ICENI™: The Silicon Answer to the EU Cyber Resilience Act (CRA)

ARCHITECTURE OF TRUST. HARD-CODED IN SILICON.

Secure Your EU Market Access.
Future-Proof Your Innovation.

Secure. Resilient.
Uncompromising

SCI Semiconductor

ICENI: The Silicon Answer to the EU Cyber Resilience Act (CRA)

Introduction

ICENI is a device family of **32-bit highly secure microcontrollers**, delivering hardware-enforced memory safety and robust isolation of software at the edge. By moving the legal and technical burden of security directly into the silicon gates, we help you future-proof your innovation and secure your access to the European market.

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

The CRA: Why Your Product Must Evolve

The Cyber Resilience Act (Regulation 2024/2847) is a mandatory set of rules for any "product with digital elements" for sale on the EU market.

If your product connects to a network or handles data, compliance is no longer optional, it is your "License to Operate."

What Makes Your Product Subject to the CRA?

- ✓ Digital Presence: Your device uses integrated hardware or software, including remote data processing.
- ✓ EU Market Access: Your products are distributed, leased, or used within the European Union.
- ✓ Active Connectivity: Your system exchanges data via wireless (e.g. WiFi/BT) or physical (e.g. USB/Serial) interfaces.

A New Design Philosophy

The CRA shifts cybersecurity from a reactive patch to a proactive foundation. Manufacturers must start with a risk assessment and produce solutions that are secure from the ground up. This ensures:

- Security from Inception: Protection is a core component, not an afterthought.
- Secure by Default: Products boot up in a secure configuration with no "open doors," test keys, or default passwords.

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: The Silicon Answer to the EU Cyber Resilience Act (CRA)

The Compliance Clock is Ticking

11 September 2026 Mandatory Reporting.

Manufacturers must report any actively exploited vulnerability to ENISA within 24 hours. This applies to all products currently on the EU market.

11 December 2027 Full Enforcement.

Every new unit placed on the EU market must be fully CRA-certified.

The Innovation Insurance

The CRA includes a Substantial Modification clause that acts as a reset button on compliance.

- Any significant upgrade after 2027, software or hardware, triggers a mandatory re-certification to the latest standards.
- If your current chip lacks hardware-enforced isolation, you may be blocked from pushing new features because the hardware cannot pass a modern security audit.

Future-Proofing Your Investment

By choosing ICENI now, you are buying architectural insurance. Our hardware-enforced boundaries mean that even as your software evolves and new threats emerge, your core security model remains as robust and resilient as ever. This eliminates the need for expensive, repetitive manual audits and protects your product's long-term market access.

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: The Silicon Answer to the EU Cyber Resilience Act (CRA)

The Open Source Trap

WHY YOUR SUPPLY CHAIN IS YOUR BIGGEST LIABILITY

Most modern products are built on a foundation of third-party and open-source software (OSS). Under the CRA, the legal relationship with this code has fundamentally inverted.

- **The Responsibility Shift:** While pure open-source projects are exempt, if you monetize a product in the EU, you are 100% responsible for the security of every integrated component, even code you didn't write [CRA Art. 10].
- **The Maintenance Burden:** You are required to provide security patches for third-party flaws. If an integrated library is abandoned, the burden of remediation falls entirely on you.

THE ICENI SOLUTION

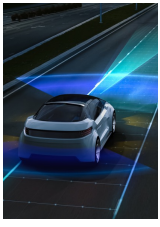
While faulty code must eventually be patched, **ICENI** fundamentally changes the stakes of a breach. By using **Hardware-Enforced Compartmentalisation**, we ensure that a flaw in an open-source library does not escalate into a reportable severe incident.

- **De-escalating the Crisis:** If a vulnerability in an integrated library is exploited, the attacker is physically trapped in a hardware "bubble." They cannot reach your core control logic or sensitive user data.
- **Regulatory Relief:** By preventing the exploit from affecting critical functions, ICENI helps you avoid the "Severe Incident" reporting track, keeping your brand out of the headlines while you develop a patch.

Critical National Infrastructure

Industrial Automation

Aerospace

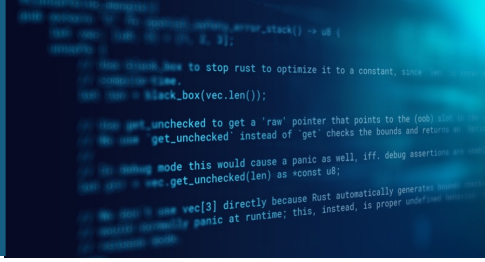


Automotive

Secure. Resilient. Uncompromising

SCI Semiconductor

ICENI: The Silicon Answer to the EU Cyber Resilience Act (CRA)



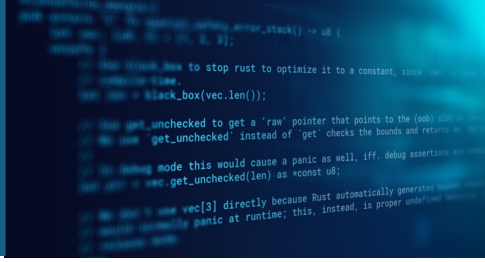
Architectural Resilience

The EU Cyber Resilience Act has fundamentally redefined "State-of-the-Art" for the embedded industry. Compliance is no longer a software patch away—it is an architectural mandate. While legacy security standards were designed for an era of physical theft and lab-based tampering, the CRA targets the modern reality of remote, network-based exploits and supply chain vulnerabilities.

To meet the CRA's "Secure by Design" requirement (Annex I), manufacturers must prove their hardware can withstand memory corruption and provide meaningful isolation for third-party code. ICENI replaces fragile software perimeters with Architectural Certainty, moving the legal and technical burden of security directly into the silicon gates.

The CRA Compliance Risk	Legacy MCU	The ICENI (CHERIoT) Advantage
Protecting the Attack Surface (Annex I, 1.1)	**Focus: Physical Access.** Unable to address remote network-based entry points.	**Focus: Remote Software Exploits.** Specifically neutralises "No-Touch" network attacks.
Duty of "Least Privilege" (Annex I, 1.3)	**Coarse Trust:** With a TEE solution a breach in one driver can expose all secrets.	**Micro-Segmentation:** Zero-Trust at silicon level. Every library is physically locked in its own compartment.
Mitigating Memory Risks (Annex I, 1.1)	**Software-Dependent:** Relies on MPU configured by code. Pointer corruption can bypass security.	**Hardware-Enforced:** Memory safety built into silicon. Pointers are "Capabilities" that cannot be forged.
Supply Chain (OSS) Liability	**High Liability:** Software boundaries are fragile. OSS bugs easily leak into core logic.	**Native Sanctuary:** Runs unverified code in "Hardware Bubbles." 3rd-party bugs cannot escalate.
The Burden of Proof	**Manual & Costly:** Requires manual code audits redone with every software patch.	**Deterministic & Automated:** CHERIoT Audit toolchain guarantees desired security policies are met

ICENI: The Silicon Answer to the EU Cyber Resilience Act (CRA)



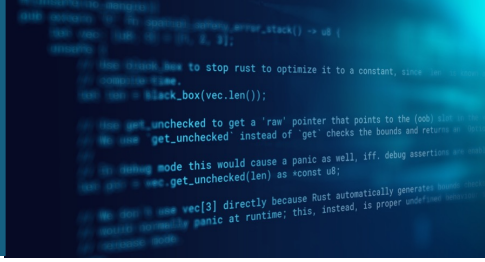
Roadmap to Compliance

HOW ICENI GETS YOU THERE

The following table outlines how ICENI hardware and tools simplify the essential steps for compliance.

Essential Requirement (Annex I)	ICENI Hardware & Toolchain Solution	Handled by Your Company
(1) Risk Assessment	✅ **Deterministic Risk Analysis:** The **CHERIoT-Audit tool** allows you to logically reason about the worst-case behaviour of vulnerabilities in dependencies.	Define application threat model.
Security by Design	✅ **Hardware-Level Integrity:** Security is integrated directly into hardware via **CHERI technology**, eliminating entire classes of vulnerabilities from inception.	Document secure design lifecycle.
(2)(a) Absence of exploitable vulnerabilities	✅ **Silicon-Enforced Safety:** Renders memory safety exploits harmless at the silicon level.	Maintain disclosure & patch programmes.
(2)(b) Secure by default configuration	✅ **Hardware-Verified Boot:** Ensures only verified trusted code bases can initialise the system.	Secure management of keys.
(2)(g) Minimised data access (Least Privilege)	✅ **Capability-Based Silicon:** Enforces "Least Privilege" in hardware. Components are only granted permissions and memory bounds they strictly require.	Define data access policies.
(2)(h) Resilience to attacks & impact mitigation	✅ **Blast Radius Containment:** Compartmentalisation isolates code. If a component is breached, the attacker is physically trapped.	Execute 24h reporting to ENISA.
Article 14: Reporting	✅🔄 **Automated Incident Analysis:** The toolchain helps understand the impact any potential breach would have and prove it remains contained.	Manage legal communication strategy. Submit 24-hour vulnerability reports to ENISA/CSIRT when an active exploit is identified.
Annex I, Part II (1) SBOM Documentation	✅🔄 **Automated Supply Chain Visibility:** The toolchain identifies and documents all software components and their possible interactions, including 3rd-party OSS.	Maintain official SBOM asset tracking.

ICENI: The Silicon Answer to the EU Cyber Resilience Act (CRA)



The Real Cost of Security Failure

Security isn't just a regulatory checkbox; it's a fundamental requirement for operational safety. Legacy microcontrollers (MCUs) rely on software boundaries that are easily bypassed once a single vulnerability is found. ICENI replaces these "hopes" with hardware-enforced guarantees.

INDUSTRY	REAL-WORLD FAILURE	THE LEGACY MCU FAILURE	THE ICENI SOLUTION
SMART FACTORY	**Triton / Trisis Malware** (2017): Targeted safety shut-offs in a petrochemical plant.	**Code Injection:** Malware injected code into memory because the space was writable and executable.	**Immutable Code Guard:** Hardware enforces strict Write XOR Execute policies; malicious code cannot be injected.
ENERGY	**Viasat "AcidRain" Attack** (2022): Malicious commands "bricked" 5,800 wind turbines instantly.	**Blind Trust:** Modems accepted commands simply because they came from a "trusted" server.	**Least Privilege Update:** The update agent runs in a sandbox, lacking the hardware capability to overwrite the bootloader.
MEDICAL	**Medtronic Insulin Pump** (2019): FDA recall due to hackers wirelessly hijacking motor controls.	**Perimeter Breach:** Once the wireless link was breached, the attacker had total control of the motor.	**Fine-Grained Compartments:** The wireless stack is isolated; a hacker cannot "break out" to reach the motor control.
AUTOMOTIVE	**The Jeep Cherokee Hack** (2015): Hackers killed brakes/steering remotely via the radio.	**Lateral Movement:** The chip relied on software firewalls. Once the radio was hacked, it had "root" access.	**Hardware Quarantine:** Infotainment is strictly isolated with no physical permission to touch braking.

ICENI

Hardware-Enforced Integrity.

ICENI enforces security through architectural law, not software hygiene. By validating pointer integrity at the hardware level, we do not just reduce risk — we remove the possibility of memory corruption.

Compromised code is instantly contained. Privilege escalation is impossible.

SCI Semiconductor

SCI Semiconductor specialises in secure, high-assurance hardware solutions for mission-critical applications. We help governments, defence partners, and commercial enterprises safeguard sensitive information and critical infrastructure by delivering solutions that strengthen cybersecurity from the silicon up, while enabling long-term trust and operational resilience.

Secure. Resilient.
Uncompromising

SCI Semiconductor