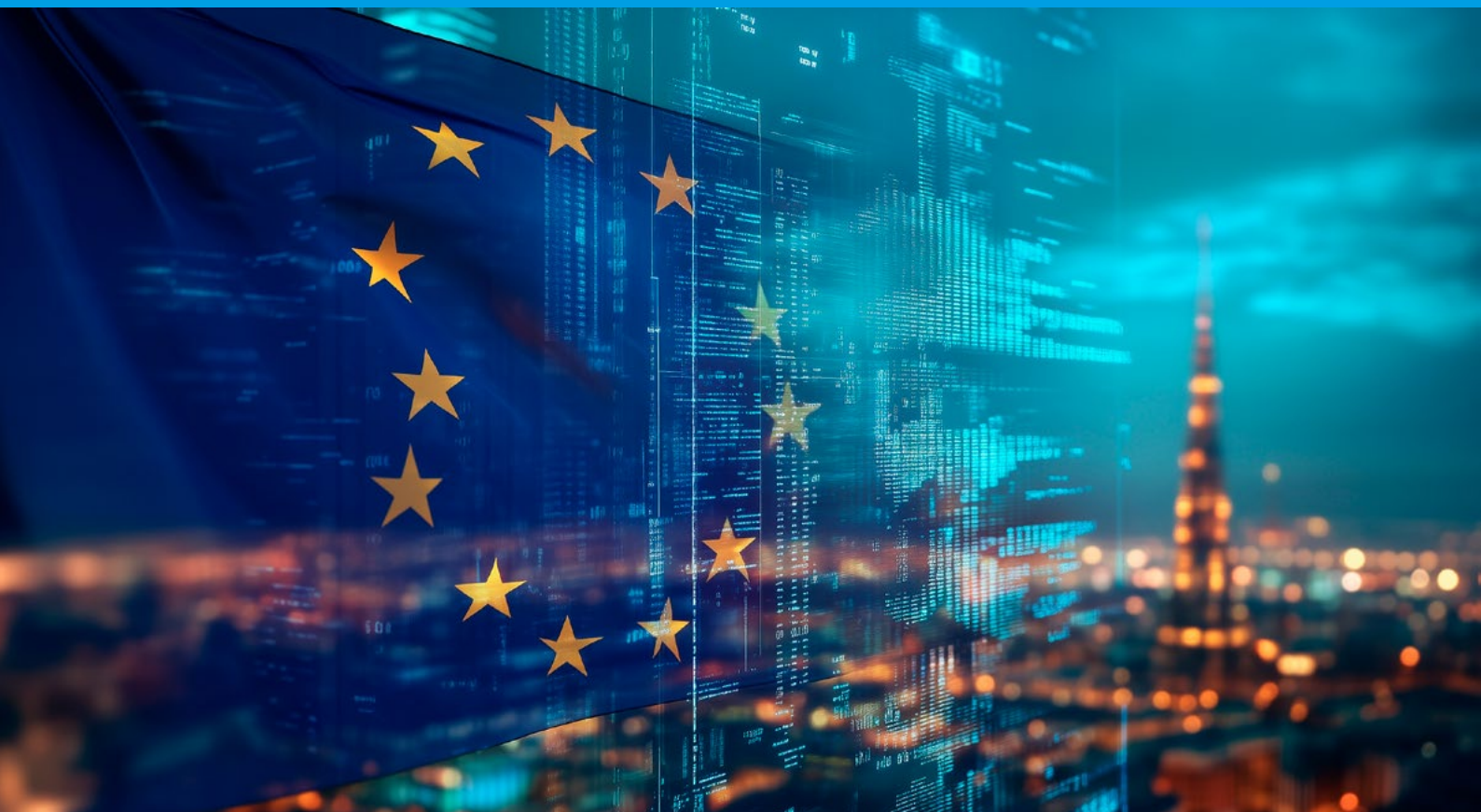
swissbit®

White Paper

Making existing products CRA-compliant

Content Page



The EU Cyber Resilience Act (CRA) [1], which came into force on December 10, 2024, requires all manufacturers of products with digital elements to implement basic cybersecurity measures. This applies to all products of this type placed on the EU market from December 11, 2027. Product managers in the industrial sector are therefore faced with the question of whether they can continue to sell their products or take a risk if the company does not improve its security. A retrofit with secure Swissbit memory components makes it possible to protect many such systems and continue to sell them in the EU. Experienced Swissbit partners can help with integration.

1. What specific requirements does the CRA impose?

This white paper does not deal with the legal details of the CRA, but with the core questions that many manufacturers in the industrial environment are facing: **Can I continue to sell my existing products in the EU after the end of 2027? Do I have to discontinue the product lines? And above all: How can I retrofit products to make them "CRA-ready"?**

First, here is a quick reminder of the most important points about the CRA: According to the CRA, all products with digital elements sold in the EU from the end of 2027 must include basic cybersecurity functions. This includes all products that can be connected digitally to another device or network: firstly, hardware products with networked functions (from smartphones and laptops to smart home solutions, connected toys, and smart electricity meters to industrial control systems); secondly, software products (from mobile device apps to computer games and enterprise software suites). Special rules apply to certain segments (national security, medical technology, vehicles, maritime, and aviation). Non-commercial open-source solutions are exempt from the CRA.

EU lawmakers require manufacturers of affected hardware and software products to make their products cyber resilient, i.e., protect them against cyberattacks and misuse. To do this, they must:

- **Take security measures into account during product design** ("security by design")
- **Secure access to the product** (e.g., through authentication, access control, protection against unauthorized physical access)
- **Carry out software updates securely** – i.e., signed and verifiable
- **Manage vulnerabilities,** i.e., disclose and fix known vulnerabilities
- **Ensure security throughout the expected or normal lifetime of the product,** but for at least five years

The CRA is an EU regulation, not a directive such as NIS 2. It therefore came into force when it was adopted by the EU without the need for national legislation.

Timeline for the introduction of the CRA

November 20, 2024	December 10, 2024	September 11, 2026	December 11, 2027
The CRA is published in the Official Journal of the EU.	The CRA enters into force.	Incidents and vulnerabilities affecting products are reportable.	The CRA requirements apply to all products with digital elements newly placed on the EU market, including compliance with essential cybersecurity requirements, the handling of vulnerabilities throughout the product lifecycle, and information obligations towards users.

Proof of CRA compliance is usually provided by means of CE marking, i.e., self-assessment by the manufacturer. For products in higher risk classes, an assessment by a notified body is required. In addition, the EU plans to set up a reporting platform where manufacturers must report actively exploited vulnerabilities and serious security incidents within 72 hours. An initial report must even be made within 24 hours.

Basic information and technical guidelines can be found on the CRA page of the Federal Office for Information Security (BSI) [2], and further useful information is available on the websites of the VDMA and VDE (see, for example, [3] and [4]). For legal questions, it will be necessary to consult a specialist lawyer. The following section, however, deals with the technical approaches Swissbit can use to help affected manufacturers achieve CRA compliance with their products.

2. What does the CRA mean for manufacturers of industrial products?

The issue of CRA compliance is particularly critical in the industrial environment. This is because it is to be expected that the EU's conformity assessment bodies (notified bodies) will keep a close eye on the CRA compliance of industrial products due to the high-risk situation in this sector.

From RED to CRA

Manufacturers of radio-enabled devices (mobile communications, Wi-Fi, Bluetooth, IoT radio standards) are already familiar with the upcoming process in principle from the EU's Radio Equipment Directive (RED) of 2014, implemented in Germany by the Radio Equipment Act of 2017. Here, too, the aim is to ensure operational safety and to verify this by means of CE marking. The "delegated regulation" 2022/30/EU published at the beginning of 2022 contains additional requirements regarding cybersecurity, data protection, and fraud prevention.

From August 1, 2025, all radio-networked devices must comply with EU requirements, i.e., meet standards such as EN 18031. Manufacturers affected by RED are, so to speak, "pioneers" of CRA compliance, although the CRA goes much further.

Important to know:

- From the end of 2027, **no new products with digital elements that are not CRA-compliant may be placed on the EU market,** except in the form of spare parts.
- **Manufacturers must plan how their new products will comply with CRA** and whether they will phase out existing products or update them to ensure CRA compliance.
- **Manufacturers may need to adapt production processes** to comply with "security by design" requirements and establish processes for vulnerability management, including timely reporting of attacks and vulnerabilities.
- To make matters worse, **suppliers in the industry sometimes have to deal with years of lead times** when products are discontinued.

Product managers for industrial products must therefore develop a strategy for CRA compliance for their portfolios as quickly as possible – after all, this cannot be done overnight. Otherwise, they run the risk of soon violating discontinuation deadlines and/or EU law. In addition, customers in the industrial sector are naturally aware that the CRA is imminent. They will therefore probably opt for CRA-compliant offers from now on. This increases the pressure to act. **So now is the time to act without hesitation!**

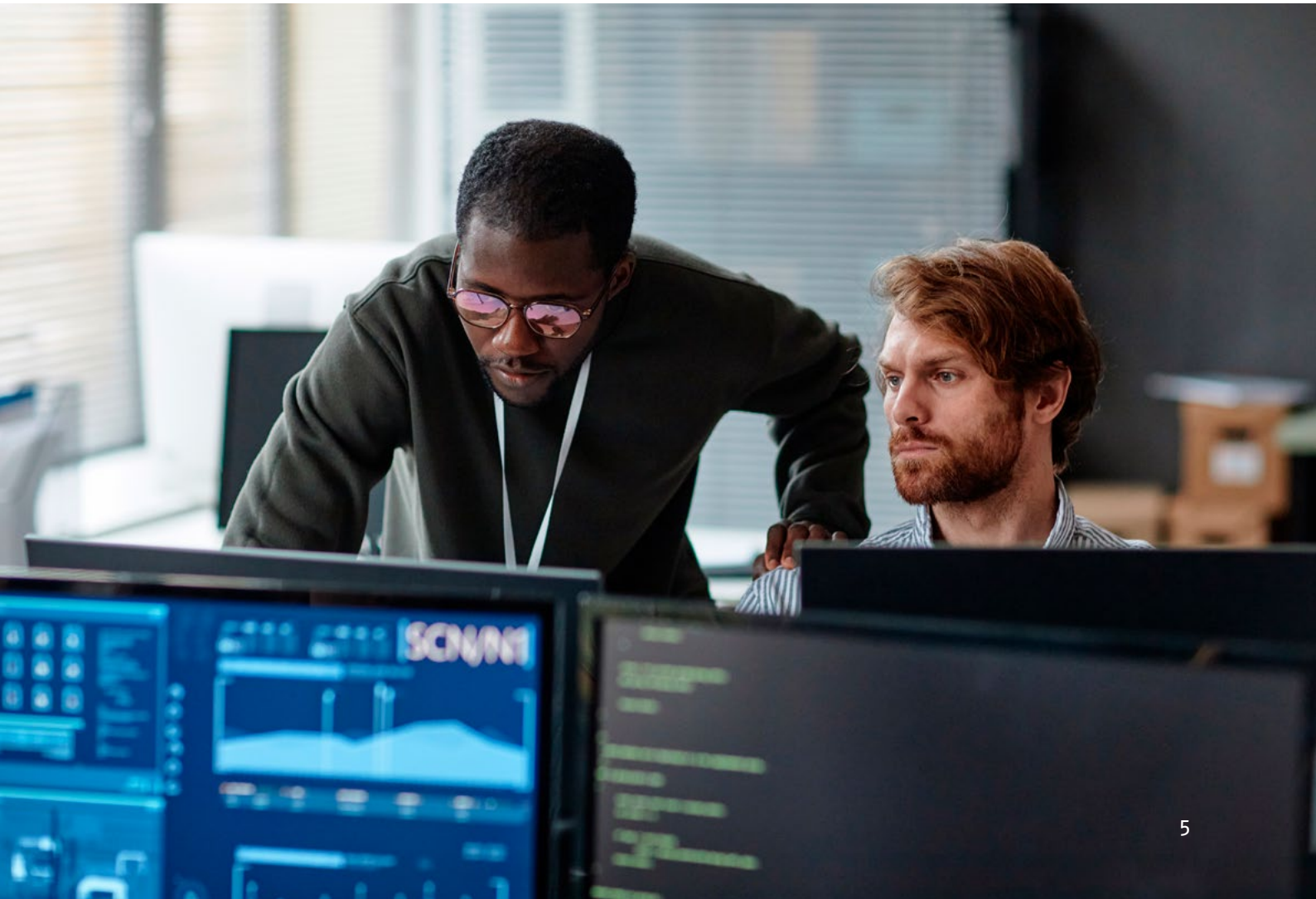
3. How can manufacturers quickly achieve CRA compliance for existing products?

Industrial products may be well designed, robust, and proven in practice, but they are not necessarily "CRA-ready." There are various reasons for this, including:

- **There are no or insufficient authentication mechanisms** for (remote) access to the product (e.g., only default passwords printed in the manuals).
- **Data,** e.g., access data, **is stored unprotected** on the device.
- **There is no secure procedure** for firmware updates.
- **The integrity of the system is not guaranteed** due to the lack of hardware anchoring of the software (secure boot).

However, this does not mean that such products will only be suitable as spare parts in the EU from the end of 2027. The magic word is **"retrofit"**: the product is expanded with a secure memory module with an intelligent controller that is tamper-proof integrated into the product and can meet some of the CRA requirements.

Depending on the design of the product, this extension can be implemented in different ways: by inserting an encrypted SD or microSD card from Swissbit, or by soldering the appropriate Swissbit components onto the circuit board of the affected device.



4. Swissbit ensures easy CRA retrofitting

How does this work exactly? In industrial environments, the main concern is to integrate the required functions such as access protection, data security, software updates, and logging into affected devices (industrial controllers, machines, systems, etc.) via a protected, tamper-proof memory area. For such retrofitting purposes – and, of course, for installation in newly developed CRA-compliant products – Swissbit offers pluggable or solderable memory solutions with integrated security functions. In many cases, Swissbit's secure memory solutions can be integrated into existing products without requiring hardware redesign.

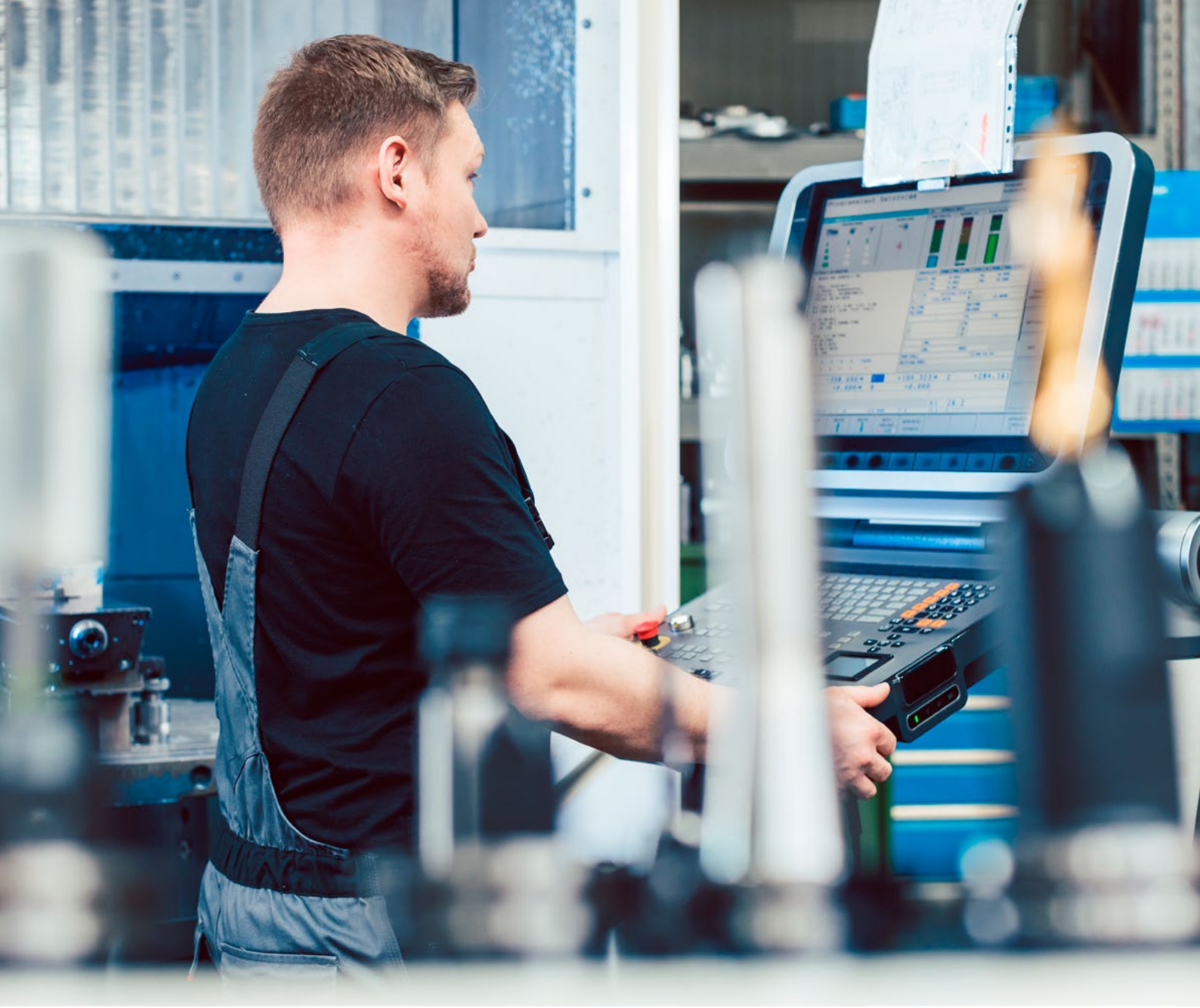
The flash controller, e.g., of a Swissbit SD card, not only checks the quality of the data in the flash memory (error correction). The microcontroller also performs protection tasks during communication between the user or external instance and the system: It requests authentication and authorization from the user via challenge-response, compares the user's identity and access rights with the stored access data, and then grants the appropriate rights, e.g., read-only rights. A cryptographic key storage ensures the secure management of encrypted communication.

In addition, the solution offers additional security levels based on the defense-in-depth principle: The firmware automatically blocks data access in the event of a power interruption, such as a power failure or removal of the card. This ensures that a removed SD card remains reliably protected against unauthorized access. Sensitive data can only be accessed after successful authorization. Secure boot functions can also be retrofitted: By combining all security mechanisms, even the integrity of embedded Linux systems that boot directly from the SD card can be ensured.

CRA requirement	Swissbit solution
Access protection	Access control via PIN, network or hash authentication
Confidentiality of sensitive data	Hidden, encrypted partitions
Integrity of firmware/configurations	Tamper-proof read-only partitions as trust anchors for secure boot
Updateability and protection against manipulation	Partitions are read-only or can be overwritten only with appropriate authorization
Secure deletion of (personal) data	Internal AES encryption and deletion of AES keys ensure that data is securely deleted in the shortest possible time
Key management	Tamper-proof certificate storage and trustworthy hidden, encrypted partitions

A CRA retrofit of industrial devices with Swissbit storage components offers manufacturers several advantages:

- **Existing devices** can continue to be sold in the EU even after December 2027.
- No changes to the circuit board are required for **plug-in solutions.**
- **Solderable components** such as e.MMC can be replaced by PIN-compatible Swissbit e.MMCs.
- **Integration** is via standard interfaces (SD, microSD, USB, e.MMC).
- **Open-source reference code** is available for common platforms (e.g., Raspberry Pi, ESP32, Linux Embedded).
- Swissbit provides **technical documentation** on CRA compliance.



5. Balancing cost-effectiveness and security

Important to know: Not every device has to be "as secure as Fort Knox." The CRA only requires security measures that are appropriate to the risk context, i.e., the "reasonably foreseeable use" of a product. A consumer gadget does not need to be as secure as a machine or system used by a KRITIS operator.

Manufacturers of products that are used in different risk contexts have two options:

1. They can design their products for maximum security across the board and achieve a competitive price structure through economies of scale, if necessary, by deactivating certain high-end security functions via software.

2. They can opt for variant production and differentiate the security functions of the product range according to the intended use and target group.

Swissbit and its partners, with experience in numerous industries, can support manufacturers in CRA projects to avoid over- or under-engineering. The goal is always to find the optimal balance between security and cost-effectiveness.

6. Practical example: How CRA retrofitting of an industrial control system (ICS) works

A fictitious example illustrates the CRA retrofit process: An ICS manufacturer wants to make a tried-and-tested product line CRA-compliant. An internal assessment reveals that the hardware platform used does not offer any intrinsic capabilities for encrypting data and verifying the authenticity of the operating system. The manufacturer is therefore now looking for possible solutions. On the Swissbit website, it finds a partner with the relevant industry expertise.

First, the partner conducts a risk analysis together with the manufacturer. They examine the ICS with regard to the protection goals of integrity, confidentiality, availability, and authenticity. They check aspects such as firmware, configuration files, network access (VPN, WLAN), certificates, etc. The analysis reveals that the ICS stores WLAN access data on unprotected flash memory; in addition, the firmware can be manipulated because it is stored on unprotected e.MMC memory.

The partner therefore recommends retrofitting with Swissbit components. The following solutions are available:

- **PS-66u DP/PE or Security Level 2/3 (SD and microSD):** if the industrial controller uses pluggable memory

- **PU-50n PE (USB):** if additional authenticity or a secure element is required

- **e.MMC PE** (currently still in development): for solderable main memory

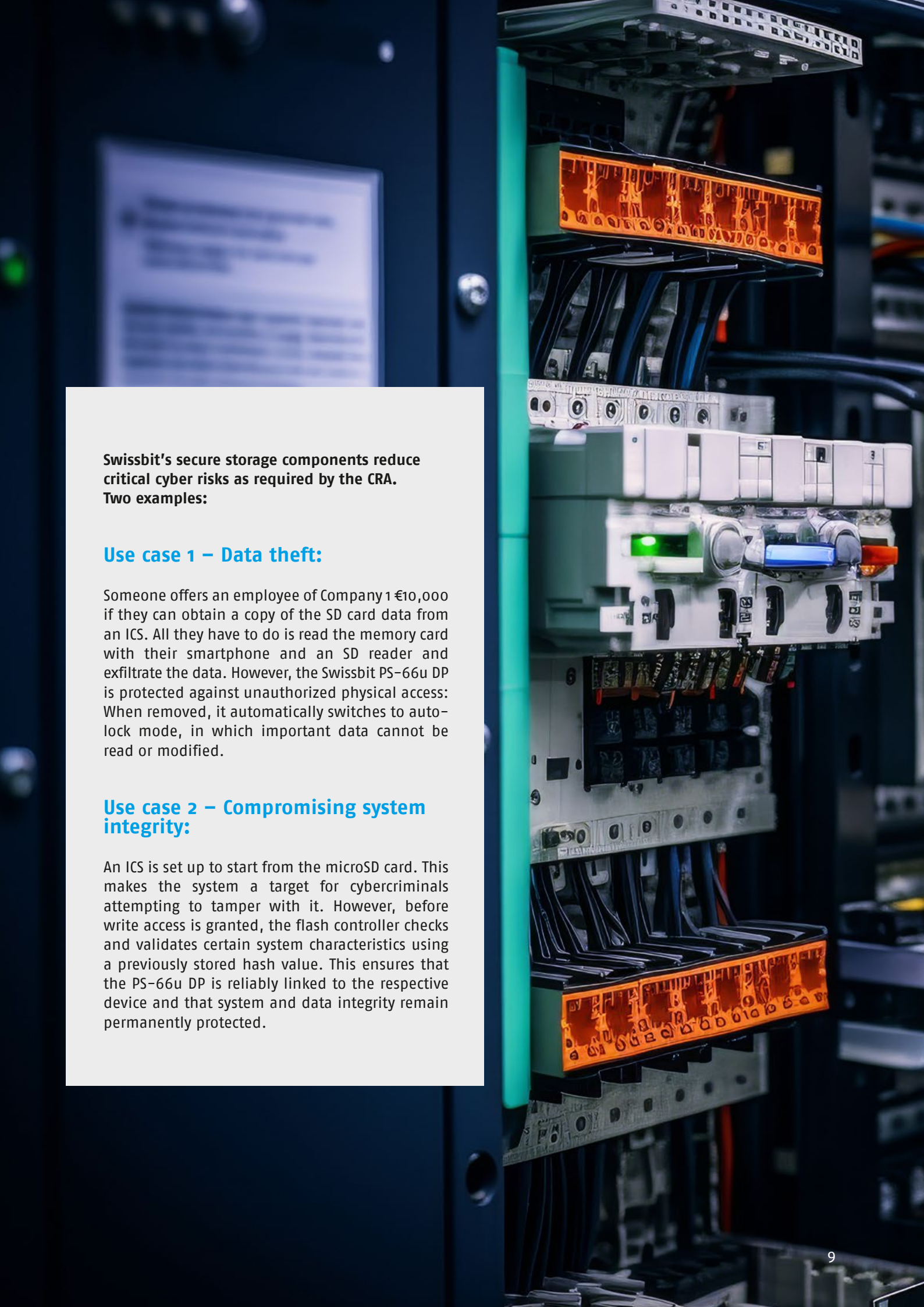
The manufacturer's ICS product line uses microSD cards. Therefore, he decides on PS-66u DP. These secure microSD cards store credentials and certificates in encrypted areas. The Swissbit partner configures protected partitions to suit the respective application so that they are operated in private or read-only mode by default. They only become visible and writable after successful authentication by the legitimate system.

The trustworthiness of the system is verified via read-only partitions for the bootloader and individual system features (HASH policy). The microSD card only grants access to further data (RootFS, applications, access data partition) if it is trusted.

For administration purposes, the manufacturer's IT team sets up the Swissbit Device Manager on a Linux system. With this tool, each card only needs to be configured and activated once. The ICS is now protected against manipulation, data loss, and misuse as required by the CRA and can be updated from a central location.

The partner then creates the CRA compliance documentation for the manufacturer. This includes a description of the protection mechanisms used (partitioning, access protection, secure boot, read-only partitions for critical data, fast data deletion when the ICS is taken out of service) as well as a mapping of the functions to the CRA requirements (CRA Annex I).

The existing gaps in the ICS in terms of compliance with important CRA requirements were thus closed by replacing the memory component and making minor software adjustments – with documented security and without costly redesign of the entire system. Finally, the Swissbit partner performs a security check and functional tests. In the case of risk class II products or critical products, it also provides support in communicating with the relevant notified body.



Swissbit's secure storage components reduce critical cyber risks as required by the CRA. Two examples:

Use case 1 – Data theft:

Someone offers an employee of Company 1 €10,000 if they can obtain a copy of the SD card data from an ICS. All they have to do is read the memory card with their smartphone and an SD reader and exfiltrate the data. However, the Swissbit PS-66u DP is protected against unauthorized physical access: When removed, it automatically switches to auto-lock mode, in which important data cannot be read or modified.

Use case 2 – Compromising system integrity:

An ICS is set up to start from the microSD card. This makes the system a target for cybercriminals attempting to tamper with it. However, before write access is granted, the flash controller checks and validates certain system characteristics using a previously stored hash value. This ensures that the PS-66u DP is reliably linked to the respective device and that system and data integrity remain permanently protected.

Important questions on the path to CRA compliance

If a manufacturer wants to retrofit industrial equipment to make it CRA-compliant, there are a few important questions that need to be answered. It is important to note that the following list is not a checklist along the lines of "We have worked through these ten points, so we are CRA-compliant." Rather, it is a series of fundamental issues that need to be addressed. Depending on the manufacturer and product type, there are certainly other questions that need to be clarified. Product management should consult with a specialist lawyer and/or the company's legal advisor. After all, the CRA is a legal act – and from a legal perspective, the world often looks very different. However, the following questions should provide a good basis for a discussion about CRA compliance:

1. **Inventory and classification:** Have all affected devices been identified, including (embedded) software and software components, firmware versions, communication interfaces, etc.? Is there a software bill of materials (SBOM) to make the software components and their dependencies transparent?

2. **Risk assessment:** Has a risk analysis been carried out using established methods such as DREAD or STRIDE analysis to identify risks and vulnerabilities as well as their potential impact on the security and resilience of the product? Was the ISO/IEC 27005 standard, which covers principles and guidelines for risk analysis and risk management, considered?

3. **Comparison of actual and target status with the CRA:** Is there a comparison of the actual status based on the risk analysis with the CRA requirements that shows in which areas existing products do not meet the EU requirements in accordance with Annex I of the CRA?

4. **Vulnerability management:** Is there a continuous process in place for identifying, assessing, and remedying vulnerabilities regarding CRA compliance, including CVE (Common Vulnerabilities and Exposures) monitoring, a vulnerability database, patch management, and incident response processes?

5. **Establishment of software updates:** Is there a process for software updates and a mechanism for cryptographically secured updates to ensure the required software updates, including security patches, throughout the product lifecycle?

6. **Authentication and access control:** Is there a role model for access rights and device access protection using identity and access management with strong authentication (e.g., password, token, biometrics), as required to protect against unauthorized access to device configuration and control?

7. **Monitoring and logging:** Are there audit logs and logging interfaces (APIs) to record, log, and centrally bundle security-related events?

8. **Technical documentation:** Is the necessary technical documentation available to prove CRA compliance, which affected manufacturers must provide according to the CRA? Are we considered a manufacturer from a segment with increased risk and therefore also required to establish processes for cooperation with competent authorities or notified bodies?

9. **Security communication and reporting:** Are we able to provide the competent supervisory authority with an initial report within 24 hours and an incident report within 72 hours in the event of a security incident? Have we established appropriate responsibilities and workflows for this? Have we also considered the processes for communicating with customers, in particular in the context of supply chain reporting obligations under NIS 2?

10. **Information, training, support:** Are there sufficient opportunities to inform all parties involved – employees as well as partners and customers – about CRA-relevant changes? Have we updated the relevant operating instructions, warranty documents, support contracts, training courses, and marketing and PR materials?

Most of these points are organizational in nature. However, by retrofitting existing products, items 5 to 7 can also be implemented on the device side – with support from Swissbit and its partners.

7. Conclusion: Retrofits prevent premature end-of-life for proven products

The EU's Cyber Resilience Act makes system and data protection essential for all products with digital components. However, many existing products – not least in industrial – do not currently meet the CRA requirements. One possible approach would be to discontinue the product by 2027 and replace it with a new development. However, this is time-consuming and cost-intensive. In addition, suppliers in the industrial sector in particular need to act quickly, as discontinuations often require one to two years' notice.

A practical alternative is therefore to retrofit existing products with secure Swissbit memory components for CRA compliance. A retrofit saves time, effort, and costs. It extends the life cycle of proven products without requiring a fundamental redesign.

Swissbit, with its secure storage solutions made in Germany and its partners with industry expertise, is happy to assist with CRA retrofit projects. Manufacturers should not waste any time, as their customers are also aware of the CRA requirements and deadlines. A faster CRA retrofit ensures consistent cybersecurity, legal compliance, and improved marketability.

8. The next steps

Here you will find further information on the following CRA aspects:

Swissbit's security partner: https://community.swissbit.com/c/security-partners

Swissbit solution – Security Upgrade Kit: https://www.swissbit.com/security-upgrade-kit

Retrofit solutions with secure storage mechanism: https://community.swissbit.com/c/security-functions/secure-storage-mechanism

Integrity protection via retrofit: https://community.swissbit.com/c/security-functions/integrity-protection

You can find a chatbot that you can ask about Swissbit's CRA solutions at www.swissbit.com/cra-swissbot-beta (OpenAI account required)

Feel free to contact us at roland.marx@swissbit.com to learn more about CRA retrofits with Swissbit technology, for example in an individual webinar.

Sources:

[1] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

[3] https://vdma.org/viewer/-/v2article/render/91012176

[4] https://www.vde.com/tic-de/news/2024/cybersecurity-wird-voraussetzung-fuer-ce-kennzeichnung

swissbit®

Author

Roland Marx
Senior Product Manager Embedded IoT Solutions

Have questions? Get in touch:

Swissbit Europe (HQ)
Tel. +41 71 913 03 00
sales@swissbit.com

Swissbit North America
Tel. +1 978-490-3252
salesna@swissbit.com

Swissbit Japan
Tel. +81 3 6258 0521
sales-japan@swissbit.com

Swissbit Asia
Tel. +886 912 059 197
salesasia@swissbit.com

About Swissbit

Swissbit AG is the leading European technology company for data storage and security solutions. Our vision is to build a connected world where data and identities are trusted, ensuring digital sovereignty.

Founded in 2001, Swissbit operates offices in Switzerland (HQ), Germany, the USA, Japan, and Taiwan, and maintains its own semiconductor production facility in Berlin, Germany.

www.swissbit.com