

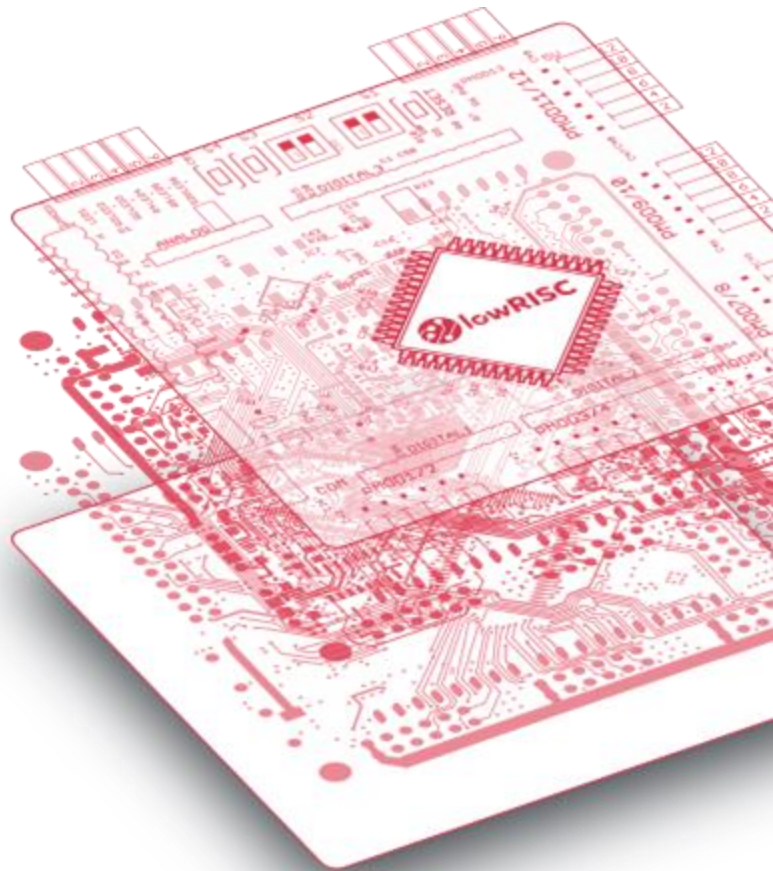


# Sonata™

A platform for high-integrity operational technology

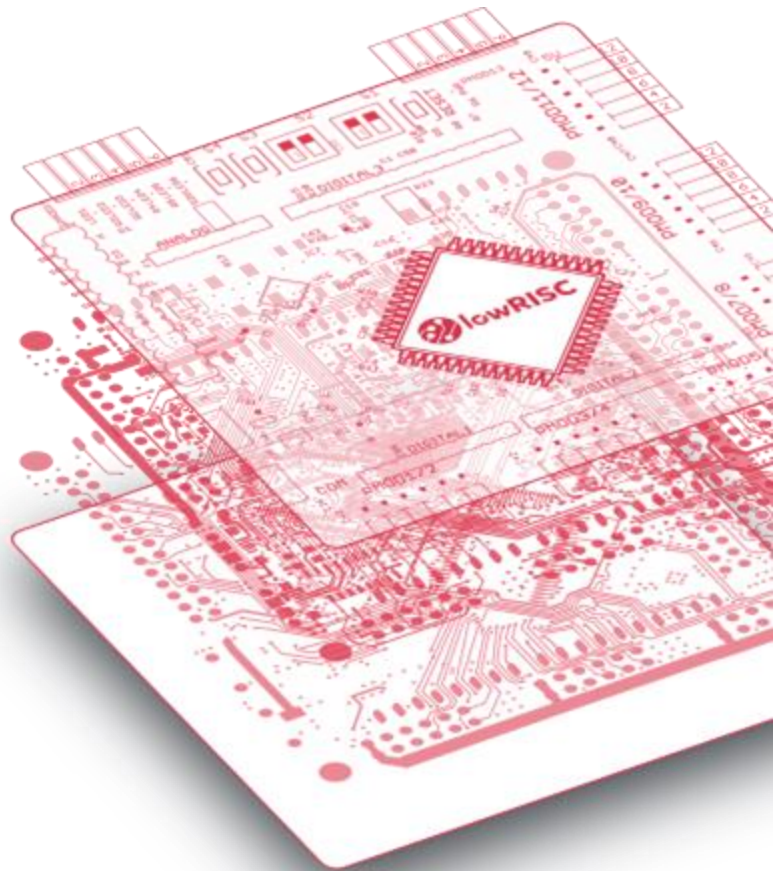
Dr Marno van der Maas

High Integrity Software Conference  
13 November, 2025




# Outline

- lowRISC overview
- Memory safety & CHERI
- Sonata development platform
- Area and code impact
- Get involved





# lowRISC overview

-  **lowRISC**
  - Founded in 2014 from Cambridge University
  - Open silicon everywhere!
  - Full stack engineering:  
HW Design/Verification, Compiler, Software



UNIVERSITY OF  
CAMBRIDGE

# lowRISC overview

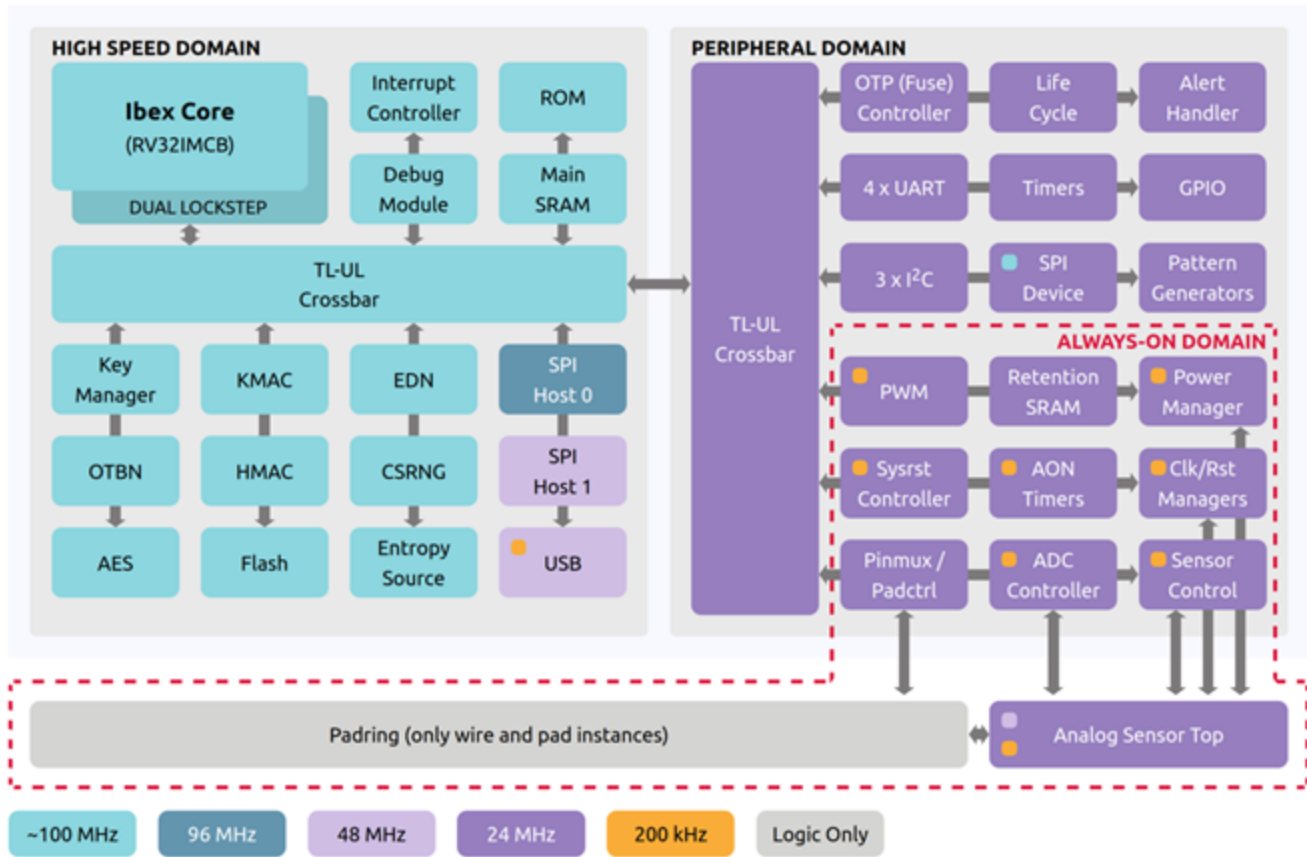
-  **lowRISC**
  - Founded in 2014 from Cambridge University
  - Open silicon everywhere!
  - Full stack engineering:  
HW Design/Verification, Compiler, Software
- 
  - Tools and training for secure hardware
  - Nova Scotia, Canada
  - Wholly owned subsidiary



UNIVERSITY OF  
CAMBRIDGE



Earl Grey	Discrete
Darjeeling	Integrated



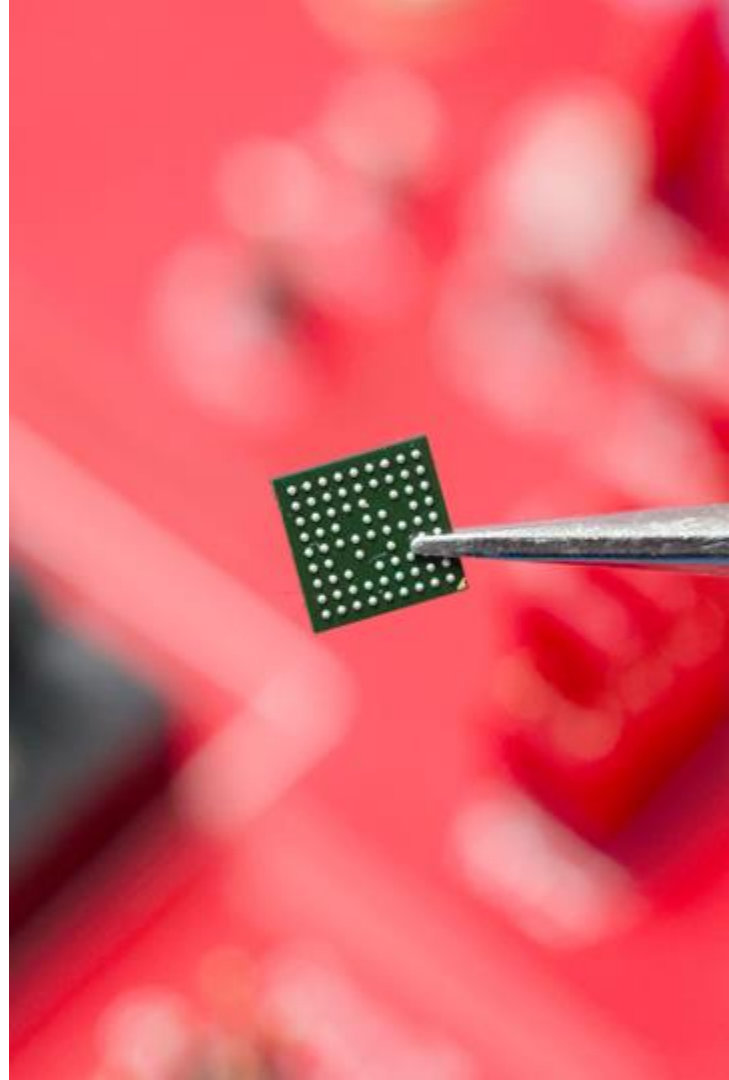


## Fabrication begins for production OpenTitan silicon

Thursday, February 6, 2025



Samples of production OpenTitan silicon are now available, with reference provisioning and application-level firmware releases coming soon. Product integrations have begun to intercept **Chromebooks** shipping later this year, with datacenter integrations following shortly after.



# Memory safety & CHERI

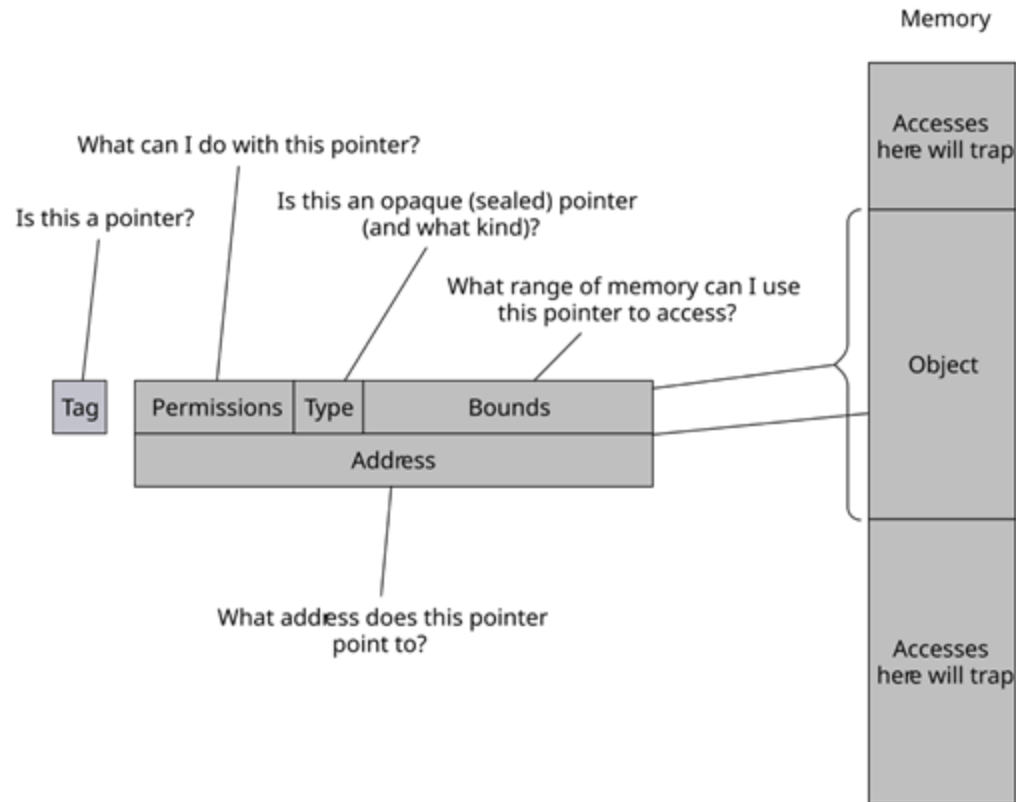
# Memory safety

- Microsoft:  
**70%** CVEs are memory safety issues
- Cybercrime:  
**\$10.5 tn** cost annually
- Crowdstrike:  
not malicious, but **\$5.4 bn** damage
- Apple invest in security:  
Enhanced memory tagging extension

Solution	Cost
New languages	Billions lines of legacy code
CHERI	Introducing hardware checks

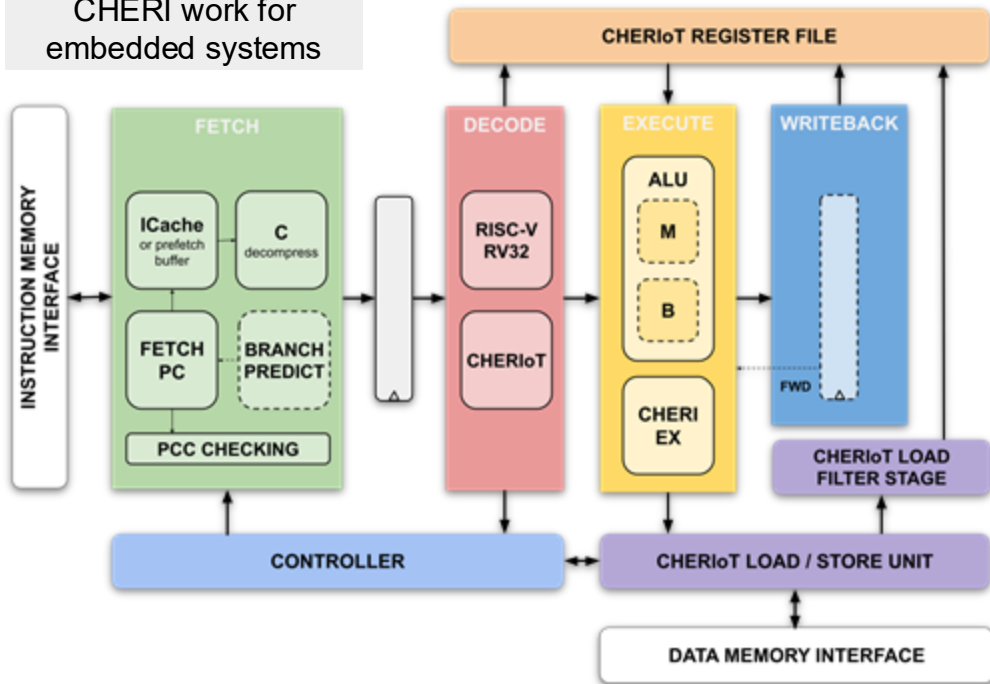


# CHERI Capabilities



# **ibex** + CHERI + RTOS = CHERIoT

CHERIoT: Making  
CHERI work for  
embedded systems



*“This is truly important foundational work, as it will help make CHERIoT-Ibex the world’s first production grade, open-source CHERI-enabled microcontroller core. We’re looking forward to seeing it broadly leveraged in commercial designs, bringing much-needed hardware security — in an efficient manner — to a broad swathe of critical applications.”*

Tony Chen  
Partner Security Architect, **Microsoft**

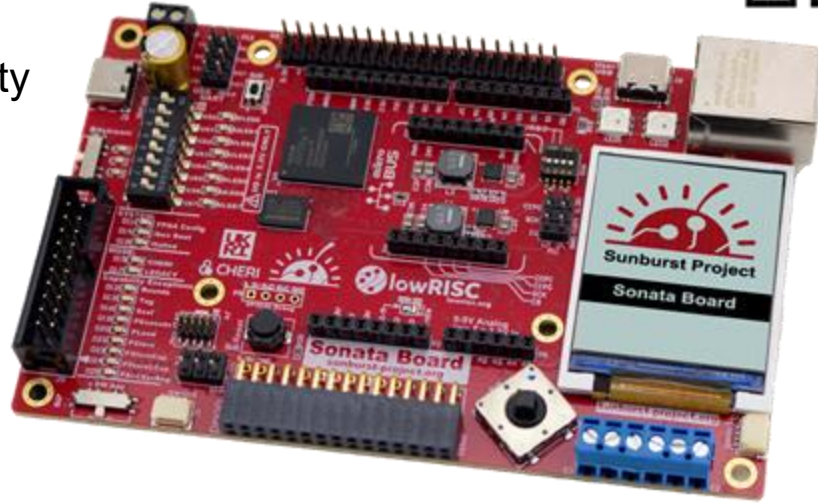
Sonata development platform

# Sonata platform

- Open RTL for baseline CHERIoT Ibex SoC + open FPGA PCB
- UKRI / DSbD funded Project [Project Number - 107540]
- 125 boards to leading commercial organisations and universities
- Support CHERIoT RTOS
  - Full compartmentalisation
  - Spatial and temporal safety
  - CHERIoT LLVM
  - Examples and demos



↑  
Buy it on  
Mouser!

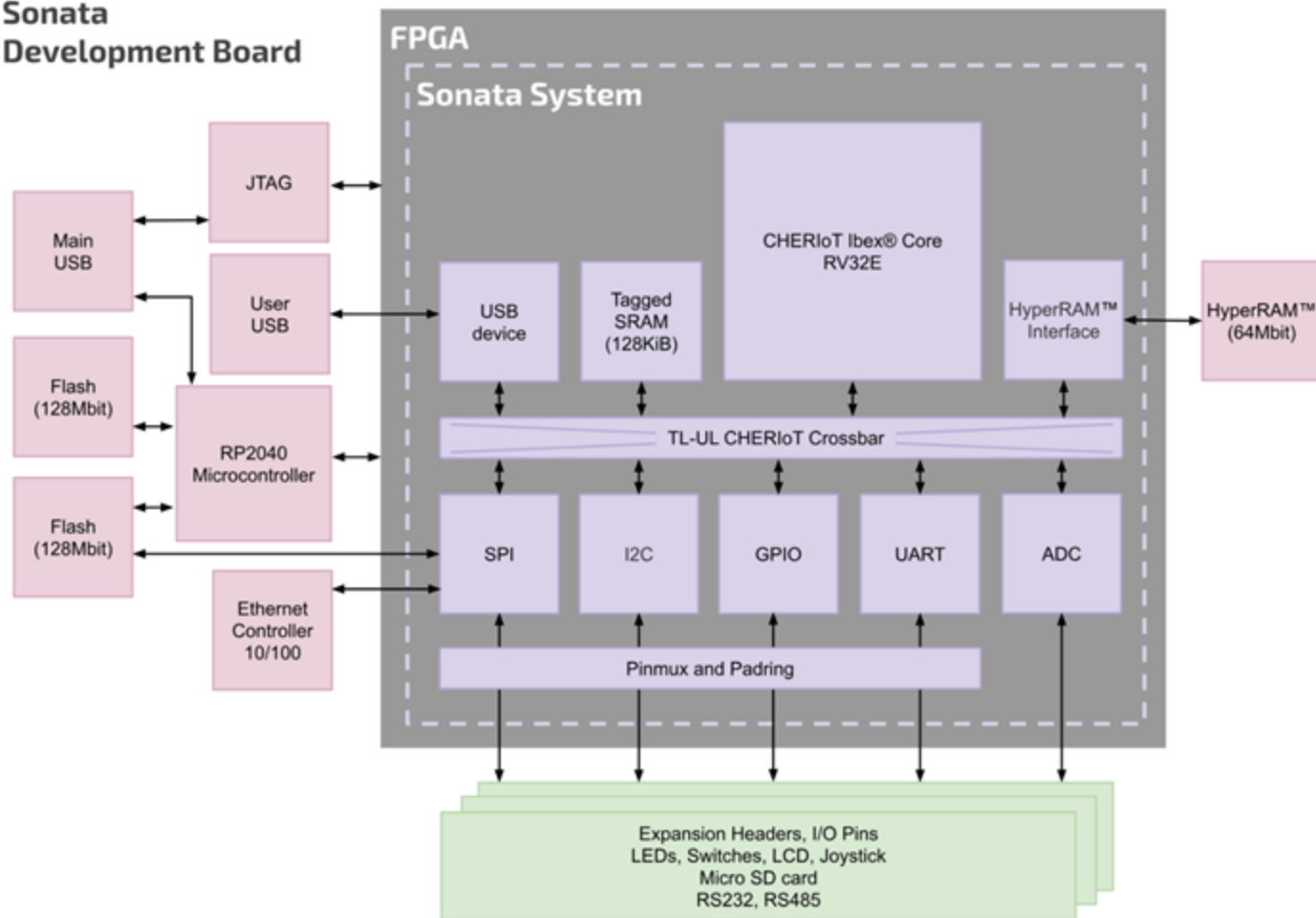


Delivered by  
Innovate UK,  
EPSRC and ESRC

Digital Security  
by Design



# Sonata Development Board



# Sonata v1.3 release

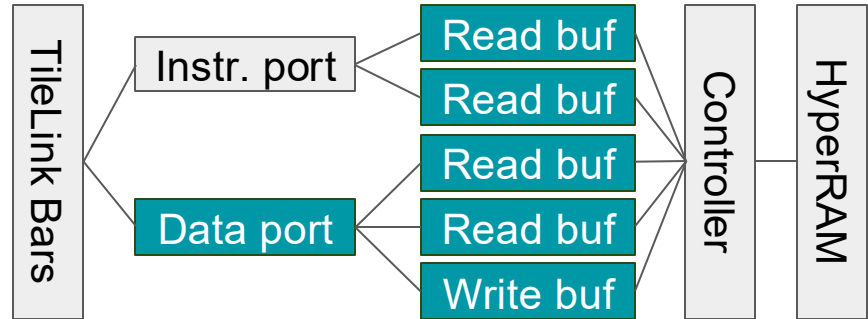
PWM  
GPIO      2 × faster  
RV\_Timer

SRAM      2 × faster

HyperRAM      3 × faster

```
end else begin : gen_access_latency0
    // Zero cycle latency; other cases caught by assertion below.
    assign timer_rdata_o = rdata_d;
    assign timer_rvalid_o = timer_req_i;
    assign timer_err_o   = error_d;
end

// TL-UL device adapters
tlul_adapter_sram #(
    .SramAw          ( SramAw ),
    .EnableRspIntgGen ( 0      ),
    .Outstanding      ( 2      )
) sram_a_device_adapter (
```



CHERI impact



# Area impact PMP vs CHERI

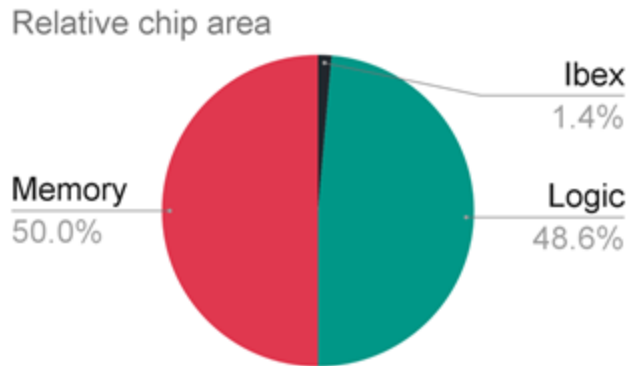
Configuration	Area	Overhead
Ibex	57 kGE	0 %
Ibex+PMP	81 kGE	42 %
Ibex+CHERI IoT	90 kGE	57 %

Chip area cost for memory safety:

- **0.6%** for PMP
- **1%** for CHERI

Mitigate memory vulnerabilities without significantly increasing area.

FreePDK45 +  OpenRAM



# Code impact - Embedded

Network code	Code size
FreeRTOS-TCP	74 kLoC
BearSSL	52 kLoC
coreMQTT	16 kLoC
coreSNTP	5 kLoC
Total unmodified	147 kLoC
CHERI wrapper	6 kLoC
Change	4%

**Table 2.** Code and data size of CHERIoT RTOS components.

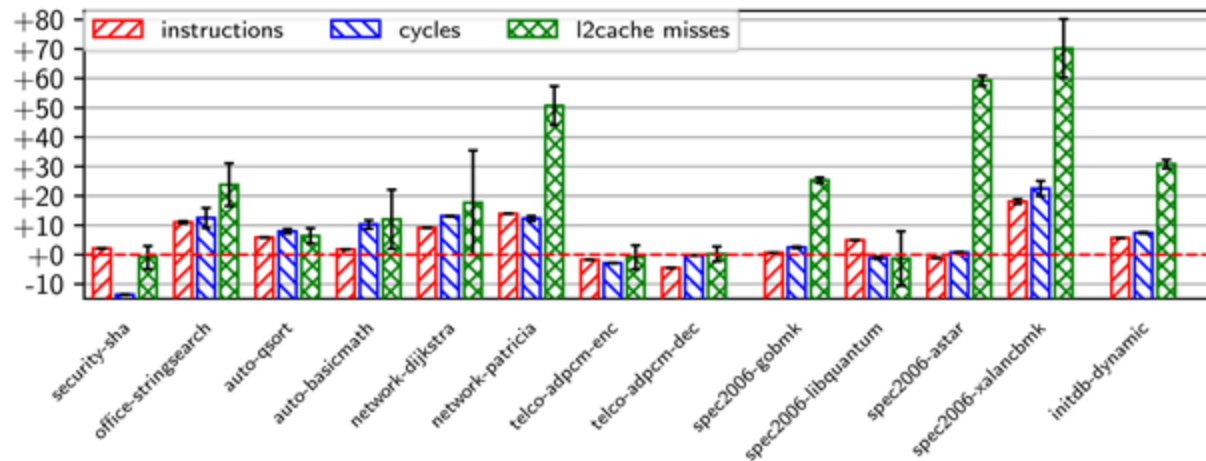
Component		Code Size	% of which for wrapper	Data Size
<b>Base System</b>		<b>25.9 KB</b>	-	<b>3.7 KB</b>
Including <sup>1</sup>	Loader	7.5 KB	0 % <sup>2</sup>	66 B
	Switcher	1.4 KB	0 % <sup>2</sup>	0 B
	Allocator	9 KB	0 % <sup>2</sup>	56 B
	Scheduler	3.3 KB	0 % <sup>2</sup>	472 B
<b>Base + Network Stack</b>		<b>151.8 KB</b>	-	<b>20.4 KB</b>
Including <sup>1</sup>	Firewall + Driver	6.6 KB	0 % <sup>2</sup>	176 B
	TCP/IP	38 KB	23 %	1.1 KB
	DNS Resolver	3.6 KB	0 % <sup>2</sup>	400 B
	SNTP	4.2 KB	47.2 %	56 KB
	TLS	56 KB	8 %	24 KB
	MQTT	11 KB	28 %	24 B

<sup>1</sup> Not detailing shared libraries, stacks, and compartment/library metadata.

# Code impact - Application-class

- Full desktop environment with CHERI:
  - Total: 6 MLoC
  - Change: **0.026%**
- Approaching 100 MLoC ported

Memory bandwidth:



Get involved

# CHERI Alliance founders



Technical  
Alignment



Promotion



Community  
Support



Join: [cheri-alliance.org/contact/](https://cheri-alliance.org/contact/)

# RISC-V standard

- Architecture review
- Extensions
  - Base: RV32/64Y
  - Zydefaultcap: default encoding
  - Zys: ambient sealing
  - Zyhybrid: mode bit
  - Zabhlrsc: byte-level loads
- **Have your say!**  
[github.com/riscv/riscv-cheri](https://github.com/riscv/riscv-cheri)

## RISC-V Specification for CHERI Extensions

Authors: Thomas Aird, Hesham Almatary, Andres Amaya Garcia, John Baldwin, Paul Buxton, David Chisnall, Jessica Clarke, Brooks Davis, Nathaniel Wesley Filardo, Franz A. Fuchs, Timothy Hutt, Alexandre Joannou, Martin Kaiser, Tariq Kurd, Ben Laurie, Marno van der Maas, Maja Malenko, A. Theodore Marketos, David McKay, Jamie Melling, Stuart Menefy, Simon W. Moore, Peter G. Neumann, Robert Norton, Alexander Richardson, Michael Roe, Peter Rugg, Peter Sewell, Carl Shaw, Ricki Tura, Robert N. M. Watson, Toby Wenman, Jonathan Woodruff, Jason Zhijingcheng Yu  
– Version V0.9.6-Draft-Ac79bdd, 20250924  
| DRAFT—NOT AN OFFICIAL RELEASE



This document is a specification snapshot built from [github.com/riscv/riscv-cheri/commit/ac79bdd0d2ad05a7c3a15a0c9cc54b52567c7c6b](https://github.com/riscv/riscv-cheri/commit/ac79bdd0d2ad05a7c3a15a0c9cc54b52567c7c6b) and is not a versioned release. The latest versioned PDF release can be downloaded from [github.com/riscv/riscv-cheri/releases](https://github.com/riscv/riscv-cheri/releases).



*This document is in the [Stable state](#)*  
Assume anything could still change, but limited change should be expected.

Open silicon everywhere



Thank you for your attention!

mvdmaas@lowrisc.org  
info@lowrisc.org

