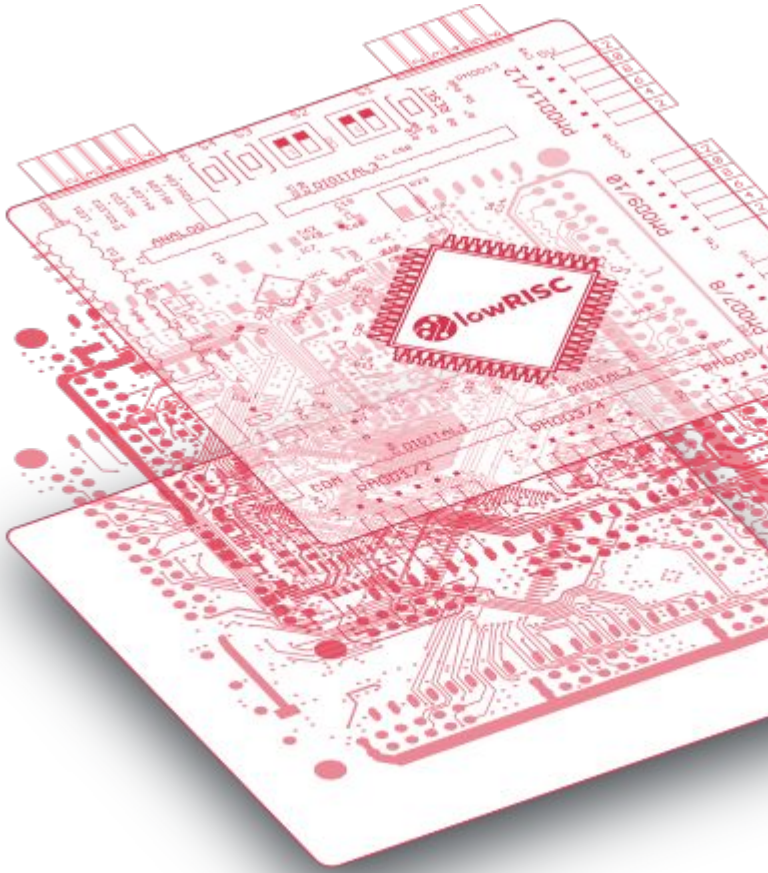
lowRISC

Sonata®

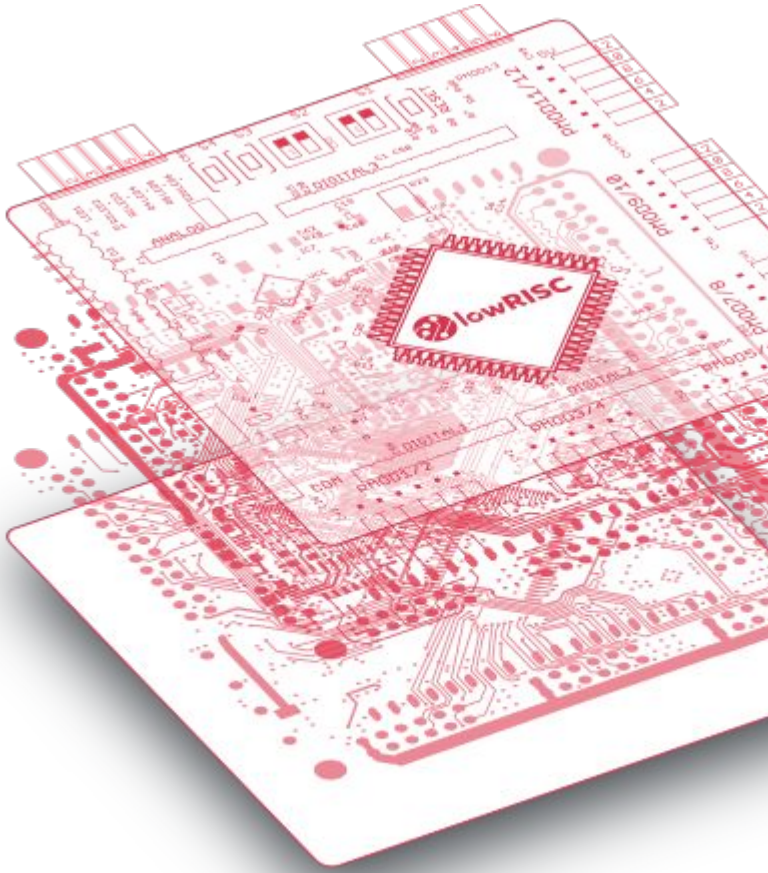
A platform for high-integrity operational technology



Dr Marno van der Maas
CHERITech'25
Manchester, UK
14 November, 2025

Outline

- lowRISC overview
- Sonata development platform
- Area and code impact
- Get involved



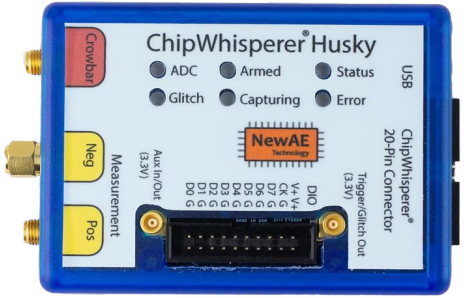
lowRISC overview

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

UNIVERSITY OF CAMBRIDGE

lowRISC overview

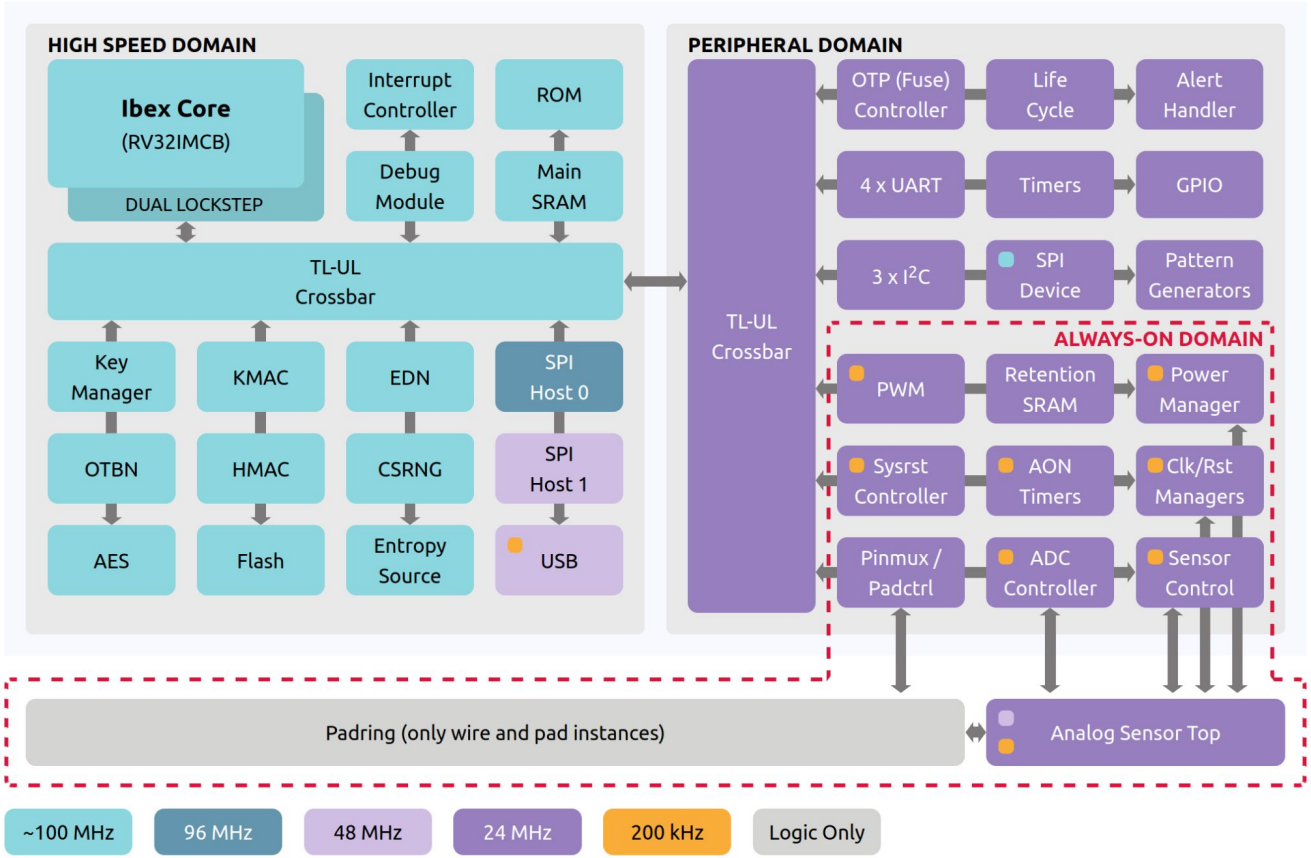
- lowRISC
  - Founded in 2014 from Cambridge University
  - Open silicon everywhere!
  - Full stack engineering:
    HW Design/Verification, Compiler, Software
- NewAE Technology
  - Tools and training for secure hardware
  - Nova Scotia, Canada
  - Wholly owned subsidiary



UNIVERSITY OF CAMBRIDGE

opentitan

Earl Grey	Discrete
Darjeeling	Integrated

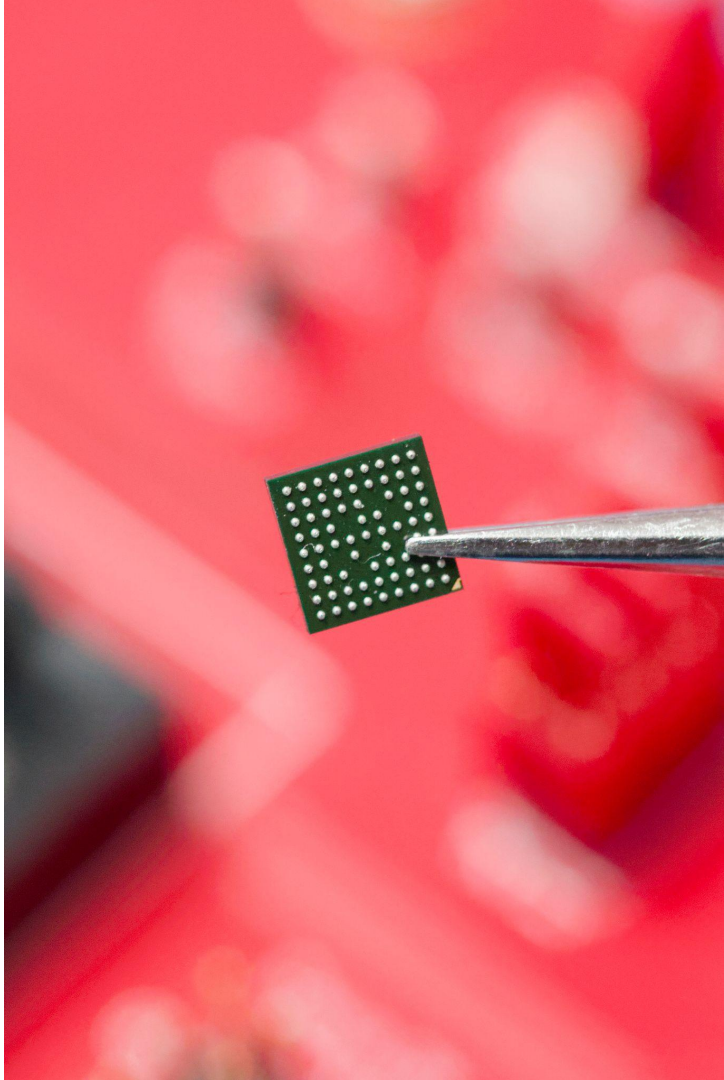


Google Open Source

Fabrication begins for production OpenTitan silicon

Thursday, February 6, 2025

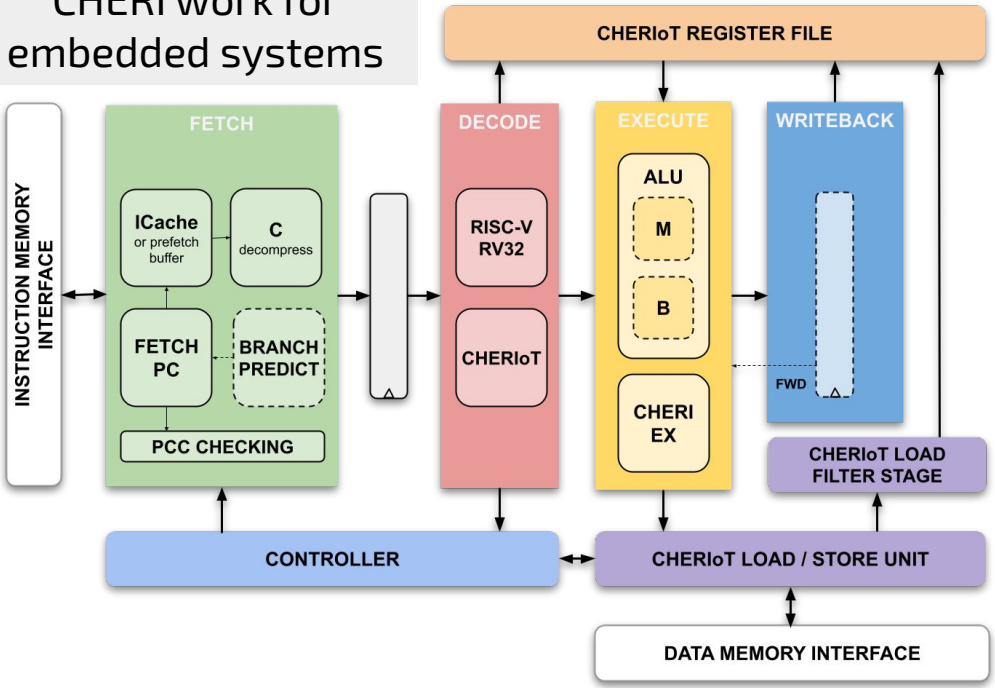
Samples of production OpenTitan silicon are now available, with reference provisioning and application-level firmware releases coming soon. Product integrations have begun to intercept Chromebooks shipping later this year, with datacenter integrations following shortly after.



Sonata® development platform

ibex + CHERI + RTOS = CHERIoT

CHERIoT: Making CHERI work for embedded systems



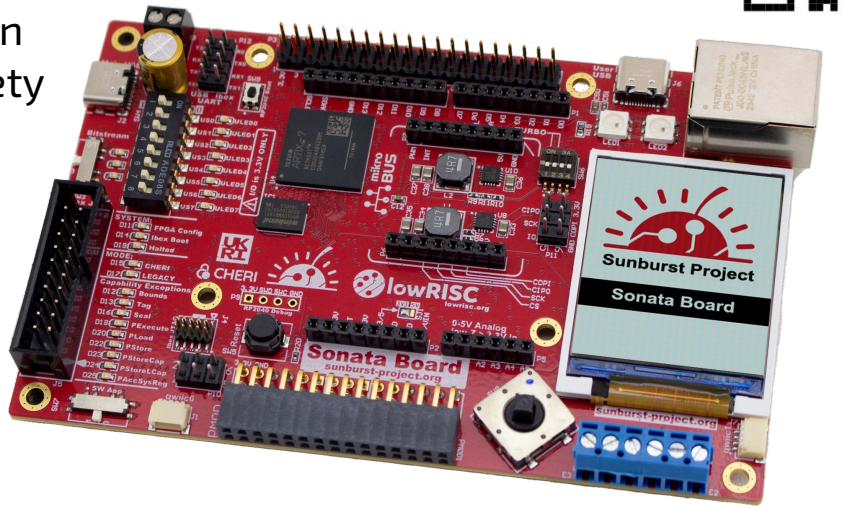
"This is truly important foundational work, as it will help make CHERIoT-Ibex the world's first production grade, open-source CHERI-enabled microcontroller core. We're looking forward to seeing it broadly leveraged in commercial designs, bringing much-needed hardware security — in an efficient manner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

Tony Chen
Partner Security Architect, **Microsoft**

github.com/microsoft/CherIoT-ibex

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

lowRISC

NewAE Technology

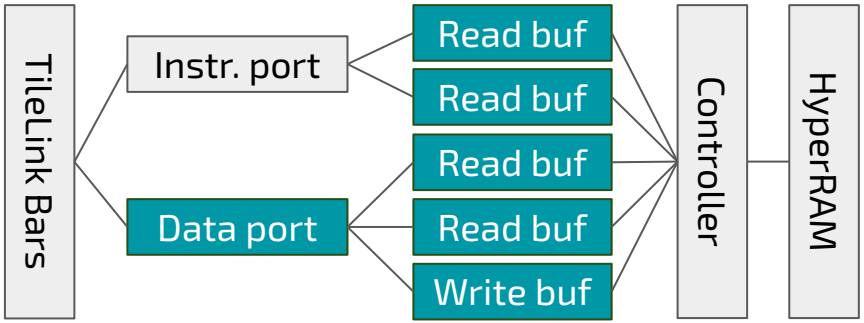
Sonata v1.3 release

PWM
GPIO 2 × faster
RV_Timer

SRAM 2 × faster

HyperRAM 3 × faster

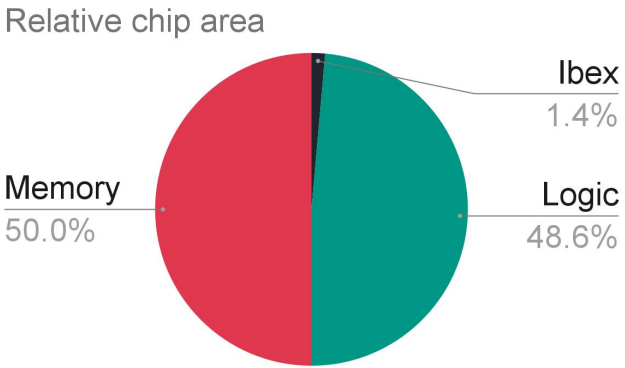
```
    end else begin : gen_access_latency0
      // Zero cycle latency; other cases caught by assertion below.
      assign timer_rdata_o  = rdata_d;
      assign timer_rvalid_o = timer_req_i;
      assign timer_err_o    = error_d;
    end

  // 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+CHERIoT	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

opentitan

Code impact - Embedded systems

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
Base System		**25.9 KB**	-	**3.7 KB**
Including[1]	Loader	7.5 KB	0 %[2]	66 B
	Switcher	1.4 KB	0 %[2]	0 B
	Allocator	9 KB	0 %[2]	56 B
	Scheduler	3.3 KB	0 %[2]	472 B
Base + Network Stack		**151.8 KB**	-	**20.4 KB**
Including[1]	Firewall + Driver	6.6 KB	0 %[2]	176 B
	TCP/IP	38 KB	23 %	1.1 KB
	DNS Resolver	3.6 KB	0 %[2]	400 B
	SNTP	4.2 KB	47.2 %	56 KB
	TLS	56 KB	8 %	24 KB
	MQTT	11 KB	28 %	24 B

[1] Not detailing shared libraries, stacks, and compartment/library metadata.

Get involved

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

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 Markettos, 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 and is not a versioned release. The latest versioned PDF release can be downloaded from 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

lowRISC

opentitan

ibex

Any questions?

mvdmaas@lowrisc.org
info@lowrisc.org