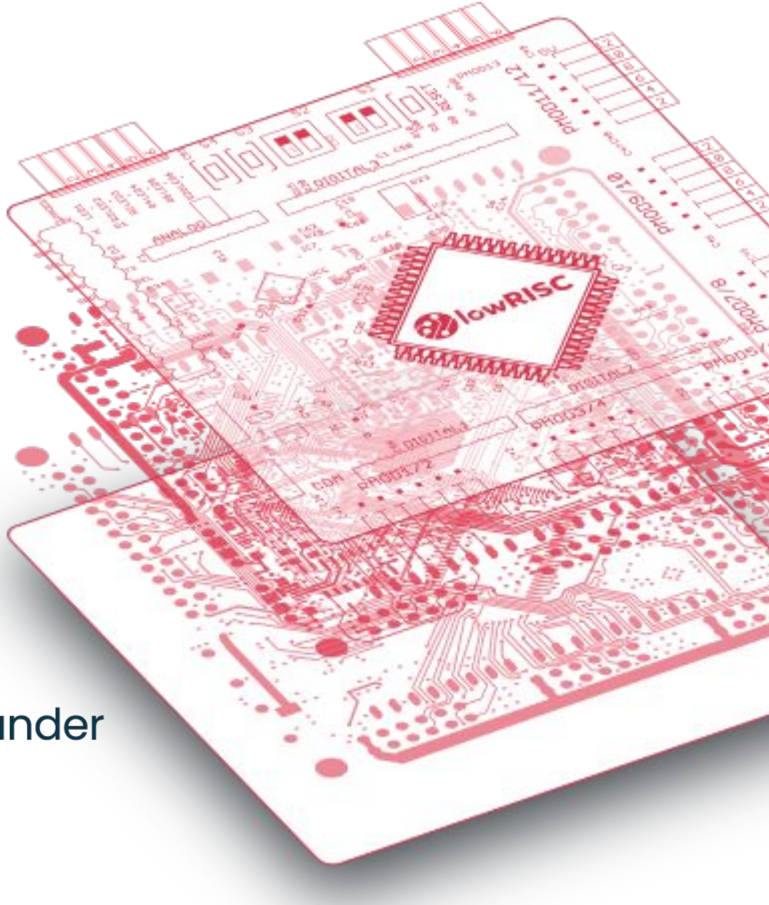
Sonata

Open source hardware and bitstream for evaluating CHERIoT

John Thomson, Project Manager, lowRISC
john.thomson@lowrisc.org

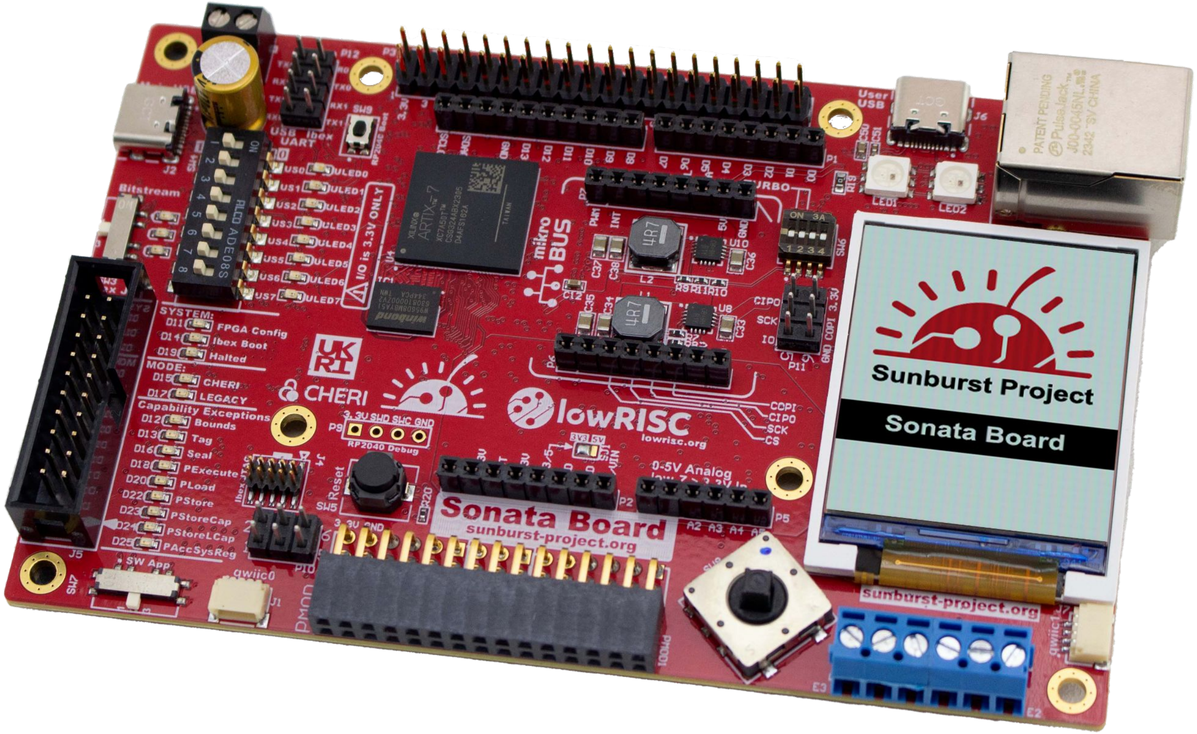


lowRISC

CHERI
Alliance Founder

2025-02-02, FOSDEM, Brussels

Sonata FPGA board and bitstream



Introduction to lowRISC

lowRISC was founded in 2014 as a spin-out from the University of Cambridge Computer Lab in the UK

UK regulated non-profit with a mission to drive commercial adoption of open source silicon

Full-stack engineering capability including silicon design, verification and security analysis as well as firmware and toolchain development

Rapidly expanding team with 20+ engineering staff and management/support staff with offices in Cambridge and Zürich

Founding member of the RISC-V Foundation (now RISC-V International) and the CHERI Alliance

Steward and maintainer of the **OpenTitan**® and **Ibex**® projects

UNIVERSITY OF CAMBRIDGE

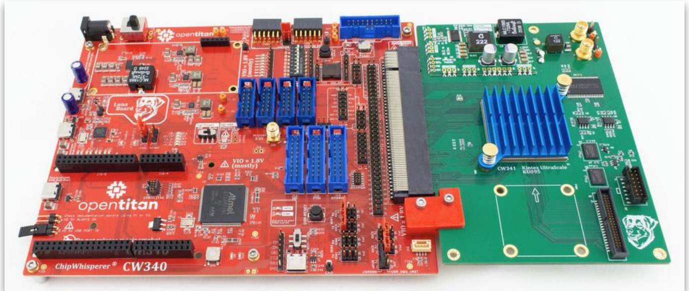
RISC-V®

CHERI Alliance Member

lowRISC FOUNDING

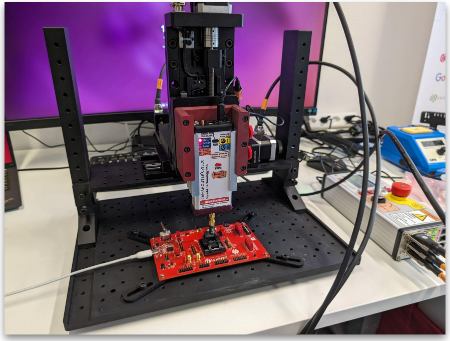
Introduction to NewAE

NewAE Technology Inc. is a **wholly-owned subsidiary** of lowRISC CIC that provides in-house electronics expertise to the group and produces security evaluation tools, including:



ChipWhisperer
Hardware for side-channel power analysis and fault injection

ChipSHOUTER
Electromagnetic fault injection (EMFI) tool, which allows precise injection of faults at specific locations on the IC surface



In addition, NewAE have produced a large amount of high quality educational material, run frequent training events at BlackHat

Introduction to OpenTitan®

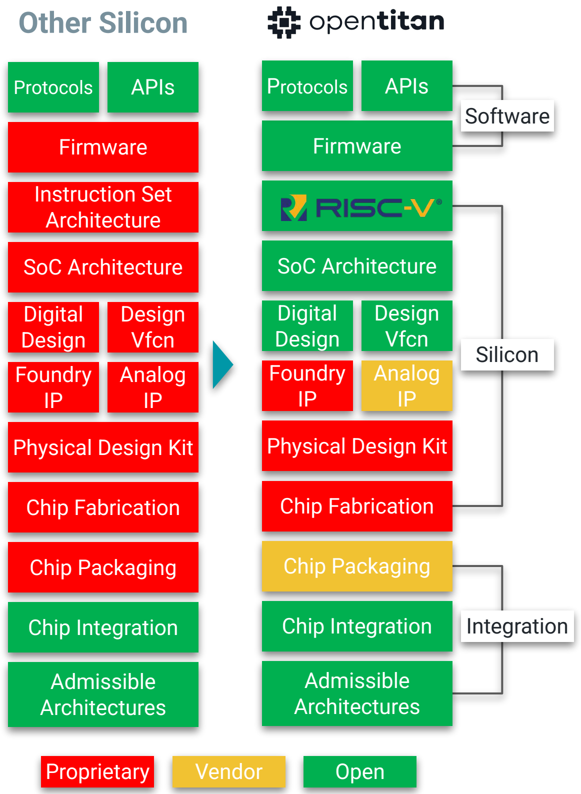
The OpenTitan® partnership develops, verifies and maintains an ecosystem of high quality - **open source** - chip designs and security IP

lowRISC

Rivos Google zeroRISC

winbond SEAGATE nuvoTon

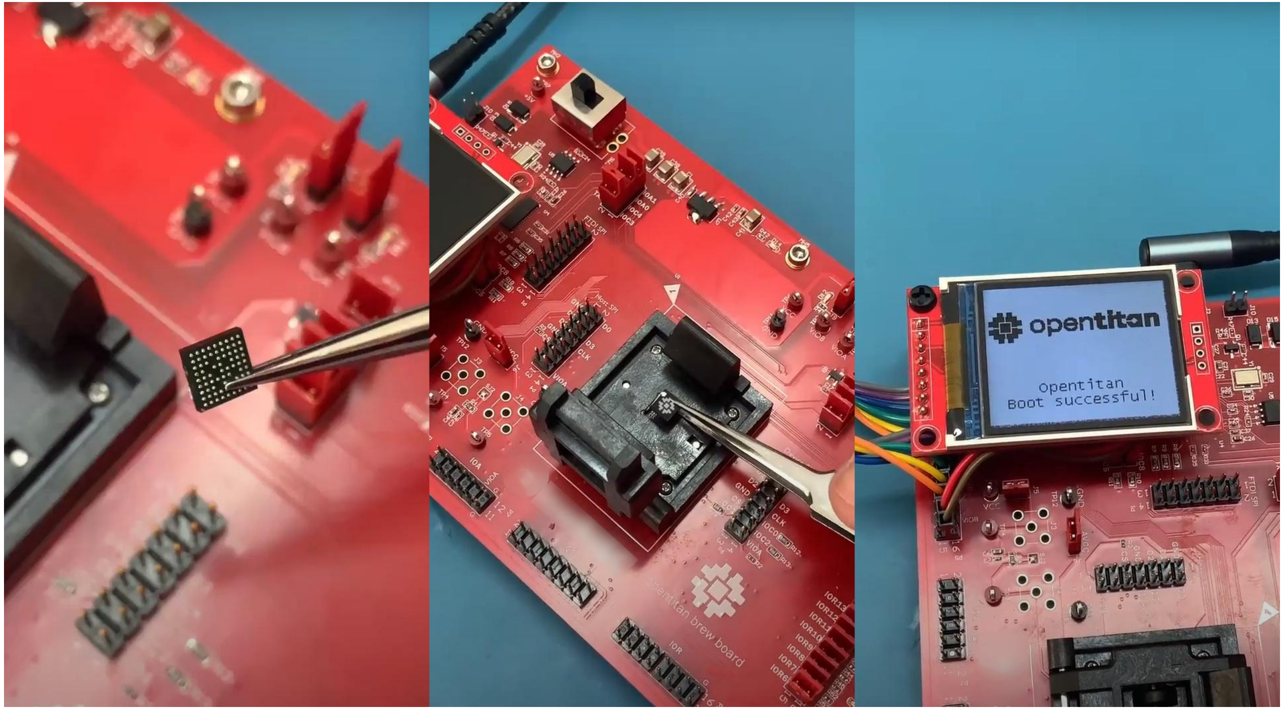
Giesecke+Devrient Western Digital ETH zürich



Other Silicon	opentitan	
Protocols 🟩	Protocols 🟩	Software
APIs 🟩	APIs 🟩	
Firmware 🟥	Firmware 🟩	
Instruction Set Architecture 🟥	RISC-V 🟩	Silicon
SoC Architecture 🟥	SoC Architecture 🟩	
Digital Design 🟥	Digital Design 🟩	
Design Vfcn 🟥	Design Vfcn 🟩	
Foundry IP 🟥	Foundry IP 🟥	
Analog IP 🟥	Analog IP 🟨	
Physical Design Kit 🟥	Physical Design Kit 🟥	
Chip Fabrication 🟥	Chip Fabrication 🟥	
Chip Packaging 🟥	Chip Packaging 🟨	Integration
Chip Integration 🟩	Chip Integration 🟩	
Admissible Architectures 🟩	Admissible Architectures 🟩	

🟥 Proprietary 🟨 Vendor 🟩 Open

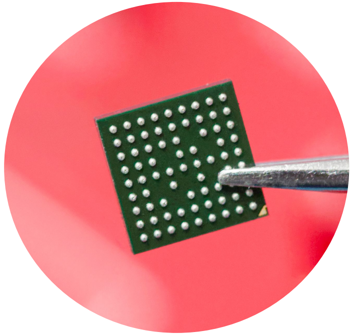
Proof: World's 1st Commercial-Grade Open Source Chip...



… Now Going into Real Sockets

“Nuvoton Technology Corporation […] announced today that ***Google’s ChromeOS plans to use the first commercial chip built on the OpenTitan*** *open source secure silicon design as an evolution of its security chip* ***for Chromebooks****.”*

Nuvoton, May 2024



*“****Hardware security is something we don’t compromise on.*** *We are excited to partner with the dream team of Nuvoton, a valued, historic, strategic partner, and lowRISC, a leader in secure silicon, to maintain this high bar of quality.”*

Prajakta Gudadhe
Sr Director, ChromeOS Platform Engineering

nuvoTon

opentitan

chromebook

https://www.nuvoton.com/news/news/all/TSNuvotonNews-000514

Proof: World's Most Active Open Silicon Project

RTL · design verification collateral · documentation · low-level firmware · tests

25,000+
total commits
(Ibex + OpenTitan)

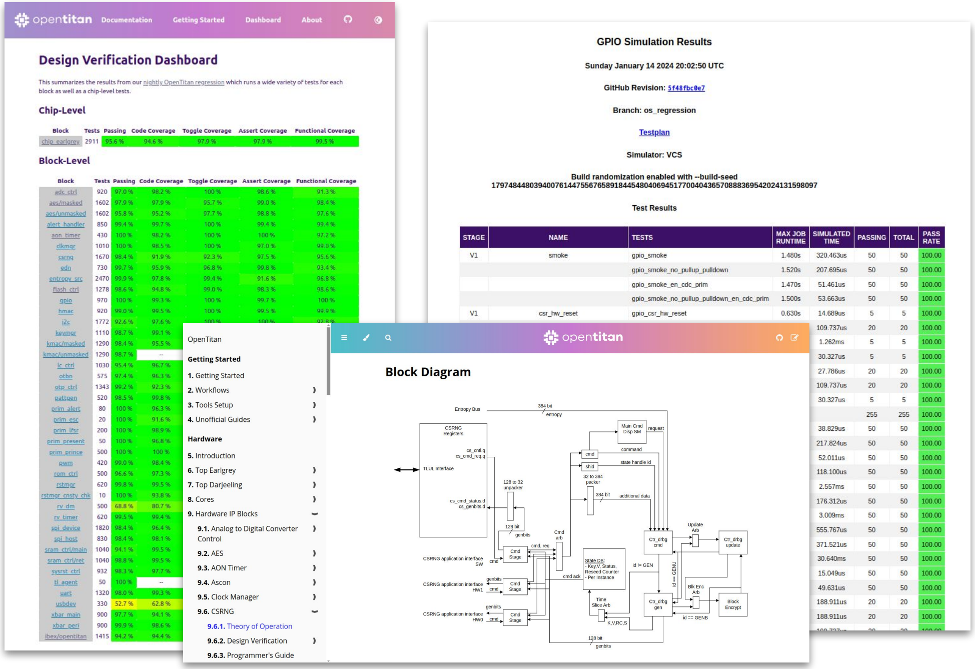
250+
contributors
(Ibex + OpenTitan)

7,200+
GitHub issues
(Ibex + OpenTitan)

3,700+
GitHub stars
(Ibex + OpenTitan)

440,000+
lines of SystemVerilog
(Digital Design and Verification for Ibex + OpenTitan)

40,000+
test runs in nightly regressions
(run multiple times per week)



Design Verification Dashboard

This summarizes the results from our nightly OpenTitan regression which runs a wide variety of tests for each block as well as a chip-level tests.

Chip-Level

Block	Tests	Passing	Code Coverage	Toggle Coverage	Assert Coverage	Functional Coverage
chip_earlgrey	2911	95.6 %	94.6 %	97.9 %	97.9 %	99.5 %

Block-Level

Block	Tests	Passing	Code Coverage	Toggle Coverage	Assert Coverage	Functional Coverage
adc_ctrl	920	97.0 %	98.2 %	100 %	98.6 %	91.3 %
aes/masked	1602	97.9 %	97.9 %	95.7 %	99.0 %	98.4 %
aes/unmasked	1602	95.8 %	95.2 %	97.7 %	98.8 %	97.6 %
alert_handler	850	99.4 %	99.7 %	100 %	99.4 %	99.4 %
aon_timer	430	100 %	98.2 %	100 %	100 %	97.2 %
clkmgr	1010	100 %	98.5 %	100 %	97.0 %	99.0 %
csrng	1670	98.4 %	91.9 %	92.3 %	97.5 %	95.6 %
edn	730	99.7 %	95.9 %	96.8 %	99.8 %	93.4 %
entropy_src	2470	99.9 %	97.8 %	99.4 %	91.6 %	96.8 %
flash_ctrl	1278	98.6 %	94.8 %	99.0 %	98.3 %	98.6 %
gpio	970	100 %	99.3 %	100 %	99.7 %	100 %
hmac	920	99.0 %	99.5 %	100 %	99.5 %	99.9 %
i2c	1772	92.6 %	97.6 %	100 %	100 %	92.8 %
keymgr	1110	98.7 %	99.1 %			
kmac/masked	1290	98.4 %	95.5 %			
kmac/unmasked	1290	98.7 %	--			
lc_ctrl	1030	95.4 %	96.7 %			
otbn	575	97.4 %	96.3 %			
otp_ctrl	1343	99.2 %	92.3 %			
pattgen	520	98.5 %	99.8 %			
prim_alert	80	100 %	96.3 %			
prim_esc	20	100 %	91.6 %			
prim_lfsr	200	100 %	98.9 %			
prim_present	50	100 %	96.8 %			
prim_prince	500	100 %	100 %			
pwm	420	99.0 %	98.4 %			
rom_ctrl	500	96.6 %	97.3 %			
rstmgr	620	99.8 %	99.5 %			
rstmgr_cnsty_chk	10	100 %	93.8 %			
rv_dm	500	68.8 %	80.7 %			
rv_timer	620	99.5 %	99.4 %			
spi_device	1820	98.4 %	96.4 %			
spi_host	830	98.4 %	98.1 %			
sram_ctrl/main	1040	94.1 %	99.5 %			
sram_ctrl/ret	1040	98.8 %	99.5 %			
sysrst_ctrl	932	98.3 %	97.7 %			
tl_agent	50	100 %	--			
uart	1320	98.0 %	99.3 %			
usbdev	330	52.7 %	62.8 %			
xbar_main	900	97.7 %	94.1 %			
xbar_peri	900	99.9 %	98.6 %			
ibex/opentitan	1415	94.2 %	94.4 %			

GPIO Simulation Results

Sunday January 14 2024 20:02:50 UTC

GitHub Revision: 5f48fbc0e7

Branch: os_regression

Testplan

Simulator: VCS

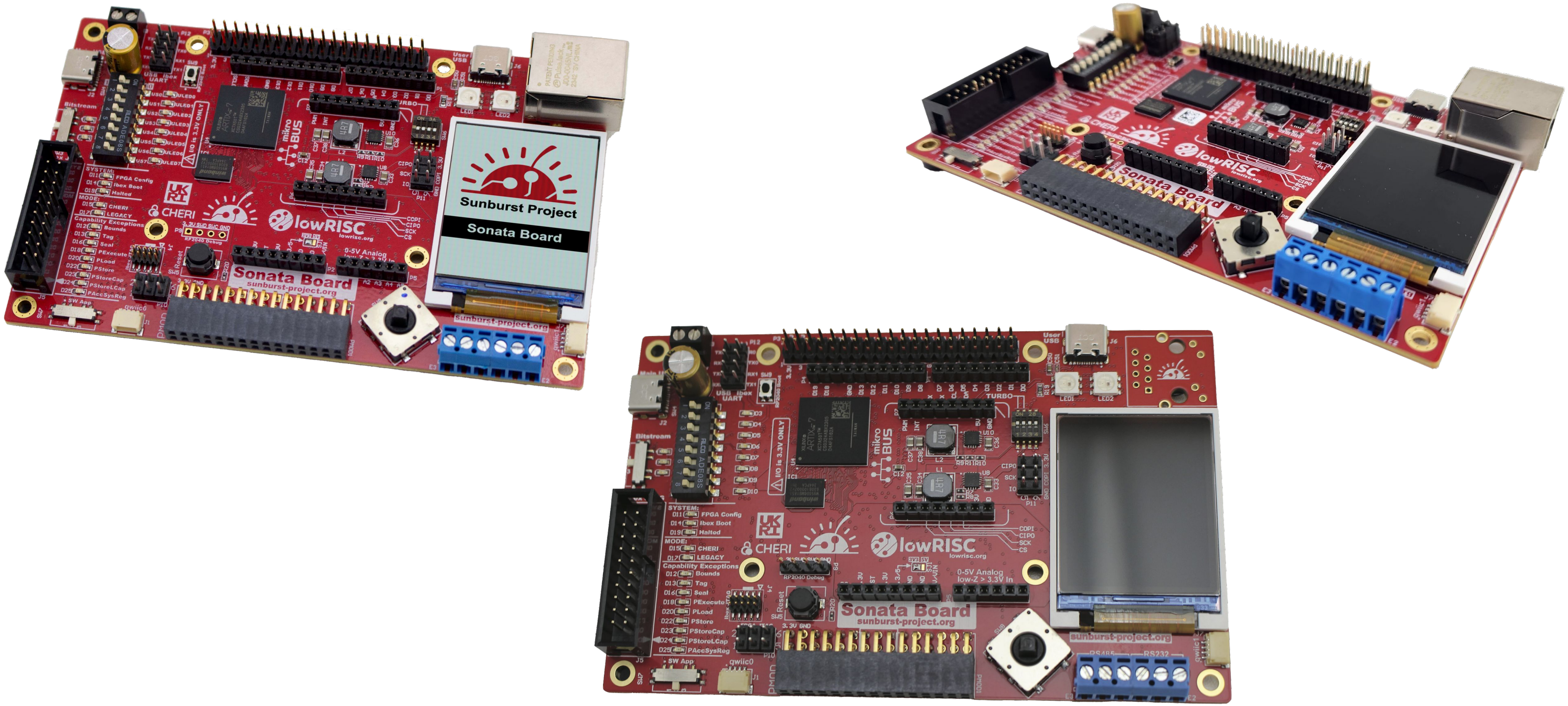
Build randomization enabled with --build-seed 17974844803940076144755676589184454804069451770040436570888369542024131598097

Test Results

STAGE	NAME	TESTS	MAX JOB RUNTIME	SIMULATED TIME	PASSING	TOTAL	PASS RATE
V1	smoke	gpio_smoke	1.480s	320.463us	50	50	100.00
		gpio_smoke_no_pullup_pulldown	1.520s	207.695us	50	50	100.00
		gpio_smoke_en_cdc_prim	1.470s	51.461us	50	50	100.00
		gpio_smoke_no_pullup_pulldown_en_cdc_prim	1.500s	53.663us	50	50	100.00
V1	csr_hw_reset	gpio_csr_hw_reset	0.630s	14.689us	5	5	100.00
				109.737us	20	20	100.00
				1.262ms	5	5	100.00
				30.327us	5	5	100.00
				27.786us	20	20	100.00
				109.737us	20	20	100.00
				30.327us	5	5	100.00
					255	255	100.00
				38.829us	50	50	100.00
				217.824us	50	50	100.00
				52.011us	50	50	100.00
				118.100us	50	50	100.00
				2.557ms	50	50	100.00
				176.312us	50	50	100.00
				3.009ms	50	50	100.00
				555.767us	50	50	100.00
				371.521us	50	50	100.00
				30.640ms	50	50	100.00
				15.049us	50	50	100.00
				49.631us	50	50	100.00
				188.911us	20	20	100.00
				188.911us	20	20	100.00

Block Diagram

Back to the Sonata FPGA board and bitstream



Sunburst Project

CHERIoT Hardware Enablement

lowRISC

NewAE Technology

UKRI Delivered by Innovate UK, EPSRC and ESRC

Digital Security by Design

Funded by DSbD / UKRI - Grant Number: 107540

sunburst-project.org

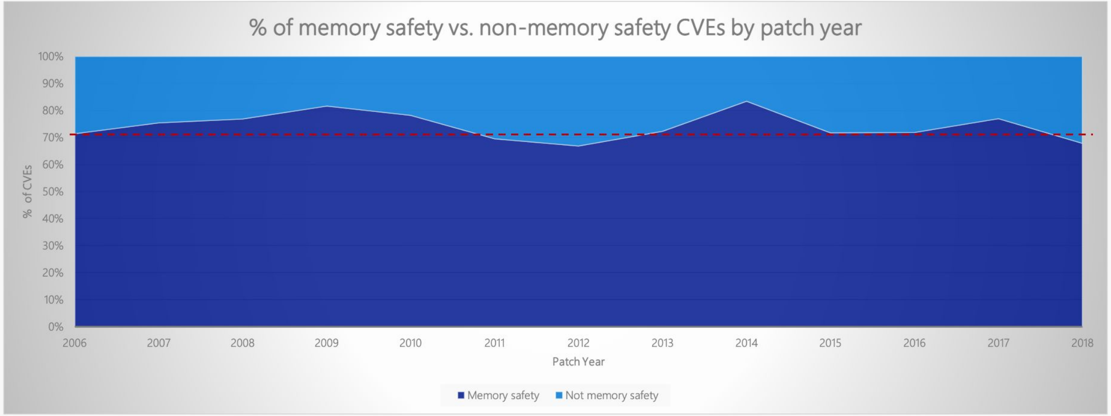
Cost of security breaches

- IBM estimates the global average cost of a data breach to be $4.45 million[1]
- Heartbleed vulnerability in OpenSSL was conservatively estimated to have cost more than $500 million[2]
- NIST NVD showed a fivefold increase in cyberattacks on embedded systems between 2017 and the end of 2022

- 4.45 M USD buys a lot beer

[1] IBM - Cost of a Data Breach Report 2023 Report
[2] ElectronicDesign - What's the Difference Between Conventional Memory Protection and CHERI?

Memory bugs and the need for CHERI



~70% of the vulnerabilities addressed through a security update each year continue to be memory safety issues

- Microsoft in 2019 reported that 70% of the CVEs they report annually are memory safety issues[1]
- Use Rust / .Net?
    - Requires rewriting trillions of lines of C/C++ code
    - Possible for new code, but no compartmentalisation

[1]: https://msrc.microsoft.com/blog/2019/07/a-proactive-approach-to-more-secure-code/

CHERI / CHERIoT

- CHERI
  - Capability Hardware Enhanced RISC Instructions
- Deterministic, fine-grained memory protection
- Scalable compartmentalisation

UNIVERSITY OF CAMBRIDGE

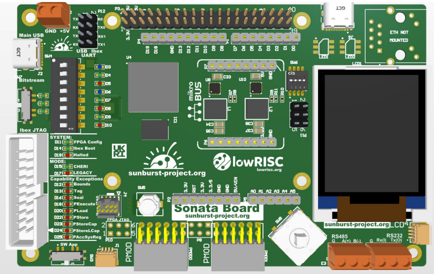
SRI

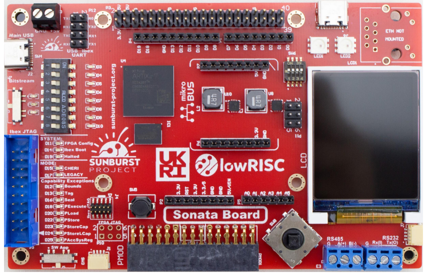
- Architectural solution
  - Works with existing software
  - Protects software with hardware
  - Extension of conventional hardware ISAs

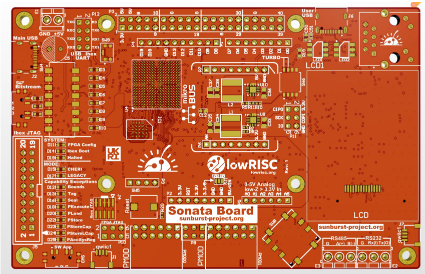
- CHERIoT
  - Microsoft built on Ibex® and added an RTOS for embedded use

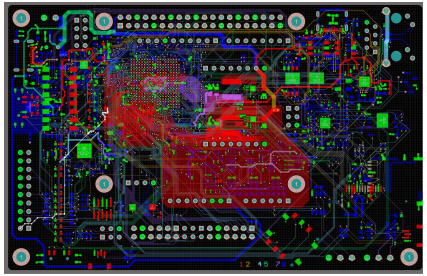
Sonata Project includes FPGA Host Board

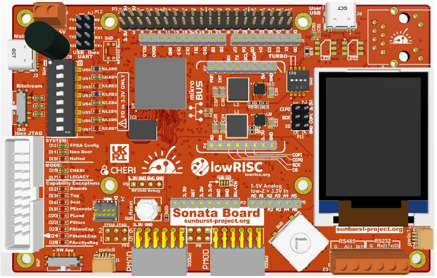
- lowRISC and NewAE have worked on getting Sonata boards prepared over the last year

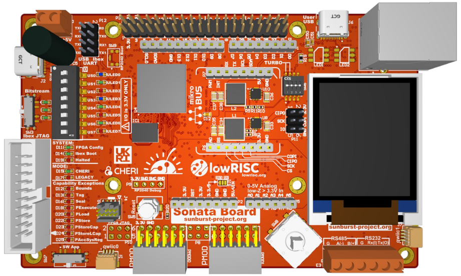


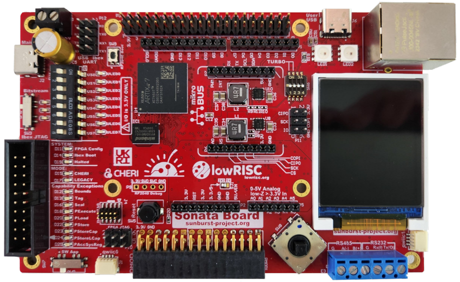


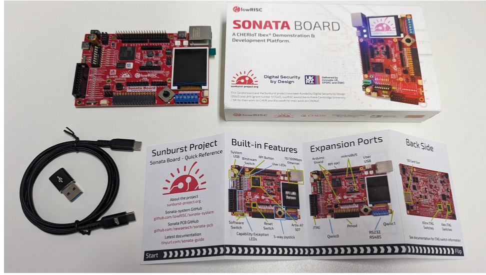








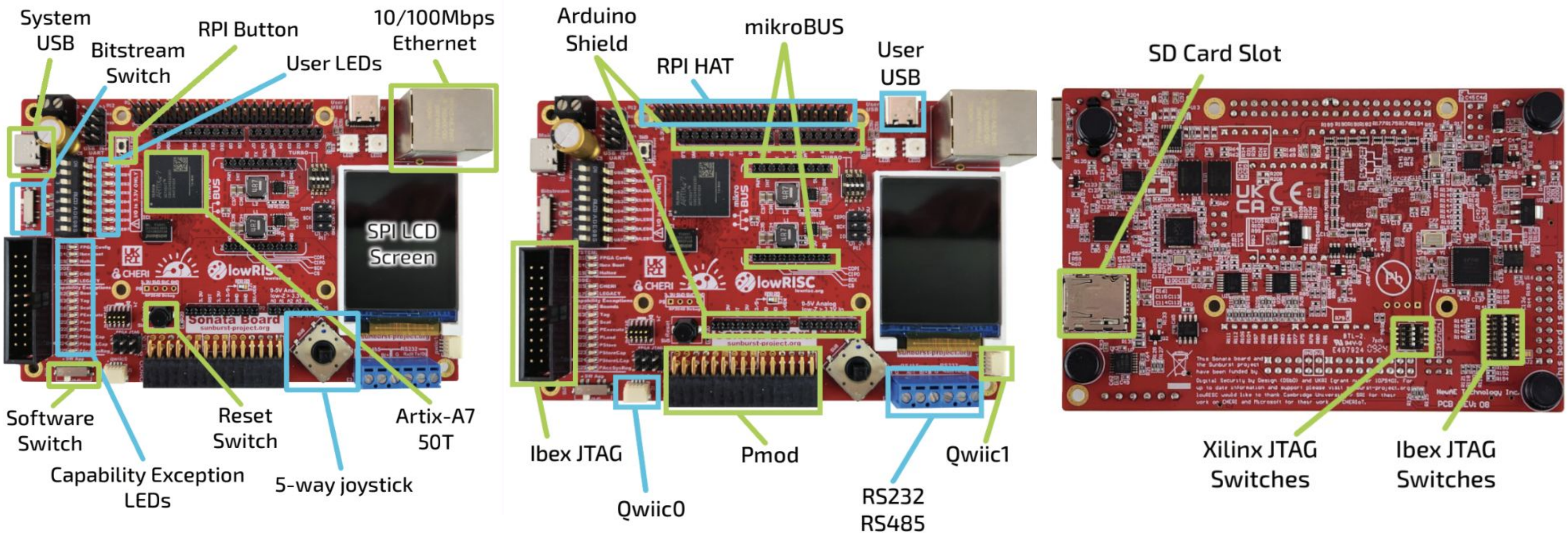



lowRISC
SONATA BOARD
A CHERIoT Ibex® Demonstration & Development Platform.
Sunburst Project
Sonata Board - Quick Reference
Built-in Features
Expansion Ports
Back Side
Start

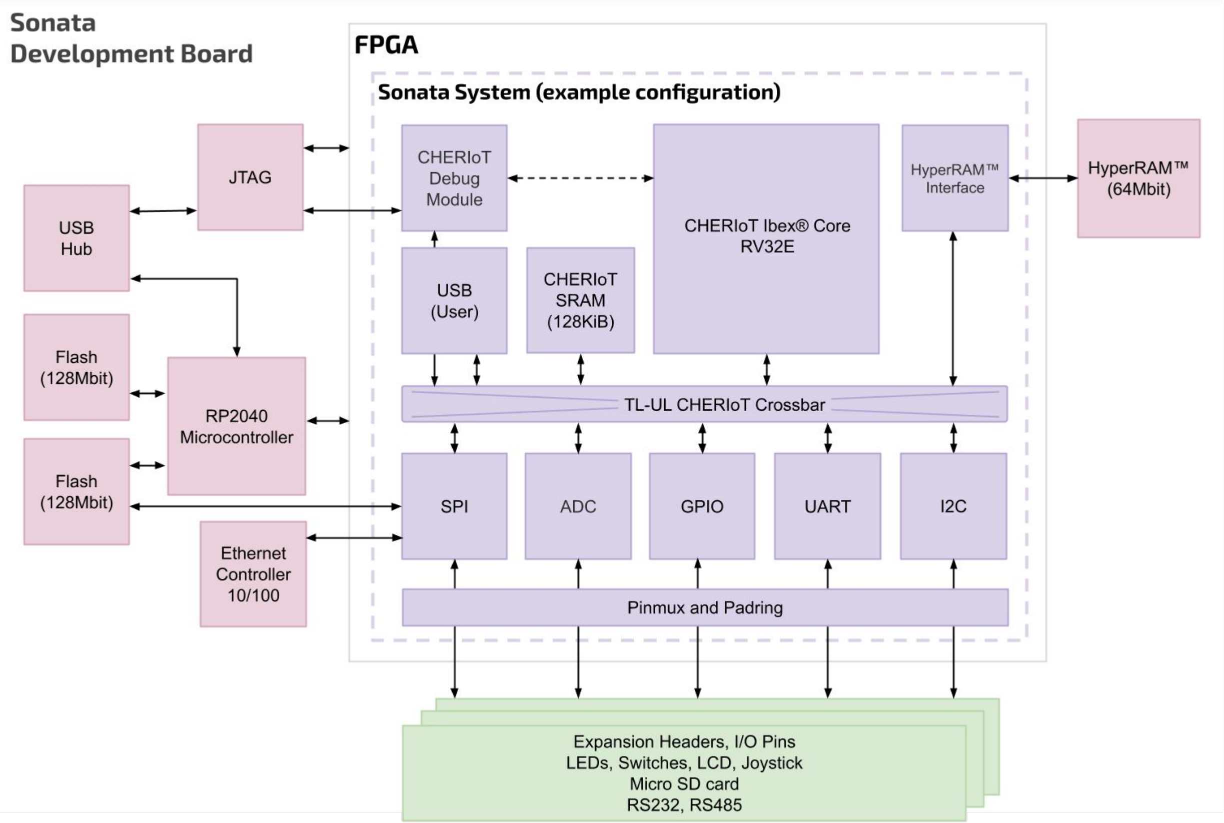
Revision 8 / 9 boards are the final version of the board
(0.9 has minor BOM modifications only)

Sonata Board Features

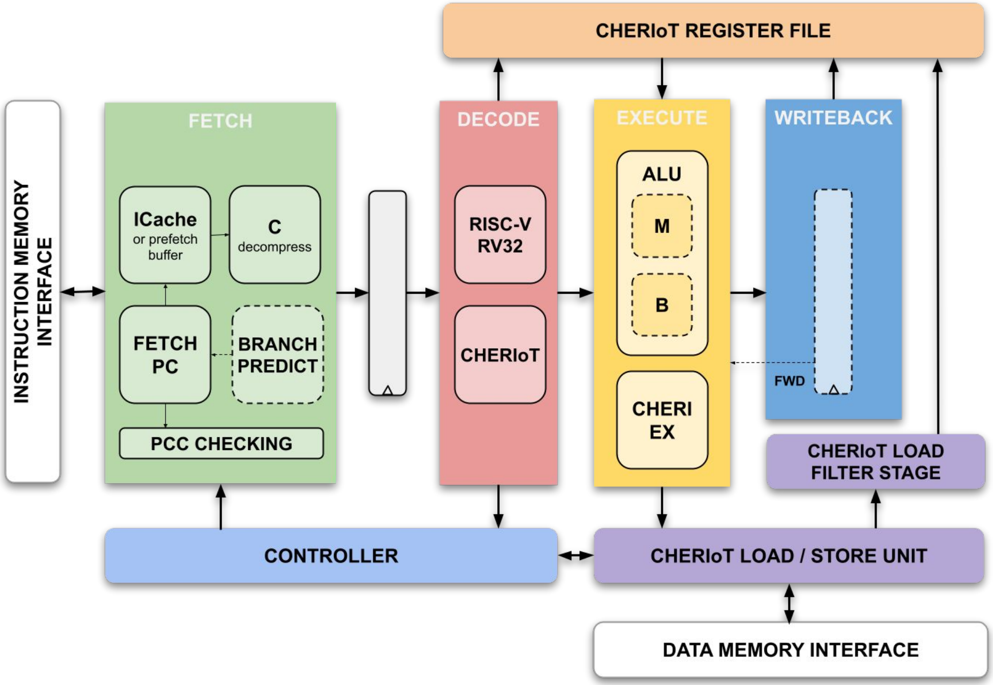
- Some of the key items / features on the boards



Sonata — Complete System Overview



IBEX + CHERI + RTOS = CHERIoT; TopLvl$_1$ = Sonata



https://github.com/microsoft/CherIoT-ibex

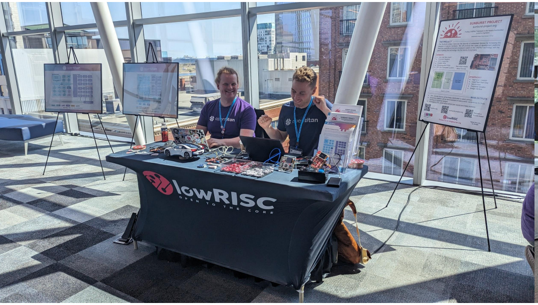
Microsoft lowRISC

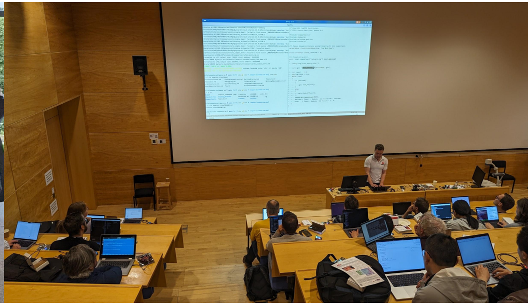
“This is truly important foundational work, as it will help make CHERIoT-Ibex the world’s first production grade, open-source CHERI-enabled microcontroller core. We’re looking forward to seeing it broadly leveraged in commercial designs, bringing much-needed hardware security — in an efficient manner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

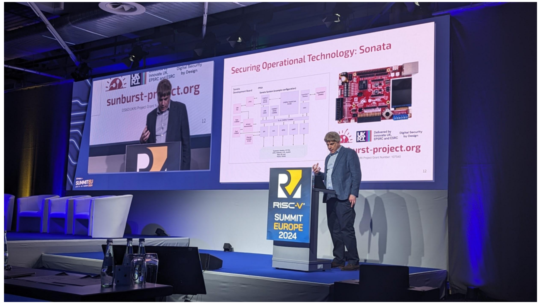
Tony Chen
Partner Security Architect, Microsoft

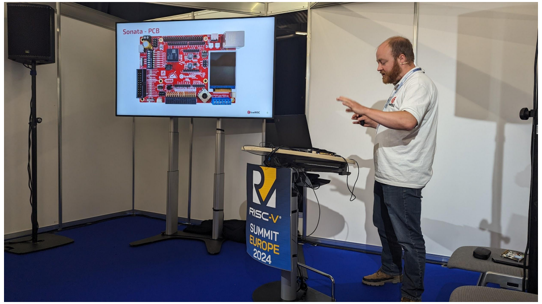
Engaging through Outreach Events

- Promoting collaboration with the wider community





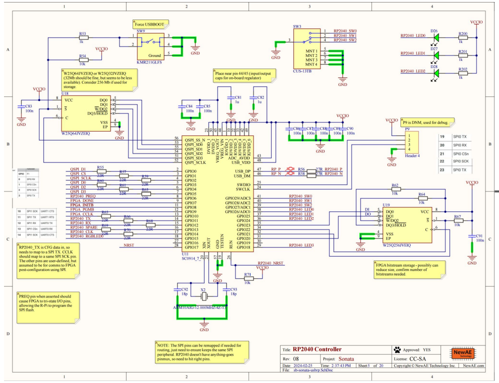




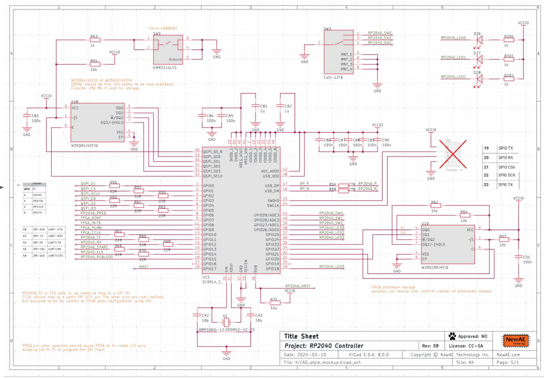
lowRISC staff regularly attend high visibility conferences including RISC-V / CHES / OCP and prepare training events

KiCad

- Making the final part of the Sonata board open source
- KiCad model of Sonata is now available



Altium

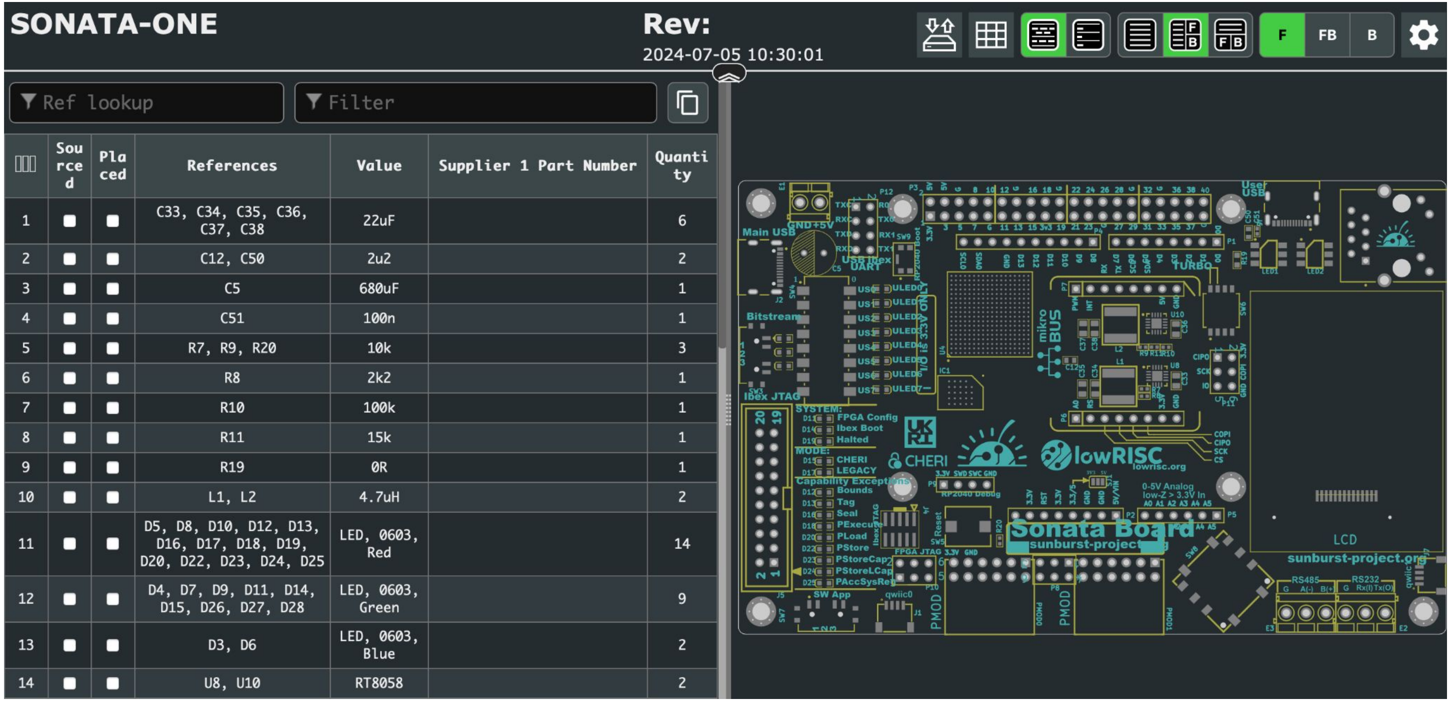


KiCad

- https://github.com/newaetech/sonata-pcb/
- https://github.com/newaetech/sonata-pcb/tree/main/sonata-one/sonata_kicad_project (more specifically)

KiCad benefits

- KiCad model allows for an interesting interactive BOM
- Fully open source



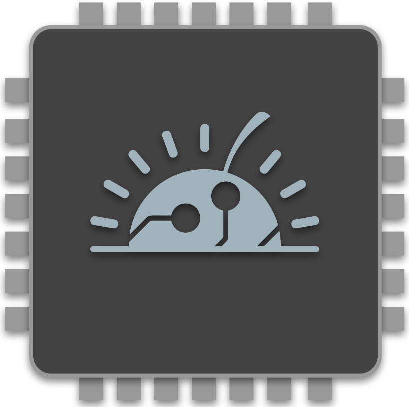
SONATA-ONE

Rev:
2024-07-05 10:30:01

	Sourced	Placed	References	Value	Supplier 1 Part Number	Quantity
1	☐	☐	C33, C34, C35, C36, C37, C38	22uF		6
2	☐	☐	C12, C50	2u2		2
3	☐	☐	C5	680uF		1
4	☐	☐	C51	100n		1
5	☐	☐	R7, R9, R20	10k		3
6	☐	☐	R8	2k2		1
7	☐	☐	R10	100k		1
8	☐	☐	R11	15k		1
9	☐	☐	R19	0R		1
10	☐	☐	L1, L2	4.7uH		2
11	☐	☐	D5, D8, D10, D12, D13, D16, D17, D18, D19, D20, D22, D23, D24, D25	LED, 0603, Red		14
12	☐	☐	D4, D7, D9, D11, D14, D15, D26, D27, D28	LED, 0603, Green		9
13	☐	☐	D3, D6	LED, 0603, Blue		2
14	☐	☐	U8, U10	RT8058		2

New! Sunburst Extension — CHERIoT SoC

- Based on success of Sonata to date, **UKRI** have agreed a **project extension**:
  - SCI Semi joined as project partners
  - lowRISC will provide open silicon IP and an open top level for integration by SCI into a commercial silicon design
  - Aim to migrate open repo to CHERI Alliance in time
  - SCI will manage proprietary IP, tapeout (22nm FDXSOI MPW)
- Will leverage formal verification work from Prof. Melham's group at the University of Oxford



lowRISC

SCI

UKRI Delivered by Innovate UK, EPSRC and ESRC

Digital Security by Design

The CHERI Alliance

Getting security embedded into electronic systems

John Thomson

lowRISC – Founding Member of the CHERI Alliance

Founding Members of the CHERI Alliance

CAPABILITIES LIMITED

CHEVIN™ TECHNOLOGY

Codasip

Critical technologies inc.
Trustworthy Networked Autonomy

CYNAM

[dstl]

FreeBSD FOUNDATION

Google

LMT 光濟科技股份有限公司
LIGHT MOMENTUM TECHNOLOGY CORP.
~ Light Your Life ! ~

lowRISC

National Cyber Security Centre
a part of GCHQ

OPENHW® GROUP
PROVEN PROCESSOR IP

PARVAT

SCI

SRI

Prifysgol Abertawe
Swansea University

TRUSTED COMPUTING
CENTER OF EXCELLENCE

TechWorks

UNIVERSITY OF BIRMINGHAM

UNIVERSITY OF CAMBRIDGE

University of Glasgow

CHERI Alliance and open source

- Intend to support and work very closely with open-source communities to port code to CHERI
- Aim to release our work in the open as much as possible
  - Open source for code, Creative Commons for documents
- Welcome open organisations (e.g. FreeBSD Foundation)
- CHERI Alliance is an independent, non-profit organisation
- Any individual can join for free
- Work collaboratively for the promotion of an open technology (CHERI)
- Support the standardisation work as part of RISC-V International

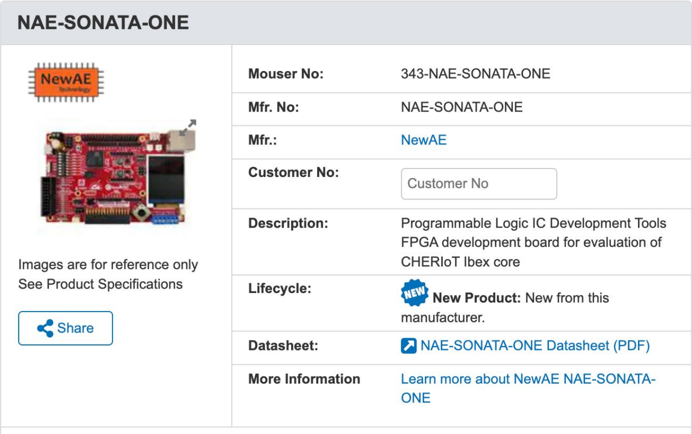
♡ Open Source

Boards are available to buy

- Boards are now available via Mouser internationally
- However with open source repos you can build your own!

tinyurl.com/sonata-int

Link also on the next slide

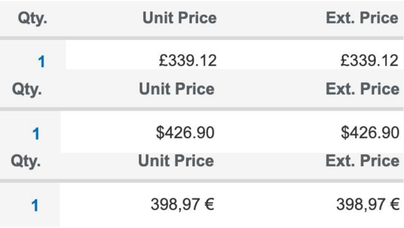


NAE-SONATA-ONE

Images are for reference only
See Product Specifications

Share

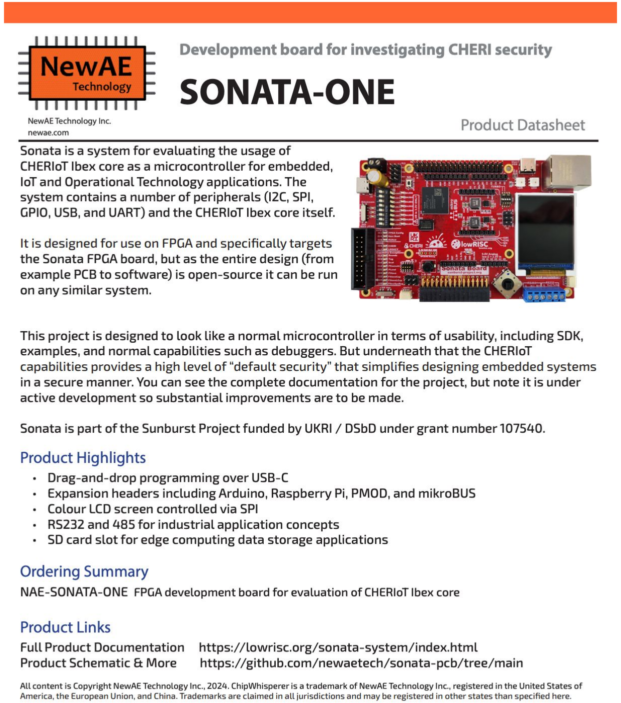
Mouser No:	343-NAE-SONATA-ONE
Mfr. No:	NAE-SONATA-ONE
Mfr.:	NewAE
Customer No:	Customer No
Description:	Programmable Logic IC Development Tools FPGA development board for evaluation of CHERIoT Ibex core
Lifecycle:	NEW **New Product:** New from this manufacturer.
Datasheet:	NAE-SONATA-ONE Datasheet (PDF)
More Information	Learn more about NewAE NAE-SONATA-ONE



Qty.	Unit Price	Ext. Price
1	£339.12	£339.12

Qty.	Unit Price	Ext. Price
1	$426.90	$426.90

Qty.	Unit Price	Ext. Price
1	398,97 €	398,97 €



NewAE Technology
NewAE Technology Inc.
newae.com

Development board for investigating CHERI security

SONATA-ONE

Product Datasheet

Sonata is a system for evaluating the usage of CHERIoT Ibex core as a microcontroller for embedded, IoT and Operational Technology applications. The system contains a number of peripherals (I2C, SPI, GPIO, USB, and UART) and the CHERIoT Ibex core itself.

It is designed for use on FPGA and specifically targets the Sonata FPGA board, but as the entire design (from example PCB to software) is open-source it can be run on any similar system.

This project is designed to look like a normal microcontroller in terms of usability, including SDK, examples, and normal capabilities such as debuggers. But underneath that the CHERIoT capabilities provides a high level of "default security" that simplifies designing embedded systems in a secure manner. You can see the complete documentation for the project, but note it is under active development so substantial improvements are to be made.

Sonata is part of the Sunburst Project funded by UKRI / DSbD under grant number 107540.

Product Highlights

- Drag-and-drop programming over USB-C
- Expansion headers including Arduino, Raspberry Pi, PMOD, and mikroBUS
- Colour LCD screen controlled via SPI
- RS232 and 485 for industrial application concepts
- SD card slot for edge computing data storage applications

Ordering Summary

NAE-SONATA-ONE FPGA development board for evaluation of CHERIoT Ibex core

Product Links

Full Product Documentation	https://lowrisc.org/sonata-system/index.html
Product Schematic & More	https://github.com/newaetech/sonata-pcb/tree/main

Thank you for your time

Questions / Answers

tinyurl.com/sonata-int

UKRI Delivered by Innovate UK, EPSRC and ESRC

Digital Security by Design

https://www.dsbd.tech

CHERI Alliance Founder

https://cheri-alliance.org

sunburst-project.org

lowRISC

john.thomson@lowrisc.org
info@lowrisc.org

https://lowrisc.org

opentitan

https://opentitan.org