplifies the process for manufacturers who no longer have to navigate between different national transpositions.

This harmonisation also facilitates the free movement of machinery within the European single market, thus reducing trade barriers and compliance costs for manufacturers.

Adapting the regulatory framework to digital technologies

The rapid development of Industry 4.0, characterized by the increasing interconnection of equipment, the use of artificial intelligence and the integration of IoT (Internet of Things) components, has made the 2006 regulatory framework obsolete. The RM responds to this transformation by introducing specific requirements for machines integrating digital elements, in particular in terms of:

- Protection against unauthorized access
- Securing communication interfaces
- Secure software and firmware updates
- Resilience to cyberattacks

Protect users from cyber-physical risks

The major innovation of the Machine Regulation lies in the recognition of **cyber-physical risks** : digital vulnerabilities can now compromise the physical security of operators. A machine compromised by a cyberattack can cause serious industrial accidents, injuries, or deaths.

By integrating cybersecurity into the Essential Security and Health Requirements (EESS), the RM requires manufacturers to consider digital threats from the design phase, using a "security by design" approach.

What changes with the RM?

Explicit cybersecurity requirements

Annex III of the Machinery Regulations introduces essential safety and health requirements specifically dedicated to the cybersecurity of machinery. These new provisions require, in particular:

- **Cyber risk assessment** : Manufacturers need to identify digital threats that could affect the security of their machines
- **Protecting against unauthorized access** : Implementing robust authentication and access control mechanisms
- **Securing communications** : Encrypting data exchanged and protecting network interfaces
- **Event traceability** : Access and change logging to detect security incidents

Enriched technical documentation

The technical file accompanying the declaration of conformity must now include a detailed analysis of the cybersecurity risks and the protective measures implemented. This documentation should demonstrate how potential vulnerabilities have been identified and mitigated throughout the product lifecycle.

The instruction notice provided to users should also contain information on good cybersecurity practices: secure configuration, update procedures, contacts in the event of a security incident.

A broadening of the scope of application

The Machinery Regulation extends its scope to new product categories that were not explicitly covered by the old directive, including:

- Artificial intelligence systems embedded in machines
- Some software equipment that impacts security
- Partially completed machines, with increased requirements

A full lifecycle approach

In contrast to the previous design-phase directive, the RM takes a view of the entire life cycle of the machine. Manufacturers should plan for post-market cybersecurity maintenance, including:

- Secure update procedures
- A process for managing discovered vulnerabilities
- Transparent communication with users about security incidents

Who is concerned by the RM?

Machine manufacturers

The first to be affected by the Machinery Regulation are of course manufacturers, whether they are established in the European Union or in a third country. Any manufacturer designing and producing machines for the European market must ensure that their products comply with the requirements of the regulation before they are first placed on the market.

This obligation applies regardless of the place of manufacture: a Chinese, American or Japanese producer exporting to the EU is subject to the same requirements as a European manufacturer.

Importers and distributors

Importers who introduce non-EU machines onto the European market have an important responsibility: they have to check that the manufacturer has complied with its obligations and that the machine bears the appropriate CE marking. In the event of non-compliance, the importer may be held liable.

Distributors, although less directly involved, must ensure that the machines they market bear the required CE marking and are accompanied by the appropriate documentation in the language of the country of marketing.

Integrators and installers

Companies that assemble multiple machines or components to create a complete industrial plant may find themselves in the position of manufacturer if they create a new assembly that has different safety features from individual components.

Industrial sectors particularly affected

Some sectors are particularly affected by the new cybersecurity requirements of the MD:

- **Manufacturing** : automated production lines, collaborative robots
- **Food & Beverage** : Packaging Machines, Connected Traceability Systems
- **Logistics** : automated conveyor systems, AGVs (automated guided vehicles)
- **Construction** : Connected construction machinery, intelligent lifting equipment
- **Energy** : machinery and production equipment incorporating control systems

What are the main obligations for industrial organizations?

Carry out a cyber-physical risk analysis

The first obligation imposed by the MD is to conduct a **comprehensive risk assessment** that integrates both physical and digital dimensions. This analysis must identify:

- Critical machine assets (PLCs, sensors, network interfaces)
- Potential threats (unauthorized access, malware, denial of service)
- Exploitable vulnerabilities (weak authentication, insecure protocols)
- The potential impact on the safety of people

This approach is in line with normative approaches such as IEC 62443 for the cybersecurity of industrial systems.

Design according to the principle of "security by design"

The Machine Regulation requires that cybersecurity be integrated **from the design phase**, and not as a layer added a posteriori. This involves:

- Segmented network architecture limiting the attack surface
- Hardening operating systems and removing unnecessary services
- Implementation of strong authentication mechanisms
- Encryption of sensitive communications and data
- Secure update mechanisms (cryptographic signature of firmware)

Compile a technical compliance file

Each machine must be accompanied by a **technical file** demonstrating its compliance with the essential requirements of the regulation. This file must contain:

- Complete risk analysis (mechanical and cyber)
- Technical specifications and design plans
- The harmonised standards applied (e.g. the future European standard EN ISO 19087 on the cybersecurity of machinery)
- The results of tests and compliance tests
- The signed EU declaration of conformity

Ensure transparent communication

Manufacturers must provide users with **clear and complete documentation** including:

- Installation and Secure Setup Instructions
- Cybersecurity best practices
- Software and firmware update procedures
- Contact information for reporting a vulnerability
- Information on the duration of planned cybersecurity support

Implement a vulnerability management process

The life cycle does not end with the time it is brought to market. Manufacturers should establish a **process for monitoring and responding** to post-market vulnerabilities, including:

- Monitoring of vulnerabilities affecting the components used
- Reporting mechanism for security researchers
- Process for assessing and remediating identified vulnerabilities
- Rapid communication to customers in the event of a critical vulnerability

What are the penalties provided for by the RM?

A harmonised sanctions framework

The Machinery Regulation provides for a **system of penalties** that Member States must implement in their national legislation. Although the precise modalities may vary from country to country, the regulation requires that sanctions be "effective, proportionate and dissuasive".

Administrative and financial penalties

National market surveillance authorities can impose **significant fines** on manufacturers, importers or distributors who fail to comply with their obligations. Although the text does not specify precise amounts (unlike the GDPR or NIS 2), member states are required to establish penalties that are large enough to deter infringements.

Penalties can be graduated according to the seriousness of the breach:

- Documentary non-compliance (lack of technical file)
- Lack of CE marking or fraudulent marking
- Failure to comply with essential security requirements
- Deliberate endangerment of users

Corrective actions and recall

In addition to fines, authorities can order binding **corrective measures**:

- Suspension of marketing until compliance is achieved
- Recall and withdrawal of machines already on the market
- Publication of the infringements observed (major reputational effect)
- Temporary or permanent ban on marketing in the EU

Civil and criminal liability

In the event of an accident caused by a non-compliant machine, the manufacturer is liable to **civil action** for damages, as well as criminal prosecution if gross negligence or deliberate endangerment is established.

European case law on liability for defective products can lead to very heavy sentences, particularly when human lives are at stake.

How to prepare for the application of the RM?

Carry out a maturity diagnosis

The first step is to **assess the gap** between your current practices and the requirements of the Machine Regulation. This diagnosis must cover:

- Current design and risk analysis processes
- Level of consideration of cybersecurity in product development
- Existing technical documentation and its gaps
- Available in-house OT/IoT cybersecurity skills
- Lifecycle management and maintenance processes

Training teams on new requirements

RM compliance requires **specific skills** at the intersection of traditional machine security and industrial cybersecurity. It is essential to train:

- Design engineers with the principles of "security by design"
- Quality managers with new documentary requirements
- Vulnerability management process support teams
- Management to strategic issues and legal risks

Adopt relevant normative frameworks

Although no standards are mandatory, the application of **harmonized standards** greatly facilitates the demonstration of compliance. Key repositories include:

- **ISA/IEC 62443** (Series): Cybersecurity of Industrial Control and Automation Systems
- **ISO/IEC 27001** : Information Security Management System
- Future European MD-specific standards (under development)

The use of these standards creates a presumption of compliance with the corresponding requirements of the regulation.

Restructure development processes

Integrating cybersecurity by design often requires a **review of the organization** of product development:

- Integrate security reviews into project milestones
- Establish cybersecurity criteria in the choice of components
- Implement pre-market safety testing
- Create a compliance documentation validation process

Establish compliance governance

At the organizational level, MR readiness involves clearly defining **responsibilities:**

- Appoint an RM Compliance Officer
- Create a steering committee bringing together R&D, quality, legal and cybersecurity
- Establish regulatory monitoring procedures
- Define a decision-making process for compliance/cost trade-offs

OT/IoT Operational Checklist (10 Key Actions)

To help you structure your compliance process, here is an operational checklist of priority actions to take:

1. Map the machines within the MR perimeter

Identify precisely which machines in your portfolio are affected by the regulation, taking into account complete, partially completed and substantial modifications.

2. Carry out a cyber-physical risk analysis

Conduct a structured assessment of the digital threats to each type of machine and their potential impact on the safety of people, using a recognized methodology (EBIOS Risk Manager, ISO 31000).

3. Harden the default configurations

Eliminate default accounts and passwords, disable unnecessary services, and configure your devices according to the principles of least privilege.

4. Segment network architectures

Isolate critical security systems from general networks, implement trusted zones, and control cross-zone flows through industrial firewalls.

5. Implement strong authentication

Replace weak authentications (simple passwords) with robust mechanisms: multi-factor authentication, certificates, or industrial identity management solutions.

6. Encrypt sensitive communications

Protect data in transit with secure protocols (TLS, VPN) and encrypt data at rest containing sensitive information (security settings, logs).

7. Establish a secure update process

Define how firmware and software will be updated in a secure manner (cryptographic signature, authenticated channel) and communicate these procedures to users.

8. Compile the technical compliance file

Compile all the required documentation: risk analysis, technical justifications, test results, declaration of conformity and enriched instruction leaflet.

9. Create a PSIRT or vulnerability management process

Establish a structure (Product Security Incident Response Team) or formal process to monitor, assess, and remediate vulnerabilities discovered after commercialization.

10. Train and raise awareness throughout the chain

Organize training sessions for all stakeholders involved, from design to maintenance, and create a culture of cybersecurity in the organization.

How does AKENATECH support you?

Faced with the complexity of the Machine Regulation and the intersection between traditional machine safety requirements and industrial cybersecurity, **we offer comprehensive and tailor-made support** to machine manufacturers and integrators.

Diagnosis and compliance roadmap

We start by **auditing your current situation** : analysis of your machine portfolio, evaluation of your design processes, review of your existing documentation. Based on this, we develop a realistic and prioritized roadmap to achieve compliance.

Cyber-physical risk analyses

Our experts conduct **in-depth risk assessments** according to recognized methodologies (ISA/IEC 62443-3-2, EBIOS RM) and adapted to the industrial context. We identify the specific threats to your machines, assess their criticality and define proportionate protection measures.

Secure design and curing

We intervene directly in your **development projects** to integrate cybersecurity from the design phase: definition of secure architectures, selection of robust components, specification of protection mechanisms, and hardening of configurations.

Creation of technical files

We assist you in the **preparation of the compliance documentation** : drafting of the formal risk analysis, compilation of the technical file, drafting of the EU declaration of conformity and enrichment of the instruction notices with the required cybersecurity elements.

Semi-outsourced PSIRT implementation

For manufacturers who do not have the necessary in-house resources, we offer a **semi-outsourced PSIRT service** : vulnerability monitoring, report management, risk assessment, patch coordination, and customer communication.

Team training

We organize **tailor-made training sessions** adapted to different profiles: awareness of management, technical training of design engineers, operational training of support and maintenance teams.

Support for the Cyber CE Marking

In addition to the RM, we are also supporting our clients with the **Cyber Resilience Act**, which will soon introduce additional cybersecurity requirements for digital products. Our cross-functional expertise allows us to optimize your compliance efforts on these two converging regulations.

Our approach combines technical expertise in OT/IoT cybersecurity, in-depth knowledge of standards (IEC 62443, ISO 27001) and understanding of the operational constraints of manufacturers. We intervene from strategy to operational implementation, always favouring pragmatic and proportionate solutions.

FAQ

When does the Machine Regulation become mandatory?

The RM will apply from 20 January 2027. Any machine placed on the European market after this date will have to comply with the new requirements, including those relating to cybersecurity.

Do my machines currently in operation need to be updated?

No, the Regulation only applies to new machines placed on the market after the date of application. Machinery already in service is not subject to a backward compliance obligation, except in the case of a substantial modification that would amount to a new placing on the market.

Is the CE mark sufficient to guarantee conformity

The CE mark certifies that the manufacturer declares his machine to comply with the applicable requirements, but it does not constitute a certification by a third party. The manufacturer remains responsible for the effective conformity of his machine and must be able to demonstrate this via his technical file in the event of an inspection.

What standards do I need to apply to be compliant with the RM?

No standard is legally binding. However, the application of harmonized standards (such as the IEC 62443 series for cybersecurity) creates a presumption of compliance and makes it much easier to demonstrate. The specific standards for the RM are being developed by CEN/CENELEC.

How do I deal with third-party software components in my machines?

You should assess the cybersecurity risks associated with the software components you integrate, including those developed by third parties. This involves selecting reliable vendors, maintaining a component inventory (SBOM), and establishing a process for managing vulnerabilities discovered in those components.

Do I need to create a PSIRT to be compliant?

The regulation does not explicitly mandate the creation of a Product Security Incident Response Team (PSIRT), but it does require a post-market vulnerability management process. A PSIRT is the most structured solution to meet this obligation, but lighter approaches may be appropriate depending on the size of your organization.

How do the RM and the Cyber Resilience Act fit together?

These two regulations are complementary. The RM covers machines as a whole with physical and cyber security requirements. The ARC focuses on digital products (hardware and software) with cybersecurity requirements throughout the lifecycle. Some equipment will have to comply with both texts.

How long is the technical file kept?

The technical file must be kept for 10 years from the date the machine is placed on the market, or for the expected life of the machine if it is more than 10 years. It must be possible to present it to the supervisory authorities in the event of an audit.

Conclusion

The EU Machine Regulation 2023/1230 marks a major evolution of the European regulatory framework, finally recognizing that cybersecurity is no longer an option but an essential component of the security of industrial equipment. By explicitly incorporating cyber threat protection requirements, the RM requires machine manufacturers to fundamentally transform their design, documentation, and lifecycle monitoring practices.

Beyond just compliance, MR represents an opportunity to truly strengthen the resilience of your products in the face of an ever-changing threat landscape. Manufacturers that can transform this regulatory constraint into a competitive advantage – by making cybersecurity a differentiating factor – will be best positioned in an increasingly demanding European market.

At AKENATECH, we are convinced that compliance with the Machine Regulation should not be experienced as an administrative burden, but as a lever for value creation. Our mission is to support you in this transformation with pragmatism and efficiency, combining technical excellence and understanding of your operational realities.

The countdown has begun. The time to act is now.

Keywords: Machine Regulation, RM 2023/1230, industrial cybersecurity, CE marking, machinery compliance, IEC 62443, OT security, Industry 4.0, cyber-physical risk analysis, PSIRT