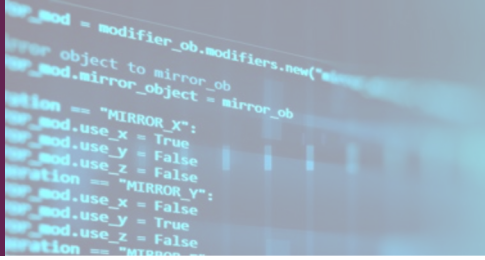
ICENI™: your companion to European Cyber Resilience Act (CRA) compliance

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: your companion to European Cyber Resilience Act (CRA) compliance



INTRODUCTION

ICENI, the world's most secure MCU for securing against memory safety exploits, is a device family of 32-bit highly secure microcontrollers, delivering hardware-enforced memory safety and robust isolation of software at the edge.

ICENI is **secure by design**, eliminating entire classes of vulnerabilities through hardware-enforced memory safety. **It brings simplicity**, being tailored for low-power embedded applications and offering pin-compatibility with legacy MCUs to ensure seamless migration to memory-safe computing. At the same time, **ICENI delivers performance without compromise**, providing real-time responsiveness and deterministic execution.

CYBER RESILIANCE ACT

In today's digital and interconnected world, large scale cyber attacks are becoming a regular occurrence. For several years the European Commission has been working on a standards document and associated regulation and has finally published a comprehensive set of cybersecurity requirements in its most recent **Cyber Resilience Act (CRA)**. This act applies to all products with a digital element sold in the European Union and entered into effect in December of 2024 with full compliance required by end of 2027.

The CRA first and foremost approaches cybersecurity with a new design philosophy. It requires product manufacturers to start with a risk assessment and to then produce product solutions that are both digitally **secure by design** and **secure by default**. This requires performing an initial threat analysis and then designing the product in a way that will effectively address these threats. This ensures a) **security is built in** from inception (and not an afterthought), and b) that the product is securely initialized and boots up with a default configuration that can also be considered secure - there are no loose ends, open doors, test keys or default passwords of any kind.

The World's Most Secure Microcontroller

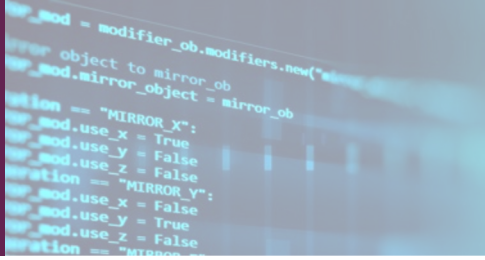
- Digital Security by Design
- 100% Memory Safety
- Hardware Compartmentalisation
- Fearless Code Reuse
- Scalable Device Roadmap

In partnership with Microsoft Google

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: your companion to European Cyber Resilience Act (CRA) compliance



The CRA offers a list of product security requirements that guide manufacturers in the way they can design secure products. As a matter of principle, the design of the product must ensure that all risk is minimized. Key tasks are to **minimize access** to data for those who don't need to know, **minimize privileges** for those who don't need to be authorized, **minimize exposure** by minimizing the attack surface, and finally, if something were to happen despite all built-in protections and security barriers, **minimize the impact** of the incident. These are extremely sound design principles and suggest a pivoting in the way we think about architecting products.

The remainder of the product security requirements are really meant to help put in place security building blocks that have proven effective in the past. Think along the lines of using cryptography to **protect secure communications; confidentiality and integrity** of the data being communicated; authenticity of the sender/receiver, and origin of the data. This involves access control to the data and a strict management of access privileges with individual rights and credentials.

Next comes system integrity with a way to securely boot the product and start in a configuration that is **secure by default**. At each stage of the product's lifecycle, it must remain protected against unwanted changes in the software and firmware, with a secure way to update or upgrade the software if necessary and ensure that there is no way that a malicious entity can inject any harmful code or compromise the secrecy of the memory of the system. Protecting the system against privilege escalation attacks and data leakage is paramount.

Critical National Infrastructure

Industrial Automation

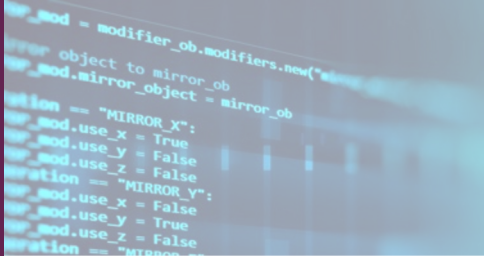
Aerospace

Automotive

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: your companion to European Cyber Resilience Act (CRA) compliance



Once the product is designed securely, consideration should be made for what would happen in event that it is still successfully attacked. Consider **resilience** and how to recover from an incident. Implement strategies to recover from potential damage and disruption. Don't let a single point of failure be the end of it all; design a graceful way to recover from crashes or security incidents; don't accept a degradation of service, and guarantee a minimal set of functionality, even under threat. Don't let the product become the base for large scale attacks, don't let malware propagate or distribute itself using the product. Limit the impact.

Furthermore, apply rigorous and responsible processes for new vulnerability disclosures and handling, such as systematic and timely reporting to control agencies (required from September of 2026), secure distribution of corresponding software security updates, dissemination of information and security patches to the ecosystem.

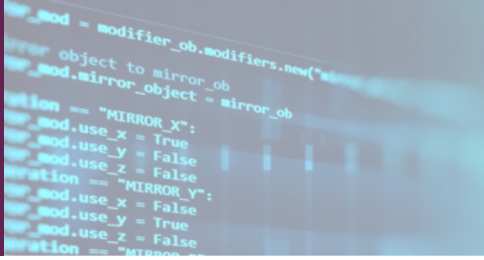
Looking at these requirements, this all seems sound and reasonable, but how do we go about approaching digital security by design?

There is a simple and elegant way to get a significant head start and simplify the complexity of the requirements by using a technology called **CHERI**/CHERIoT (Capability Hardware Enhanced RISC Instructions – for IoT). This technology allows a designer to avoid a large-scale take-over of the system to do harm by limiting the impact of what software can do; by isolating pieces of code into compartments and only allowing these compartments to safely share data when they wish. By using the CHERI **memory safety** security methodology, it becomes impossible to exploit memory corruption vulnerabilities (such as buffer overflows, use-after-free memory misuse or corrupted pointer allocation), impossible to elevate privileges if one compartment is compromised, and impossible to take over the system and leak data or spread the threat more broadly.

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: your companion to European Cyber Resilience Act (CRA) compliance



Cryptographic techniques and access control management can now safely be deployed on top of CHERI technology and are no longer at risk of being compromised. Keys and secrets remain securely protected within safeboxes and can only be used the way they were intended to. The whole design approach is based on the least privilege principle and data is only shared safely between compartments when needed and when it is appropriate to do so. Each compartment is like an individual sandbox.

Using the CHERI technology toolchain also provides access to built-in software **auditing** tools which can help identify and document existing and zero-day vulnerabilities in third party code as well as your own. This helps to massively reduce the attack surface. These same auditing tools open the way to an even more advanced security posture: they allow logical reasoning about the worst-case behaviour of such vulnerabilities in a dependency (such as third-party open-source code).

Significantly, with this level of protection, one can argue that security patches are no longer required and, that in the not-so-distant future, having to ship security updates due to vulnerabilities discovered in third party code will be a thing of the past.

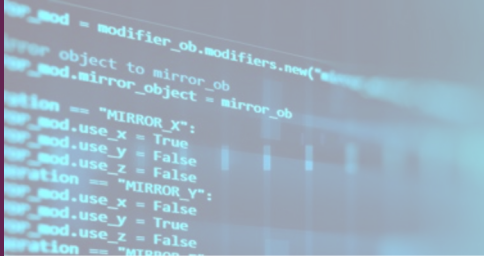
CHERI is readily available in **ICENI** devices, which have been designed and architected with exactly the CRA requirements in mind. They support the use of TLS and TCP/IP protocols and let you create safeboxes to securely manage keys and certificates. ICENI devices have been designed with the **least privilege principle** in mind and support any access control application of your choice. The devices offer **secure boot** and **secure initial configuration**, and they **enforce** bounds and permissions on memory accesses that **protect** against the effects of rogue software. ICENI is architected to limit the blast radius of any malicious piece of code to a single compartment and to recover gracefully because only that compartment will crash. It cannot serve as a basis to attack other devices or further distribute malware to a botnet.

Visit www.scisemi.com to discover more about the groundbreaking ICENI devices - **the world's most secure microcontrollers**.

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: your companion to European Cyber Resilience Act (CRA) compliance

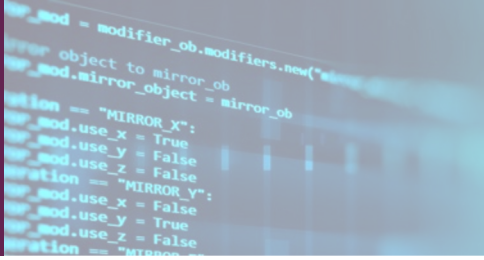


CRA Requirements - Part I	ICENI devices with CHERIoT Technology / Toolchain
(1)Risk Assessment Security By Design	ICENI is based on CHERIoT technology which allows product manufacturers to compile their applications in a secure compartmentalized way, utilising the principle of Least Privilege. Secure by Design is the essential and fundamental design principle of CHERI-enabled hardware.
(2)(a) Absence of known exploitable vulnerabilities	CHERI technology has been assessed by expert security teams at well-known universities; it has no known vulnerabilities at this time. Products based on this technology benefit from code and application isolation and permissions management for memory accesses; even zero-day vulnerabilities identified in the product software cannot be exploited because they are self-contained in specific compartments with no rights/permissions to access or contaminate anything else. Software Auditing tools help ensure that software (including third party open-source software) does not contain any known exploitable vulnerabilities. They make sure any known/new vulnerability becomes unexploitable.
(2)(b) Secure by default initial configuration	ICENI enables the implementation of a secure boot process which initialise a product in a secure configuration. Only the verified trusted code base can be used to start up the boot process which implements a security environment where the product application is protected.
(2)(c) Security updates	Security updates can be performed when vulnerabilities are identified in specific compartments; however, those compartments do not put any other part of the system at risk.
(2)(d) Managed and Secure Access Control	ICENI devices have permissions checking built into the hardware ISA; the CPU checks that memory accesses can only be performed by the correct entity and to the correct addresses within given bounds and with specific read/write/execute permissions. The product application can utilize these capabilities to manage access control and secure sharing of data based on identity and relevant credentials.
(2)(e) Data confidentiality	Data at rest and in transit within the application can be encrypted and keys securely stored in safeboxes to which only the legitimate owner has access.
(2)(f) Data Integrity	Data at rest and in transit within the application can be authenticated and signed, or integrity protected by cryptographic means using keys securely stored in safeboxes to which only the legitimate owner has access.
(2)(g) Mimimized data access	This is an essential pilar of ICENI technology; minimizing access to data and strictly managing permissions to read, write and execute any address in memory is the fundamental concept behind CHERI-enabled hardware.
(2)(h) Availability and resilience to attacks	ICENI protects applications against denial-of-service attacks by confining software within compartments such that any incident will remain contained and rogue code is unable to contaminate or expose other compartments or keys/data within the application.

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: your companion to European Cyber Resilience Act (CRA) compliance



CRA Requirements - Part II	ICENI devices with CHERIoT Technology/Toolchain
(1) Identify and document vulnerabilities and components in an SBOM	Software Auditing tools can help to ensure that third party code (including third party open-source software) does not contain any known exploitable vulnerabilities. It also helps identify new and existing such vulnerabilities.
(2) Remediate vulnerabilities without delay (SW updates)	Vulnerabilities in third party software components are no longer a concern. They are rendered harmless.
(3) Regular Product Security Testing	Software Auditing tools can help identify known and zero-day vulnerabilities in third party code and open-source software.
(7) Securely distribute and automate security updates	Vulnerabilities in third party software components no longer a concern. They are rendered harmless.
(8) Disseminate security updates without delay and free of charge	Vulnerabilities in third party software components no longer a concern. They are rendered harmless.

CHERI OVERVIEW

CHERI (Capability Hardware Enhanced RISC Instructions) technology integrates security **directly** into hardware design, providing a robust foundation for digital systems. By **eliminating** memory safety vulnerabilities and enabling stronger **compartmentalization**, CHERI significantly reduces cyber risks and enhances system resilience. This built-in security empowers businesses to adopt digital technologies with confidence, unlocking greater **productivity** and **efficiency** across the economy.

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI

The World's Most Secure MCU

PRODUCT OVERVIEW

ICENI, the world's most secure MCU for securing against memory safety exploits, is a device family of 32-bit highly secure microcontrollers, delivering hardware-enforced memory safety and robust isolation of software at the edge.

ICENI is **secure by design**, eliminating entire classes of vulnerabilities through hardware-enforced memory safety. **It brings simplicity**, being tailored for low-power embedded applications to ensure seamless migration to memory-safe computing. At the same time, **ICENI delivers performance without compromise**, providing real-time responsiveness and deterministic execution.

KEY FEATURES

Robust Security – Hardware-level CHERI-enabled security against cyber threats.

Advanced Performance – Optimized processing architecture with high throughput and low latency.

Energy Efficiency – Low-power design ensures reduced operational costs and improved sustainability.

Scalability – Modular platform for entry-level to enterprise-scale deployments.

Interoperability – Standards-based design for seamless integration.

Future-Proof Design – Ready for AI, ML, and data-intensive analytics.

APPLICATIONS

ICENI delivers the **performance** and **reliability** demanded by critical systems. Its robust, real-time architecture ensures **seamless** operation, even under the toughest conditions.

- **Secure** and fault-tolerant for uninterrupted uptime
- **Deterministic** and **responsive** for maximum efficiency
- **Proven**, **compliant**, and **scalable** for mission-critical use

Secure. Resilient. Uncompromising

SCI Semiconductor