

EXECUTIVE SUMMARY

The EU Cyber Resilience Act (CRA) makes cybersecurity a lifecycle requirement for products with digital elements, including secure design, vulnerability handling, security updates and evidence that security functions remain effective over time. For engineering teams, that puts added attention on how persistent system state is written, retained and recovered through updates, resets and power interruptions.

This white paper examines how memory behavior can support CRA-relevant security functions by comparing generic NOR Flash with Everspin MRAM. MRAM does not make a product CRA-compliant, but its high endurance, fast writes, non-volatility and no erase-before-write behavior can simplify frequently updated persistent state and improve robustness in applications that must preserve critical information across the product lifecycle.

THIS PAPER FOCUSES ON

Secure boot | OTA firmware updates | Security logs and audit trails | Security counters and anti-rollback | CRA technical documentation and evidence

Important scope: MRAM does not make a product automatically CRA-compliant. The paper evaluates how memory characteristics can support implementation robustness for CRA-relevant functions.

Contents

Introduction.....2

EU Cyber Resilience Act regulation and its requirements.....2

Critical scope for Chipmakers.....3

Advantages to use Everspin MRAM for EU Cyber Resilience Act (CRA).....4

Everspin MRAM vs traditional non-volatile technologies such as NOR Flash.....4

Detailed comparison of MRAM vs NOR Flash for Secure boot, OTA updates, Security logs and CRA evidence requirements.....5-6

Summary Table.....7

Conclusions.....7



Introduction

This document provides a detailed technical comparison between NOR Flash memory and Everspin Technologies MRAM in the context of compliance with the EU Cyber Resilience Act (CRA). It evaluates how each memory technology supports key security functions required under the CRA, focusing on secure boot, over-the-air (OTA) firmware updates, security logs and audit trails, security counters and anti-rollback and the generation of technical documentation and evidence for CRA compliance. The document also includes a summary table and guidance Everspin customers can use to communicate how MRAM supports CRA-related security goals in their own products.

What is the EU Cyber Resilience Act regulation and its requirements?

Cybersecurity is now a core design requirement for industrial and connected devices. In addition to protecting data and ensuring regulatory compliance, modern systems must be **resilient by design**, enabling secure boot, preserving firmware and data integrity and sustaining a trusted operational state across the product's lifetime.

The Cyber Resilience Act (CRA) is an EU regulation establishing mandatory cybersecurity requirements for hardware and software products with digital elements. It mandates secure design, vulnerability handling and free security updates across a product's lifecycle. It covers connected consumer devices, industrial hardware and software sold in the EU, excluding sectors with independent cybersecurity regulations such as aviation, medical devices and automotive. Mandatory reporting obligations beginning in September 2026 and full CRA compliance required for products placed on the EU market from December 2027, organizations need to understand not only what the regulation requires, but how to translate those obligations into real engineering, documentation and lifecycle processes, backed by CE marking requirements.

EU Cyber Resilience Act (CRA) requirements

Secure Firmware Updates address security vulnerabilities and maintain up-to-date protection against the latest threats.	Unauthorized Access Protection protect the operation and behavior of products and their data.
Secure Data Storage protect the confidentiality and integrity of stored data.	Secure Communication protect the confidentiality and integrity of transmitted data.
Secure Boot protect product operation and behavior.	CRA Timing Mandatory reporting obligations beginning in September 2026 and full CRA compliance required for products placed on the EU market from December 2027.



Critical Scope for Chipmakers

If a general purpose semiconductor (like a standard DRAM or NAND flash drive) is sold separately on the open market, it is legally treated as an integrated component. If it is "reasonably foreseeable" that an OEM will build it into a connected device (such as a smart home appliance, a router or an industrial equipment), the semiconductor falls fully in-scope of the CRA. Everspin Technologies MRAM chips do not fall directly under the EU Cyber Resilience Act as standalone raw hardware components, but devices utilizing them might if they are integrated into finished connected products.

PERSISTENT SECURITY STATE

A system-level view of the CRA-relevant functions discussed in this paper

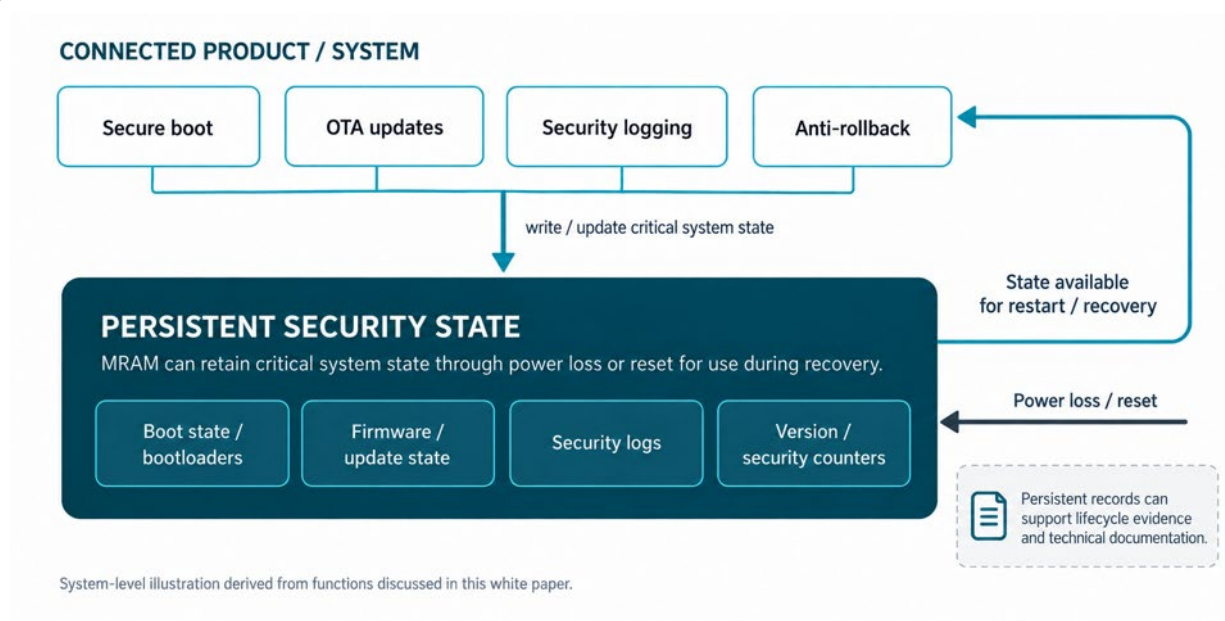


Figure 1. System-level illustration derived from functions discussed in this white paper.



Advantages of using Everspin MRAM for EU Cyber Resilience Act (CRA)

Using Everspin MRAM helps to meet the stringent EU Cyber Resilience Act (CRA) requirements by protecting data at the hardware level. MRAM natively supports "**security by design**" by preventing tampering, eliminating the need for vulnerable external batteries and enabling ultra-fast, secure firmware rollbacks to survive active exploits.

01 Instant and Permanent Data Retention Unlike volatile RAM, MRAM is non-volatile. During sudden power losses, brownouts or deliberate fault-injection attacks, MRAM instantly freezes and retains the exact system state without losing encryption keys or running logs.	02 No Battery Required Traditional battery-backed SRAM (BBSRAM) is vulnerable to physical degradation, requires maintenance and adds a significant attack surface to your software Bill of Materials. MRAM does not degrade, reducing physical maintenance and avoiding the need for continuous power.
03 Secure Boot and Rollbacks The CRA demands that the product handle vulnerabilities dynamically. MRAM's near-infinite read/write endurance allows to securely log system states and rapidly write new firmware updates. If an update fails or is compromised, the device can instantly and reliably reboot from a secure, previously saved state.	04 Immutable Hardware Root of Trust MRAM can permanently store cryptographic keys, bootloaders and initial firmware states in one-time programmable (OTP) sectors. This establishes a physical Hardware Root of Trust, making it virtually impossible for attackers to alter the initial device identity.
05 Resistance to Power-Glitch Attacks Hackers often use power-interruption techniques to bypass access controls. Because MRAM is a magnetic technology, it isn't susceptible to having its memory bits altered or corrupted by power-glitching.	06 Enhanced Obfuscation The magnetic nature of MRAM makes reverse engineering, chip de-capping and reading memory contents using electron microscopes significantly more difficult than with traditional Flash or EEPROM.

MEMORY TECHNOLOGY COMPARISON

Everspin MRAM vs traditional non-volatile technologies such as NOR Flash

From a Cyber Resilience Act (CRA) perspective, the choice is usually not MRAM or NOR Flash, because the CRA is focused on security capabilities, vulnerability management, secure updates and lifecycle support, not on specific memory technology. The CRA regulation sets cybersecurity requirements for products with digital elements, rather than mandating a particular non-volatile memory type. That being said, if you're designing an embedded product that must be CRA-compliant, MRAM can offer some practical advantages over a generic NOR Flash.



Advantages of MRAM for CRA-related security goals

- **Higher endurance** for frequent secure logging, audit trails, configuration updates, and key rotation.
- **Faster write performance**, which can simplify secure event logging and firmware management.
- **No erase-before-write requirement**, reducing software complexity and lowering the risk of corruption during unexpected power loss.
- **Excellent data retention and resilience**, helping preserve security-critical state information.

Detailed comparison of MRAM vs NOR Flash for Secure boot, OTA updates, Security logs and CRA evidence requirements

1. Secure Boot

MRAM does not make a product automatically CRA compliant, but it can reduce security implementation risks and improve robustness of certain CRA relevant functions.

NOR FLASH

NOR Flash implementation typically involves a Boot ROM verifying the digital signature of firmware stored in NOR Flash, with firmware either executed directly from NOR (execute-in-place, XIP) or copied to RAM. This approach is widely deployed and well understood. However, challenges include the need to erase sectors before reprogramming during firmware updates, managing boot image integrity in case of power loss during updates and additional software logic for rollback and recovery.

MRAM

MRAM offers advantages such as no erase-before-write requirement, easier implementation of atomic updates, better tolerance to unexpected power interruptions and the ability to frequently update boot status variables and rollback metadata without wear concerns. The latest xSPI STT-MRAM family of products also supports execute-in-place. While the CRA does not specifically mandate MRAM, its features can simplify secure boot implementation and enhance robustness.

2. OTA (Over-the-Air) Firmware Updates

NOR FLASH

NOR Flash architectures commonly include an active image, a backup image and an update staging area. Challenges involve erase cycles during firmware replacement and the need for larger memory to store two complete images and wear concerns with frequent updates.

MRAM

MRAM provides fast writes, very high endurance, no erase operations, more flexibility for delta updates and reduced concerns about update frequency. For industrial devices requiring security patches over 10+ years, MRAM's endurance is particularly beneficial. CRA requires manufacturers to deliver security updates and remediate vulnerabilities throughout the product's supported lifetime.



3. Security Logs and Audit Trails

Cybersecurity frameworks often require recording authentication attempts, security events, firmware update history, tamper events and diagnostic information.

NOR FLASH

NOR Flash has issues with frequent writes accelerating wear and may require wear-leveling software. Logs are typically buffered in RAM and periodically committed.

MRAM

MRAM offers extremely high write endurance, near-RAM-like write behavior, immediate persistence and better retention of logs after sudden power loss. This enables immediate writing of login failures, secure boot failures, cryptographic key usage counters and intrusion detection events without worrying about erase cycles. While CRA does not mandate a specific logging technology, MRAM's persistent and reliable security-event storage supports vulnerability management and incident handling.

4. Security Counters and Anti-Rollback

Secure systems maintain firmware version counters, monotonic counters, secure boot state information, and anti-rollback protection.

NOR FLASH

NOR Flash counters require repeated writes to the same areas, necessitating additional wear-management mechanisms.

MRAM

MRAM allows counters to be updated almost like RAM variables with very high endurance and simpler implementation.

5. CRA Technical Documentation and Evidence

The CRA requires security risk analysis, secure development practices, vulnerability handling, delivery of security updates and ongoing functionality of security features during the product lifetime.

NOR FLASH

NOR Flash evidence packages typically include secure boot design, firmware signing architecture, OTA update mechanism, flash endurance analysis, recovery and rollback testing.

MRAM

MRAM evidence packages include the same items, but may make it easier to justify long-term endurance, frequent security logging, high-update environments and power-failure resilience. CRA conformity assessment is based on security design and lifecycle processes and MRAM potentially can help to ease engineering evidence.



Summary Table

This summary table highlights MRAM's advantages in robustness, endurance and flexibility for CRA-relevant security functions.

CRA Security Function	Generic NOR Flash	Everspin MRAM
Secure Boot	Good	Better power-fail robustness
OTA Updates	Good	Enhanced endurance, increased write bandwidth and flexibility
Security Logs	Adequate with wear management	Excellent
Intrusion/Event Logging	Adequate	Excellent
Anti-Rollback Counters	Requires wear considerations	Ideal
Lifetime Security Updates	Good	Near infinite write endurance for frequent updates
CRA Compliance	Yes	Yes
CRA Risk Reduction	Medium	High

Conclusions

The document suggests a positioning statement for products under the Cyber Resilience Act. Products expected to receive security updates for many years, maintain persistent security logs and withstand power interruptions can benefit from MRAM's endurance and instant-write characteristics. These features reduce implementation complexity and improve robustness of CRA-relevant security functions compared with conventional NOR Flash. This statement is presented as the most technically accurate CRA-oriented value proposition for Everspin MRAM.



Contact information and legal notice

AUTHOR / HOW TO REACH US

Author: Paolo Schiappacasse

Title: EMEA Field Technical Specialist

How to Reach Us:

www.everspin.com

E-Mail:

support@everspin.com

orders@everspin.com

sales@everspin.com

REGIONAL CONTACTS

USA/Canada/South and Central America

Everspin Technologies

5670 W. Chandler Road, Suite 100

Chandler, Arizona 85226

+1-877-347-MRAM (6726)

+1-480-347-1111

Europe, Middle East and Africa

support.europe@everspin.com

Japan

support.japan@everspin.com

Asia Pacific

support.asia@everspin.com

LEGAL NOTICE

Information in this document is provided solely to enable system and software implementers to use Everspin Technologies products. There are no express or implied licenses granted hereunder to design or fabricate any integrated circuit or circuits based on the information in this document. Everspin Technologies reserves the right to make changes without further notice to any products herein. Everspin makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Everspin Technologies assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. "Typical" parameters, which may be provided in Everspin Technologies data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters including "Typical" must be validated for each customer application by customer's technical experts. Everspin Technologies does not convey any license under its patent rights nor the rights of others.

Everspin Technologies products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Everspin Technologies product could create a situation where personal injury or death may occur. Should Buyer purchase or use Everspin Technologies products for any such unintended or unauthorized application, Buyer shall indemnify and hold Everspin Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Everspin Technologies was negligent regarding the design or manufacture of the part. Everspin™ and the Everspin logo are trademarks of Everspin Technologies, Inc. All other product or service names are the property of their respective owners.