SCI Semiconductor

Memory Safe Compute For Regulated Industries

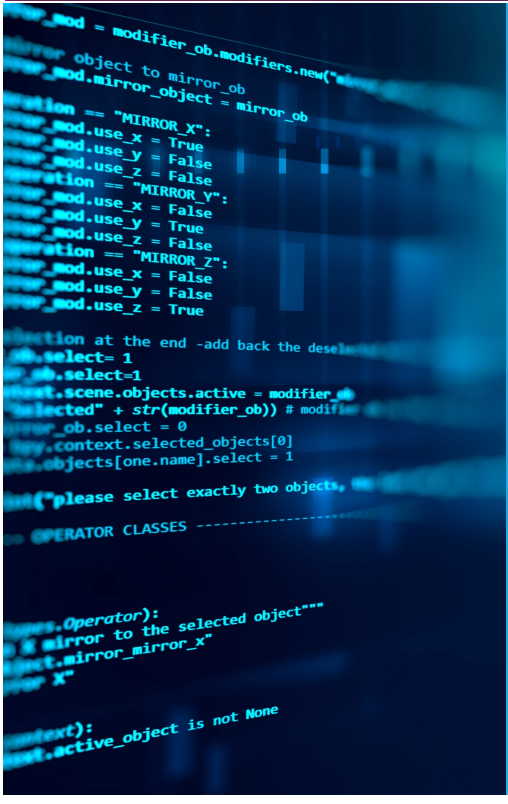
Delivering memory safe solutions with ICENI™

Learn how CHERIoT RISC-V technology can support Regulated Industry applications to reduce CVEs by 70⁺%

What Is Memory Safety?

Memory safety is a property of computer systems that ensures programs only access memory locations they are permitted too, preventing unintended or malicious behaviour.

- ✓ **Security**: Majority of critical software vulnerabilities stem from memory safety violations.
- ✓ **Reliability**: Memory errors often lead to program crashes or unpredictable behaviour.
- ✓ **Maintainability**: Ensure memory safety makes debugging easier & reduces technical debt
- ✓ **Compliance**: Many industries require memory-safe programming to meet regulatory standards.



Traditional Memory Safe Challenges

Unpredictability

Memory safety bugs let one part of a program modify a completely unrelated part of the program's state. Exact effects of this depend on what the program has done, will do, or is doing. They may be unexploitable in one version, but an unrelated change may allow an attacker to gain arbitrary-code execution in the next.

Buffer Overflow

Writing past the allocated memory bounds may leak secrets, such as Heartbleed

Use-After-Free/Dangling Pointer

Using a pointer after its memory has been deallocated leads to crashes, leaks or arbitrary code execution.

Uninitialized Memory Access

Using memory before setting a valid value will likely cause undefined behavior

ICENI™ CHERIoT RISC-V

With SCI ICENI™ devices, based on integrated CHERIoT foundations, it is now possible for memory safe security to transform into a business benefit, creating significant value along the supply chain, for developers, integrators and end users.

1 Software Supply Chain

Fearless code reuse is enabled through robust fine-grained isolation, significantly lowering software development cycles and accelerating time to market

Limiting the "blast radius" of any attack, providing an application "run-flat tyre"

Maintain system availability by automatically restarting compartments

2 Cost Efficiency

Code reuse by simple recompilation without lengthy code re-writing to support custom TEE's

Simple and low-cost development reducing the need for specialist skill sets

No endless code patching required - reducing the cost of the upgrade treadmill

3 Enterprise Mission Critical Focus

Enhanced integrity ensures exploits are trapped before data can be corrupted

Improved availability ensures system stability isn't impacted by compartment crashes

Fine-granularity compartmentalization supports rapid & reliable restarts after attack detected

4 Application Security

Multi-stage secure boot enables progressively reduced privileges for each stage, minimising the attack surface, and reducing costs

Compartmentalisation ensures that compromised function cannot expose other software to attackers

CVEs in third-party components are isolated within the system

5 Legislation & Regulation

Delivering standard hardware-enforced framework reduces the cost of legislation

Reduced application specific security requirements low costs and simplifies solutions

Simple purchasing requirement ensure organizations always meet stringent and complex customer demands

Industrial Automation

Secure and manage software risks across cyber physical systems. Integrating Memory Safe technologies, utilizing the ICENI™ platform, instantly reduces threats from misconfiguration and software supply chain .

Considered the #1 risk by many IACS vendors the impact of Memory Safe technology will reduce vulnerabilities, reduce customer challenges and ensure system security over extended lifetimes

Supporting Standards

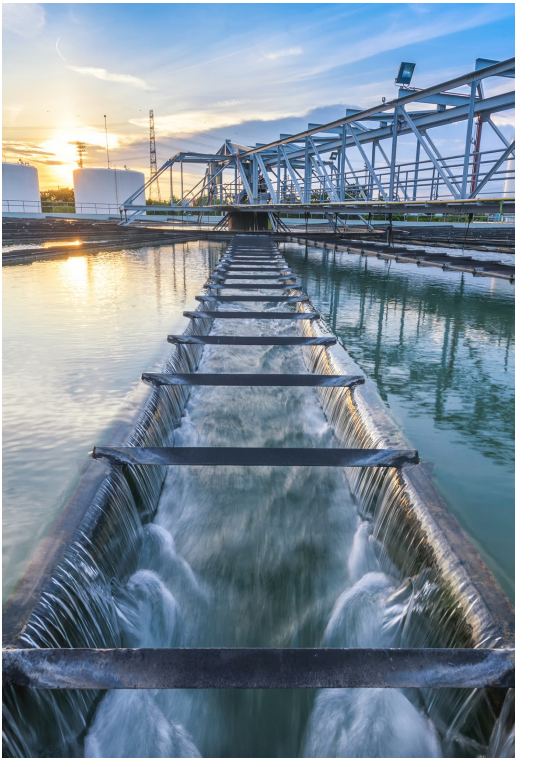
Meeting emerging aggressive regulations and standards including IEC 62443-4 is both challenging and expensive. CHERIoT / CHERI technology substantially reduces the effort whilst increasing availability and integrity.

Critical Infrastructure

Water processing, energy generation & transmission, public transportation systems, and many other systems are often described as the soft underbelly of a nations defense. The critical systems that enable us to go about our everyday lives are often invisible, but critical to supporting a healthy economy.

As we continue to transition to digital control and communications, we become ever more reliant of a bedrock of aging digital control systems, that often host a range of Memory Safe issues, waiting for exploitation.

It is impractical, and too expensive, to remove legacy systems, but by transitioning to ICENI™ with pin compatible devices, a simple code recompile may just save you industry millions by removing attack vectors and securing control and communications.



Automotive Systems

The automotive industry is defined by robust systems, often having undergone years to safety testing. However, as is true of any connected systems the automotive platforms are not immune to Memory Safe failures, creating significant attack surfaces that have been show to impact powertrain and braking systems. The advent of regular OTA updates is an additional challenge, as while these enable rapid deployment of updates and patches, they also enable bad actors to impact the system

Safety & Security

Safety and security are two sides of the same coin, with security being critical to managing safety, and visa versa. However, driver safety remains paramount. The ICENI™ platform is defined to capture security failures without impacting safety, providing auditing, fine-grained control and limiting blast radius of attack vectors.

V2V / V2X

Vehicle to vehicle (V2V), vehicle to infrastructure (V2X), and autonomous vehicles are all critical domains where humans are surrendering control to automated systems, and hence a major challenge for security and safety. The need to ensure platforms remain secure from attack over their entire lifetimes of 20 years, or more, create major technology headaches, and has led to the removal of several platforms from the market.

The CHERI technology underpinning the ICENI™ devices provides both Memory Safety & fine-grained compartmentalization, enabling systems to rapidly reuse code without having to surrender critical safety metrics, ensuring that even if a flaw is identified in the code base that exploits cannot be easily formed into remote attacks.

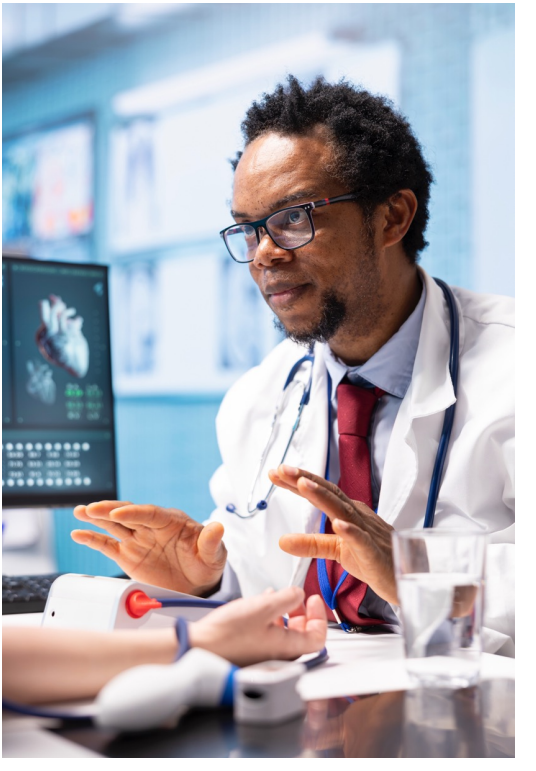
Aerospace

Aerospace and defense applications have driven high integrity and high availability systems for many years, with high grade mission critical systems. The need for “right first time, every time” has, in turn driven improvements in memory safety and system definition, primarily through formal methods, and the definition of high integrity languages, such as Fortran, Cobol, and Ada. The challenge is these languages are specialist and often limited in use, reducing the engineering talent pool v traditional C/C++, creating a significant technical gap. Similarly, the challenges of formal methods, with a focus on crafting complex specifications and engineering to these, leads to a far higher cost base, normally 30x vs traditional methods, and prolonged time to market. CHERI technology resolves these challenges enabling high integrity programs written in C, within nominal timescales.

Medical Applications

Medical applications often require the highest level of safety and security, especially implantation devices which may need to be in place for 20 years or more. As medical science progresses, so does the need to transition from older formal methods” type development, with high costs and many years to market, to a more flexible, faster and ultimately cheaper methodology, while maintaining a strong focus on safety, security, and compliance.

The requirements of standards such as IEC62304 the medical device software standard, covering planning and detailed design, implementation and verification, are well suited to the ICENI™ and CHERIoT memory safe programming flow, with strong isolation between compartments while providing safe sharing of data, enabling more modular and robust, high availability applications



ICENI™ Devices & Development

- Initial SCI ICENI™ devices available 2H25
- FPGA exploration platform available
- LLVM mature compiler and development tools
- CHERIoT RTOS + networking libraries

ICENI™ Family 32-bit CHERIoT RV32I — JTAG

Memory	Analog	Timer	Protection
Code Up to 2MB MRAM SRAM Up to 1MB ECC SRAM 8KB Data MRAM 8KB	12-bit A/D x 10ch Comparator (2ch) Temperature Sensor DAC (2ch) Internal v REF	16-Bit Timer Counter (x8) 32-bit Interval Timer (8-bit, 4ch) Watch Dog Timer Unit Real Time Clock	CHERI Compartmentalisation Capability Memory Safety Security Subsystem* Unique ID MRAM read protection

Communication	System	Safety	HMI / Package
SPI x6 UART x6 Simple I2C x6 USB Host	Capability DMA Integrated System Level Revoker Capability Interrupt Controller Clock Generation Multi On Chip Oscillator Low Power Modes Clock Output PinMux	SRAM Parity Check SRAM ECC Clock Monitor CRC Independent WDT ADC Self-Test Boot swap (startup area select)	HMI: LCD Controller Package: QFN 64, 48, 32, 24 (QFP 64, 48, 32)

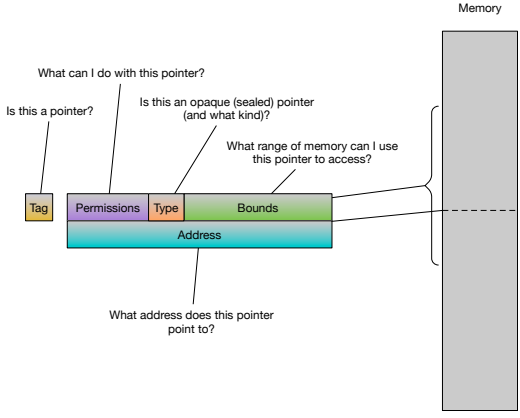
Subject to change

Capabilities

Capabilities are core to the functionality of CHERI, providing a range of critical functions to replace the traditional pointer.

Recompiling uses capabilities to represent every pointer in your system, giving the following security guarantees:

- **Unforgeability**, guaranteed by the tag bit.
- **Precise bounds,** preventing buffer overflows.
- **Revocation** hardware-acceleration**,** preventing use-after-free vulnerabilities.
- **Rich permissions** for secure sharing of language-level objects with other compartments.
- **Sealing** for type-safe opaque types shared with other compartments.



CHERI vs. CHERIoT

CHERI (Capability Hardware Enhanced RISC Instructions) is the foundational new technology for implementing memory safe and compartmentalization. It has been developed in response to the growing cyber attacks, which today are estimated to cost over $10Trillon every year to global GDP. CHERI is an open specification, and implementations have been produced in Arm64, RISC-V 64 bit and other architectures.

CHERIoT is the smallest standard instantiation of the CHERI specification delivering memory safety, fine-grained compartmentalization, and static auditing of applications. It is ideal for a range of low and mid-performance applications, including pin-compatible microcontrollers, delivering real-time performance and low power implementation.

SCI Semiconductor

www.scisemi.com

© SCI Semiconductor 2025