# Cybersecurity for Secure-by-Design machinery

Navigating the EU Machinery Regulation (MR 2023/1230)
and Cyber Resilience Act (CRA 2024/2847)

# Table of contents

# Executive Summary

The compliance environment for industrial machinery is rapidly shifting, with direct implications for product design, lifecycle cost, and EU market access. The EU Machinery Regulation (MR) and the Cyber Resilience Act (CRA) place greater emphasis on product architecture, software governance, update management, and post-market lifecycle support. OEMs that underestimate these changes risk increased retrofit costs, delayed market access, and growing lifecycle complexity.

For OEMs, cybersecurity is increasingly becoming part of core product development and lifecycle management. Greater focus is now placed on demonstrating that machines can be operated, updated, and supported in a secure and controlled manner over time. As industrial machinery becomes more connected and software-driven, OEMs are placing greater focus on secure-by-design practices, supplier coordination, and lifecycle support readiness within product development and service models.

## This white paper addresses three fundamental questions:

**What is changing under the EU Machinery Regulation and Cyber Resilience Act?**

**Why does this matter to OEMs, distributors, and supply chain partners?**

**How can Danfoss help machine manufacturers and distributors navigate this transformation effectively and competitively?**

Danfoss Power Solutions supports customers through cybersecurity-aware product development, lifecycle compliance assessment, retrofit strategy, supplier coordination, and long-term platform modernisation. Early preparation may help customers improve lifecycle planning, reduce retrofit complexity, and align future platforms with evolving regulatory and customer expectations.

# 1. Regulatory landscape: EU MR and CRA

The European industrial sector is undergoing a regulatory transition. The Machinery Regulation (EU) 2023/1230 and the Cyber Resilience Act (EU) 2024/2847 increase focus on machinery safety, software governance, cybersecurity, and lifecycle accountability for products placed on the EU market.

For OEMs, distributors, and technology partners operating within the off-highway machinery ecosystem, the implications extend beyond compliance documentation into broader operational and product development decisions. The regulations are influencing platform roadmaps, software strategies, validation approaches, and lifecycle support planning across both new and existing product families.

## 1.1 EU Machinery Regulation (MR) 2023/1230

The EU Machinery Regulation (MR) 2023/1230 replaces the previous Machinery Directive and establishes an updated regulatory framework for machinery placed on the EU market. The regulation places greater emphasis on the integration of safety, software-related functions, and digital risk considerations throughout the machinery lifecycle. Compared with the earlier directive-based framework, the regulation is intended to support more consistent application across EU member states while reflecting the increasing digitisation and automation of industrial equipment.

**EU Machinery Regulation (MR): enforcement timeline**

| 19 July 2023 | 20 January 2027 |
|---|---|
| Regulation Entered Into Force | Regulation Become Applicable |

## 1.2 Cyber Resilience Act (CRA) 2024/2847

The Cyber Resilience Act (CRA) 2024/2847 establishes harmonised cybersecurity requirements for products with digital elements placed on the EU market. The regulation addresses cybersecurity across the product lifecycle, including secure design and development practices, vulnerability handling, software updates, technical documentation, and incident reporting obligations. The CRA applies to each individual product with digital elements within off-highway sector: software, hardware with embedded software, or any digital components or programmable parts. OEMs and technology suppliers are expected to review cybersecurity governance, software maintenance processes, and supply-chain responsibilities as part of future product development and EU market access planning.

**Cyber Resilience Act (CRA): enforcement timeline**

| 10 December 2024 | 11 September 2026 | 11 December 2027 |
|---|---|---|
| Regulation Entered Into Force | Vulnerability Reporting Obligations | Main CRA Compliance Obligations |

Under both regulations, EU market surveillance authorities are also empowered to take corrective actions in cases of non-compliance, including restrictions on market access, product withdrawal measures, and financial penalties as defined within the respective regulation.

Compliance is becoming more closely linked with long-term product architecture decisions, cross-functional engineering governance, and platform modernisation priorities rather than being addressed solely as a downstream certification activity. Early and integrated planning may help reduce redesign complexity, documentation gaps, and supply-chain coordination challenges as implementation timelines approach. Late alignment can significantly increase redesign efforts and impact time-to-market.

# 2. Product development lifecycle implications under EU MR and CRA


For off-highway OEMs, the Machinery Regulation (EU) 2023/1230 and the Cyber Resilience Act (EU) 2024/2847 extend beyond traditional conformity assessment into broader product architecture, cybersecurity, software governance, and lifecycle-support considerations. OEMs increasingly need to reassess whether existing electrical, electronic, and software architectures can support evolving expectations around secure connectivity, controlled updates, traceability, and long-term operational supportability.

## 2.1 Shifts across the product lifecycle

The transition is influencing product development, validation, deployment, and post-market support activities across four key lifecycle phases:

| Lifecycle phase | Expected transition under machinery regulation | Expected transition under the cyber resilience act |
|---|---|---|
| New product design | Cyber-related risks are considered as part of safety engineering, with controls and software assessed together. | Cybersecurity shall be ensured over the entire product lifecycle from design to decommissioning. (Product integrity, availability and confidentiality wherever necessary). |
| Validation and launch readiness | Validation increasingly covers misuse scenarios, software behaviour, and alignment of technical documentation prior to market placement. | Testing increasingly includes cyberattack scenarios, secure-update validation, and documented security posture evidence. |
| Lifecycle maintenance | Safety-relevant updates and post-launch changes need to be managed within the product's conformity framework. | Manufacturers are expected to maintain vulnerability monitoring, coordinated disclosure processes, timely security updates, and maintenance commitments over the applicable support period. |
| Retrofit and legacy systems | Existing product families should be reassessed when design changes or recertification are required. | Risk-assessed retrofit measures may include authenticated updates, access control, security logging, containment controls, or phased replacement strategies. |

# 3. Secure by design - operational and lifecycle challenges for OEMs

Industrial machinery increasingly combines embedded software, connected electronics, cloud interfaces, telematics, and remote-access capabilities within integrated system architectures. As a result, cybersecurity and compliance risks extend across multiple interconnected layers rather than isolated machine components.

OEMs therefore need to address cybersecurity and lifecycle considerations during early concept definition and architecture planning rather than after development is complete.

During early product-definition phases, OEMs may need to evaluate:

- Connectivity exposure and remote-access risks
- Third-party software dependencies and inherited vulnerabilities
- Long-term update and patch-management capability
- Secure communication requirements between machine systems
- Supplier cybersecurity maturity and lifecycle-support commitments
- Hardware and software traceability requirements

## 3.1 Product design challenges:

Architecture-Level Cybersecurity and Compliance Implications for OEMs.

| Layers | Compliance implications | Key challenge |
|---|---|---|
| Connectivity layer<br>IoT connectivity / remote access/ cloud APIs / industrial protocols (e.G., MQTT, OPC UA) | Secure integration across controllers, HMIs, cloud services, and supplier systems. | Managing secure interoperability across multiple systems and suppliers. |
| Embedded software<br>Firmware / control logic / RTOs / OS / safety-related software | Third-party software increases inherited vulnerability and update-management complexity. | Tracking inherited CVEs (Common Vulnerabilities and Exposures), security updates, and third party component risks. |
| Electrical systems<br>Sensors / actuators / PLCS / HMIs / drives | Connected machine communication may require authenticated and encrypted channels. | Protecting signals and data between connected machine components. |
| Mechanical systems<br>Hydraulics / pneumatics / drivetrain / actuators | Compliance increasingly requires traceability between physical systems, embedded software, risk assessments, and conformity documentation. | Maintaining end-to-end traceability across system architecture, software components, and compliance evidence. |

## 3.2 Product development challenges:

As products move from architecture planning into implementation, validation, integration, and deployment, OEMs need to operationalize cybersecurity controls, supplier coordination, documentation management, and lifecycle governance across the machine platform.

OEMs also retain accountability for the cybersecurity posture of the final integrated machine, even where controllers, software platforms, sensors, cloud services, and connectivity modules originate from multiple suppliers.

## 3.3 Cybersecurity and lifecycle challenges across product development

As machinery lifecycles often extend over many years, supplier support duration and update availability become important considerations during component selection and commercial contracting.

OEMs may also require closer coordination with suppliers and software partners around vulnerability disclosure, Software Bill of Materials (SBOM) transparency, patch-management timelines, incident-response processes, and long-term maintenance commitments. In practice, many organisations adopt phased prioritisation across product families based on connectivity exposure, installed-base risk, commercial importance, and modernisation feasibility.

| Development layer | Compliance implications | Key challenge |
|---|---|---|
| Validation and testing Functional testing / cybersecurity testing / failure simulation | Validation increasingly includes misuse scenarios, software update behaviour, and representative cyberattack simulation. | Expanding validation scope beyond traditional testing approaches while addressing evolving cybersecurity scenarios. |
| Compliance documentation and traceability technical documentation / SBOM / risk assessments / declaration of conformity | OEMs may need lifecycle documentation covering controls, risk treatment, and conformity evidence. | Managing fragmented documentation across teams and suppliers while maintaining traceability. |
| Supplier and system integration Controllers / HMIS / sensors / telematics / multi-supplier platforms | Multi-supplier integration requires coordinated cybersecurity and interoperability management. | Managing suppliers with varying cybersecurity maturity and reducing integration gaps across the hardware-software. |
| Lifecycle support and maintenance vulnerability monitoring / secure updates / patch management / legacy retrofit | Lifecycle support increasingly includes vulnerability monitoring, updates, traceability, and long-term maintenance. | Establishing clear ownership, repeatable processes, and effective tooling for lifecycle cybersecurity management. |

## 3.4 Retrofit and legacy system challenges:

Legacy industrial platforms present additional complexity because many installed machines were originally designed for reliability and deterministic control rather than secure connectivity, continuous software maintenance, or long-term cybersecurity management. As a result, many existing platforms may lack:

- Secure boot capability
- Encryption support
- Logging and monitoring functionality
- Remote-update capability
- Modern authentication mechanisms
- Software traceability visibility
- Adequate computing or memory resources for cybersecurity upgrades

Many legacy systems were also not designed to support segmentation, secure remote access, or continuous patch management. Unsupported operating systems, unavailable security updates, limited hardware capability, and incomplete software documentation may further restrict long-term vulnerability management and lifecycle support activities.

In addition, retrofit feasibility can vary significantly across installed platforms. Hardware limitations, operational downtime constraints, validation complexity, unavailable supplier support, and high implementation costs may limit the practicality of full modernisation or redesign.
As a result, OEMs increasingly require structured, risk-based approaches to retrofit prioritisation rather than attempting large-scale replacement across all installed systems simultaneously.

Where technically feasible, retrofit activities may include, controlled remote-access mechanisms, gateway-level security controls, logging and monitoring capability, managed update frameworks, and additional detection measures designed to reduce operational exposure. However, retrofit measures may not always fully eliminate cybersecurity risk or achieve complete alignment with evolving lifecycle expectations.

# 4. Ecosystem dependency and risk assessment

The transition toward connected, software-driven industrial machinery is reshaping cybersecurity and compliance responsibilities across the industrial ecosystem. Under the Machinery Regulation and the Cyber Resilience Act, compliance depends on coordinated support across technology providers, OEMs, integrators, service partners, distributors, and end users throughout the machine lifecycle.

As machinery architectures become more interconnected, cybersecurity exposure can extend across embedded software, cloud interfaces, remote-access environments, third-party components, and field-service activities. While OEMs retain responsibility for the final machine platform placed on the EU market, long-term operational stability also depends on supplier coordination, secure integration practices, and lifecycle support capability. Supplier gaps and integration issues can significantly impact compliance readiness.

## 4.1 Cybersecurity across the machine lifecycle

| **Technology providers** (components / software / cloud platforms) | **OEMs** (Product Design / Integration ) | **System integrators / service partners** (Deployment / Retrofit / Field Support) | **End users and operators** (Operations / Maintenance) |
|---|---|---|---|
| • Secure technology<br>• Patch support<br>• Vulnerability management | • Secure-by-design implementation<br>• System validation<br>• Lifecycle accountability | • Secure deployment<br>• Retrofit and update support<br>• Service continuity | • Secure operations<br>• Access control<br>• Operational risk management |

Technology providers support secure components, embedded software maintenance, and update management capabilities, while OEMs integrate these technologies into machine architectures and operational workflows. System integrators and service partners also influence deployment quality, retrofit execution, and ongoing support across installed machinery environments.

Consequently, cybersecurity readiness increasingly depends on coordination across the broader industrial ecosystem rather than on the OEM platform alone.

## 4.2 Distributor responsibilities under the CRA

Under the Cyber Resilience Act, distributors may assume additional responsibilities where products are modified, configured, integrated, or rebranded before placement on the EU market. Activities such as firmware customisation, software integration, non-standard deployment, or product modification may increase the need for conformity validation and documentation visibility across distribution channels.

As a result, distributors may increasingly require closer coordination with OEMs and technology partners to validate product status, software provenance, and conformity evidence prior to market placement or operational deployment.

# 5. Strategic considerations for OEMs

The Machinery Regulation (EU) 2023/1230 and the Cyber Resilience Act (EU) 2024/2847 are accelerating the transition toward connected and software-enabled machine platforms. For OEMs, the focus is extending beyond initial compliance toward lifecycle management, supplier governance, and long-term platform supportability.

## 5.1 Key decision areas for OEMs

OEMs increasingly need to translate regulatory expectations into practical product-development and lifecycle-management decisions. Key considerations may include:

- Can existing platforms support secure updates, traceability, and lifecycle monitoring?
- How will Software Bill of Materials (SBOM) governance be managed across suppliers and product lifecycles?
- Who is responsible for vulnerability monitoring, patching, and update management after deployment?
- Are suppliers able to support cybersecurity transparency, traceability, and long-term maintenance expectations?

These decisions directly influence product viability and long-term competitiveness in the EU market.

Addressing these questions may require OEMs to strengthen lifecycle governance, supplier coordination, platform maintainability, and installed-base planning across both new and existing machine environments.

These considerations may also influence long-term operating expenditure (OPEX), particularly where vulnerability management, software maintenance, retrofit planning, and update support extend across large installed machine bases.

## 5.2 Operational priorities under the EU MR and CRA

| Strategic priority | Business impact |
|---|---|
| Platform modernisation | Supports secure updates, scalability, and long-term maintainability |
| Lifecycle management | Improves visibility into vulnerability management and support planning |
| Supplier governance | Reduces integration gaps and traceability challenges |
| Installed base planning | Helps prioritize retrofit and replacement decisions |
| Cross-functional alignment | Improves coordination across engineering, compliance, IT, and service teams |

# 6. Danfoss Power Solutions role in supporting OEM compliance transformation

Under the Machinery Regulation (EU) 2023/1230 and the Cyber Resilience Act (EU) 2024/2847, OEMs are moving beyond product-level compliance toward system-level and lifecycle accountability, where secure update capability, traceability, and long-term supportability become critical.

Danfoss Power Solutions works with OEMs across real machine platforms, translating evolving EU regulatory expectations into practical and scalable engineering, integration, and lifecycle management approaches across both new and existing machine platforms. This enables end-to-end support across the machine lifecycle, from early architecture planning and system integration through deployment, retrofit, and ongoing lifecycle management.

This is built on system integration expertise, component knowledge, and lifecycle experience across complex machinery environments.

## 6.1 Danfoss Power Solutions end-to-end compliance and lifecycle enablement


## 6.2 Danfoss Power Solutions support areas across the machine lifecycle

Danfoss Power Solutions supports OEMs across key product-development and lifecycle-management areas, including:

- Secure-by-design product architecture
- Embedded software development
- SBOM readiness and technical documentation support
- Multi-system integration and interoperability management
- Vulnerability monitoring and update-management processes
- Retrofit assessment and legacy platform modernisation
- Lifecycle governance and long-term maintenance planning
- Supplier coordination and traceability across distributed machine ecosystems

As regulatory expectations continue to evolve, OEMs increasingly require partners that can support both compliance readiness and long-term platform maintainability. Danfoss Power Solutions combines product engineering, lifecycle expertise, and system-integration capabilities to support OEMs across complex machinery environments.

# 7. OEM action priorities and next steps

## What to do next: prioritized actions for EU MR and CRA readiness

### Immediate (0–6 Months)

- Conduct EU MR and CRA gap assessments across product portfolios
- Assess installed-base and legacy-system cybersecurity risks
- Establish cross-functional compliance governance
- Initial supplier cybersecurity and software-dependency reviews

### Mid-Term (6–18 Months)

- Implement SBOM and software-traceability processes
- Develop vulnerability monitoring and secure update capabilities
- Strengthen cybersecurity testing and incident-response readiness
- Prioritise retrofit versus replacement strategies across installed bases

### Long-Term (18+ Months)

- Transition toward secure-by-design product architectures
- Integrate cybersecurity into lifecycle support models
- Establish monitoring, update, and governance processes
- Align product roadmaps and retrofit strategies with EU regulation

OEMs that proactively align product architecture, cybersecurity governance, and lifecycle support planning may be better positioned to reduce long-term complexity, strengthen competitiveness, and capture new market opportunities as regulatory expectations evolve.

## Turn EU MR and CRA readiness into a competitive advantage

Don’t just navigate the new regulations. Use them to build the future.

Contact your local Danfoss experts

# 8. Frequently asked questions

## EU Machinery Regulation (MR)

### 1. What is the EU Machinery Regulation (MR)?

The MR introduces mandatory cybersecurity requirements for machinery as part of product safety. It extends OEM responsibility beyond mechanical systems to software, connectivity, and system behaviour.

### 2. Which machines fall under the cybersecurity requirements?

Cybersecurity requirements apply to machinery where cyber risks may impact safety, including machines with connectivity, remote access, external interfaces, or safety-critical control systems.

### 3. What are OEM obligations after product launch?

Manufacturers must ensure machines remain safe over time, including after updates or modifications, by controlling software changes, configurations, and system behavior to prevent safety risks and keep cybersecurity aligned with safety requirements throughout the lifecycle.

### 4. When does the Machinery Regulation apply?

The regulation applies fully from 20 January 2027. Manufacturers should begin adapting product design and development processes early, as cybersecurity requirements directly impact system architecture, safety concepts, and lifecycle management.

### 5. What does the Machinery Regulation mean for customers?

The regulation protects machinery against cyber risks that could affect safe operation. Customers benefit from improved safety and reliability and are expected to follow secure usage, maintenance, update, and access practices.

## Cyber Resilience Act (CRA)

### 1. What is the Cyber Resilience Act (CRA)?

The CRA sets harmonized mandatory cybersecurity requirements for products with digital elements on the EU market, covering the full product lifecycle to ensure consistent cybersecurity, resilience, and vulnerability management over time.

### 2. Which products fall under the CRA?

The CRA applies to products with digital elements capable of connecting, directly or indirectly, to networks or other devices, including embedded systems, control systems, and industrial equipment. In practice, most modern industrial and mobile machinery products fall within the scope.

### 3. How do the CRA and the Machinery Regulation differ?

The CRA and the MR set complementary cybersecurity requirements: the CRA covers lifecycle cybersecurity, while the MR addresses cybersecurity as a safety-related requirement to prevent hazardous situations. Together, they require manufacturers to manage both lifecycle and safety-related cyber risks.

### 4. What are OEM obligations after product launch?

The CRA introduces continuous obligations beyond market placement, requiring manufacturers to monitor vulnerabilities, provide timely updates and patches, ensure secure update mechanisms, report actively exploited vulnerabilities, and maintain structured lifecycle governance across the organization and supply chain.

### 5. When does the CRA apply?

The CRA's vulnerability handling and incident reporting apply from 11 September 2026, with full application from December 2027. Early preparation is essential given the impact on development, supplier management, and lifecycle responsibilities.

### 6. What does the CRA mean for customers?

The CRA strengthens cybersecurity and transparency across products, providing customers with better protection and long-term support, while requiring timely updates, secure configuration, and incident cooperation.

### 7. How does the CRA affect the supply chain?

Under the CRA, manufacturers remain responsible for product compliance, including third-party components and software. This requires supplier due diligence, clear allocation of responsibilities, secure component design, and rusted partnerships across the value chain.

## Disclaimer:

This document is provided for general informational purposes only. Any information contained herein is non-binding and shall not be considered as legal or regulatory advice. Customers are responsible for assessing the applicability of regulatory requirements to their specific products and use cases. Danfoss makes no representation or warranty regarding the completeness or accuracy of the information provided and reserves the right to make changes without notice. 

**Danfoss A/S**
Nordborgvej 81
6430 Nordborg
Denmark
danfoss@danfoss.com
CVR reg. no. 20165715

BE563358262398en-000101