Cybersecurity and Machine Safety Under the EU Machinery Regulation

Picture an industrial robot connected to a factory network. Its safety PLC, firmware and configuration data all affect how it behaves. If one of those is altered, the problem can move quickly from cybersecurity to machine safety.

That is what the EU Machinery Regulation (EU) 2023/1230 is designed to address. Beginning Jan. 20, 2027 the regulation becomes mandatory, replacing the Machinery Directive 2006/42/EC for machinery placed on the EU market from that date. Because it is a regulation rather than a directive, it applies directly across EU member states.

Why does that matter to manufacturers? Because if you build connected industrial equipment, cybersecurity can no longer be treated as separate from machine safety. How the machine protects safety-related software, data and control systems now has to be part of the design discussion.

Cybersecurity enters the machine safety conversation

The Machinery Regulation includes requirements under “protection against corruption.” In practical terms, safety-related hardware, software and data have to be protected from accidental or intentional changes that could affect the safe operation of the machine.

That includes changes introduced through another connected device, including remote connections, as well as unauthorized changes to software, configuration or other data the machine relies on to operate safely.

For a connected industrial system, that can mean protecting things such as safety PLC settings, control system software and configuration data from changes that could create hazardous conditions.

There is a recordkeeping requirement that deserves attention from system designers as well. For applicable control systems, a tracing log covering intervention data and versions of safety software uploaded after the machine is placed on the market or put into service must be enabled for five years after the upload, for purposes of demonstrating conformity if requested by a competent national authority.

Go back to that connected industrial robot.

If someone alters a safety PLC setting, replaces firmware or changes configuration data in a way that affects motion, cybersecurity has become a safety problem. The manufacturer may need to know what changed, which software version was running and what happened in the system around the event.

What does the EU Machinery Regulation mean for memory architecture?

The Machinery Regulation does not tell an engineer to use MRAM, flash or any other memory technology. It does create reasons to look carefully at what information the system needs to keep and how reliably it needs to keep it.

© 2026 Everspin Technologies, Inc. | everspin.com

Think about the data inside a machine that may matter after something goes wrong: configuration and calibration values, safety-related parameters, event histories, fault records, diagnostic information, software versions, counters, update status and recovery state.

Some of that information may change only occasionally. Other data may be updated continuously over years of machine operation.

Now consider what happens during an interruption.

If the machine records an event immediately before power disappears, is the record still there when the system restarts?

If configuration changes, is the latest state preserved?

If firmware is being updated, can the system retain the status or version information it needs for recovery?

If the design relies on battery-backed memory to preserve machine state, is that still the architecture you want to carry forward?

Those are memory questions as much as they are software questions.

Why MRAM fits some of these workloads

Everspin MRAM is non-volatile, so committed data remains in memory when power is removed. It also supports high write endurance and fast writes, which makes it useful for information that changes frequently rather than data that is written once and left alone.

That combination is useful in systems that continuously record alarms, faults, operating events or diagnostic information. Everspin already supports industrial control applications where MRAM is used to retain logs, configurations and real-time data through power interruptions.

The same persistence can be useful for configuration and machine state. Values updated during operation remain available after a reset or loss of power without relying on a battery to keep volatile memory alive.

Everspin's xSPI STT-MRAM also supports byte-level reads and writes in persistent-memory mode without requiring an erase before rewriting the same location. For frequently changing records, that can simplify how persistent data is managed compared with architectures that have to account for erase operations around updates.

Firmware status, software version data, configuration parameters and recovery state are other examples of information the larger system may need during an update or restart.

The memory does not decide whether the firmware is authentic or whether a rollback should be permitted. It provides a persistent place to keep the state those functions may depend on.

MRAM is one part of the security architecture

Persistent memory gives the system a place to keep information it may need after a power loss or reset, whether that is an event record, configuration data, software version information or update

© 2026 Everspin Technologies, Inc. | everspin.com

state. What happens to that information, and how it is protected, depends on the rest of the architecture.

The processor and security software still have to authenticate firmware, verify signatures and enforce update or rollback policies. The system decides who can change configuration data and how the integrity of logs or other records is protected. MRAM keeps the information available; it does not perform those security functions.

Using MRAM does not make a machine compliant with the EU Machinery Regulation. The manufacturer is still responsible for the risk assessment, applicable safety and cybersecurity controls, technical documentation and conformity assessment.

How does the EU Machinery Regulation overlap with the Cyber Resilience Act?

A connected industrial machine may also fall within the scope of the EU Cyber Resilience Act, or CRA. That can include systems built around PLCs, embedded controllers, HMIs and industrial PCs, particularly when they include Ethernet or wireless connectivity, remote maintenance or other connections to devices and networks. Whether the CRA applies depends on the particular product and its intended or reasonably foreseeable use, so the presence of a PLC or HMI alone is not the legal test.

The two regulations address different parts of the problem.

	EU Cyber Resilience Act	EU Machinery Regulation
Primary focus	Cybersecurity	Machine safety
Applies to	Products with digital elements within the CRA's scope	Machinery and related products covered by Regulation (EU) 2023/1230
Key requirements	Cybersecurity risk assessment, secure development, vulnerability management, security updates and incident reporting	Essential health and safety requirements, including protection against corruption and safety and reliability of control systems
Lifecycle	Addresses cybersecurity throughout the product lifecycle	Focuses on machinery safety throughout design, manufacture and use
Protects	Confidentiality, integrity and availability of products and data	People from hazards created by machinery, including hazards that can result from digital or cybersecurity failures

The Machinery Regulation is focused on machinery safety. In the cybersecurity context, the practical question is whether a digital event could create a hazardous machine.

© 2026 Everspin Technologies, Inc. | everspin.com

The CRA looks more broadly at cybersecurity across the product lifecycle. It includes requirements around cybersecurity risk assessment, secure design and development, vulnerability handling, security updates, software bills of materials, coordinated vulnerability disclosure and support throughout the product's defined support period. Reporting obligations for actively exploited vulnerabilities and severe security incidents took effect Sept. 11, 2026, with the CRA applying more broadly beginning Dec. 11, 2027.

The CRA itself recognizes that the two regulations can overlap. It specifically points to the Machinery Regulation's requirements covering protection against corruption and the safety and reliability of control systems. A manufacturer's work to address the same cybersecurity risks may support compliance under both regulations, but that relationship still has to be demonstrated as part of the applicable conformity processes.

What should machine designers be looking at now?

Jan. 20, 2027, is close enough that manufacturers developing machinery for the EU market should already be looking at these requirements in the context of the system architecture.

Start with the data the machine cannot afford to lose.

Which safety-related records need to survive a restart? What configuration or calibration information changes during operation? What intervention or software version information needs to be traceable? Are event and diagnostic records being written frequently? Does the system rely on a battery or capacitor simply to keep critical state alive?

Then look at the memory behind those functions.

The EU Machinery Regulation does not prescribe MRAM. It does make the handling of safety-related software, configuration, intervention records and control system data more consequential.

For machines that update important information frequently and need that information to remain available through power loss or reset, persistent memory belongs in the design conversation.

If you are working through the EU Machinery Regulation, the Cyber Resilience Act or the memory architecture in a connected industrial system, Everspin can help you look at where MRAM makes sense and where it does not.

© 2026 Everspin Technologies, Inc. | everspin.com