OpenTitan®

Past, Present & Future of Open Secure Silicon

Dominic Rizzo

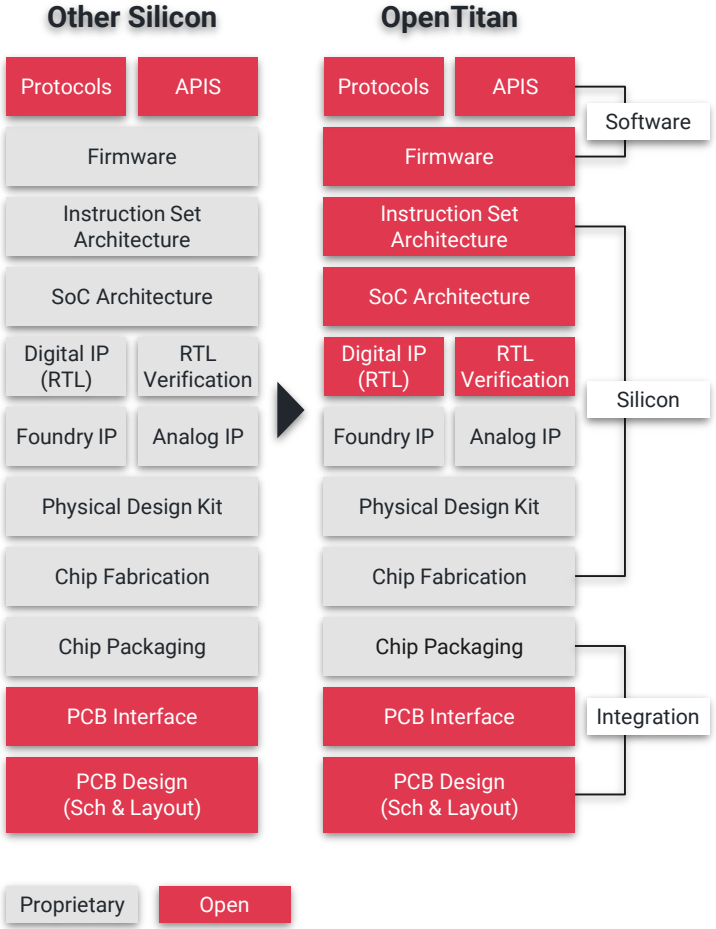
zeroRISC Inc. CEO
OpenTitan Project Director

domrizzo@zerorisc.com
domrizzo@opentitan.org

June 7th, 2023

The world's most active open-source silicon project

- @ RTL Freeze, chip-in-hand 2023, integrated upstream by EoY
- Transparent, flexible, high quality ecosystem – a resilient and growing coalition of partners
- This talk: the past, present and future of open secure silicon



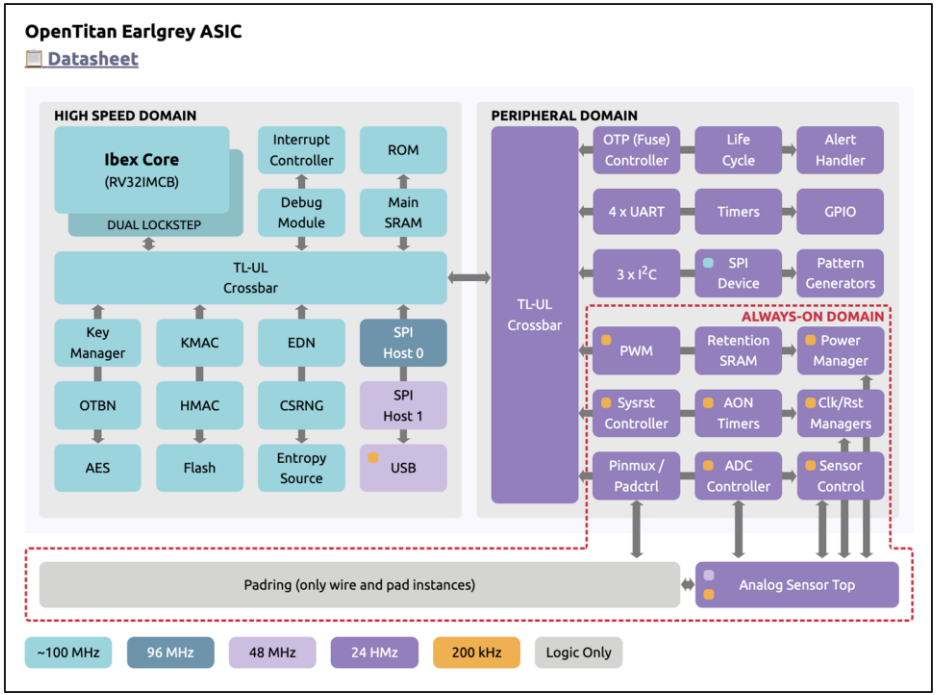
Past: Building an Open Silicon Coalition

Key OpenTitan Milestones

- ~2018 Silicon Transparency Working Group chartered: lowRISC, Google & ETH Zürich
- Feb 2019 – First definition of **Comportable IP**; first use of **standard, auto-gen'd documentation**
- Jun 2019 – **SystemVerilog style guide** defined
- Jun 2019 – OpenTitan **Technical Charter** defines Steering Committee, Technical Committee roles
- ~July 2019 OpenTitan chartered: Silicon, Security & Software Working Groups established
- Aug 2019 – **Continuous Integration** running on every pull request
- Oct 2019 – Structured **Hardware Development Milestones** defined
- Nov 2019 – Public launch of the OpenTitan repository
- …
- Oct 2020 – Continuous Integration extended to include **running tests on FPGA**
- July 2022 - Integrated WG chartered
- July 2022 – regular **Silicon Commons training** for new starters established
- May 2023 – Silicon Commons delivers: open-source chip with 35+ IPs developed by 140 contributors from 10 partners enables 2023 Engineering Sample tapeout with RTL freeze
- Ongoing – 10 partner organizations actively contribution to discrete and integrated top-level development

OpenTitan Discrete: the “Earl Grey” Top-Level

- RV32IMCB RISC-V "Ibex" core:
  - 3-stage pipeline, single-cycle multiplier
  - Selected subset of the bit-manipulation extension
  - 4kB instruction cache with 2 ways
  - RISC-V compliant JTAG DM (debug module)
  - PLIC (platform level interrupt controller)
  - U/M (user/machine) execution modes
  - Enhanced Physical Memory Protection (ePMP)
  - Security features:
    - Low-latency memory scrambling on the icache
    - Dual-core lockstep configuration
    - Data independent timing
    - Dummy instruction insertion
    - Bus and register file integrity
    - Hardened PC
- Security peripherals:
  - AES-128/192/256 with ECB/CBC/CFB/OFB/CTR modes
  - HMAC / SHA2-256
  - KMAC / SHA3-224, 256, 384, 512, [c]SHAKE-128, 256
  - Programmable big number accelerator for RSA and ECC (OTBN)
  - NIST-compliant cryptographically secure random number generator (CSRNG)
  - Digital wrapper for analog entropy source with FIPS and CC-compliant health checks
  - Key manager with DICE support
  - Manufacturing life cycle manager
  - Alert handler for handling critical security events
  - OTP controller with access controls and memory scrambling
  - Flash controller with access controls and memory scrambling
  - ROM and SRAM controllers with low-latency memory scrambling
- Memory:
  - 2x512kB banks eFlash
  - 128kB main SRAM
  - 4KB Always ON (AON) retention SRAM
  - 32kB ROM
  - 2kB OTP
- IO peripherals:
  - 47x multiplexable IO pads with pad control
  - 32x GPIO (using multiplexable IO)
  - 4x UART (using multiplexable IO)
  - 3x I2C with host and device modes (using multiplexable IO)
  - SPI device (using fixed IO) with TPM, generic, flash and passthrough modes
  - 2x SPI host (using both fixed and multiplexable IO)
- Other peripherals:
  - Clock, reset and power management
  - Fixed-frequency timer
  - Always ON (AON) timer
  - Pulse-width modulator (PWM)
  - Pattern Generator
- Software:
  - Boot ROM code implementing secure boot and chip configuration
  - Bare metal applications and validation tests



[Greg Chadwick, 6/8 @ 16:30: “ Building commercially relevant open source silicon: The many aspects of Ibex”]

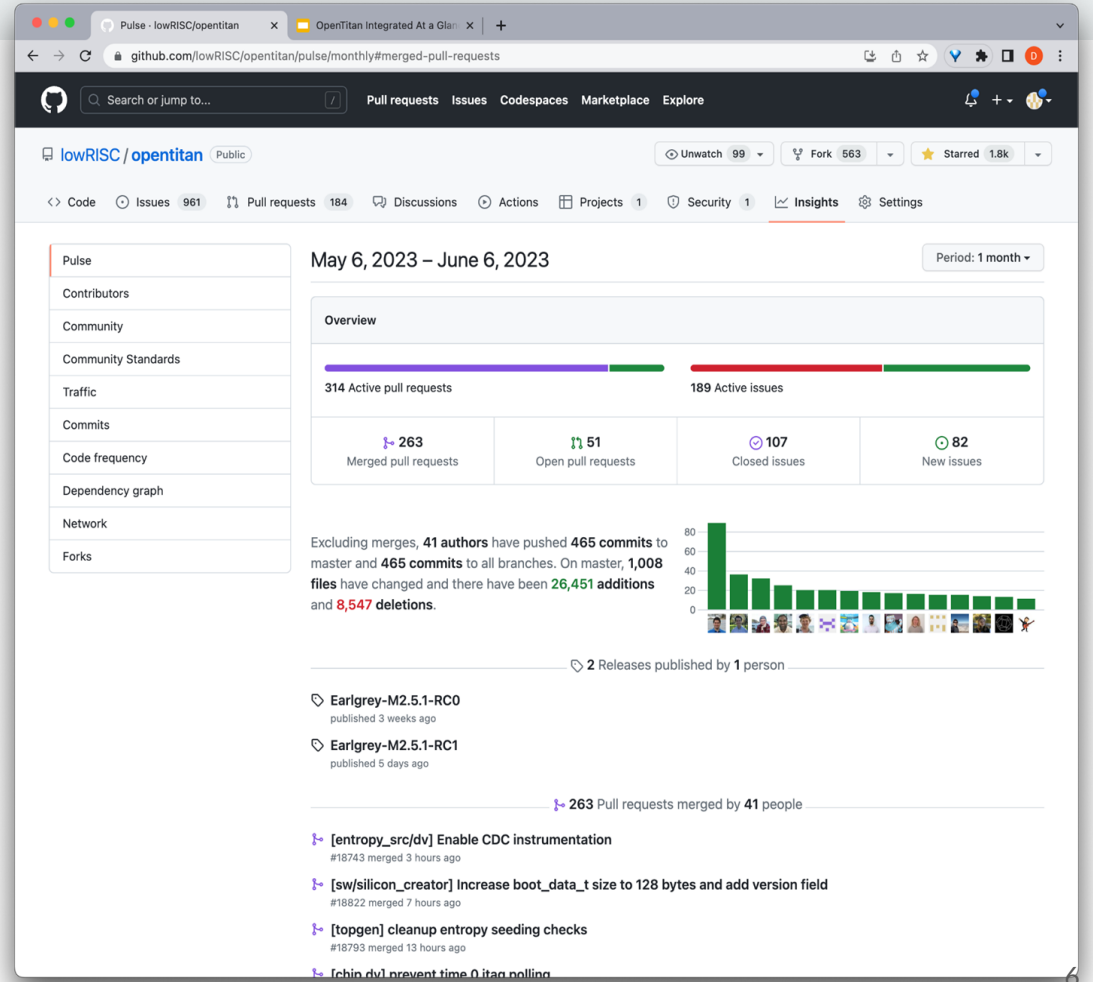
Individual Contributors

Monthly

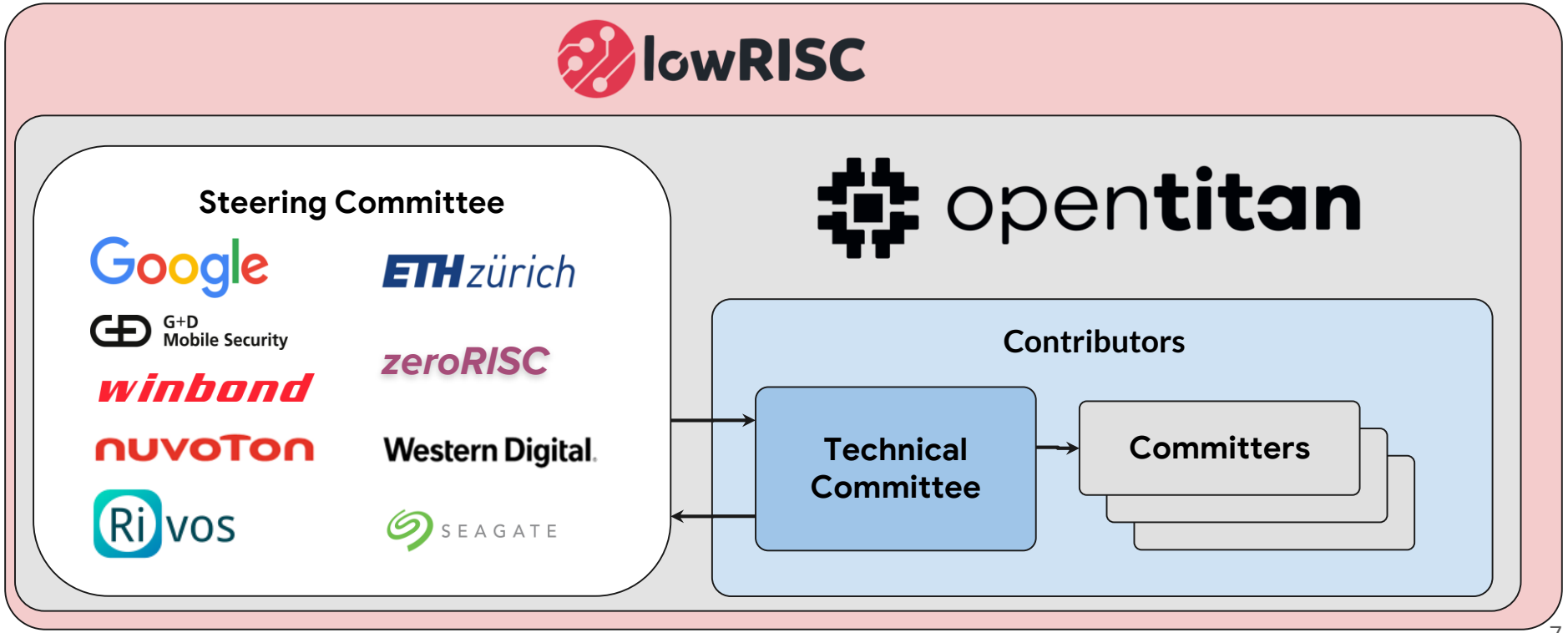
- ~10 organizations
- 40+ contributors
- 100s of commits, issues, PRs
- 1000s of file changes
- 10,000s of individual edits

5+ Years (chartered 2018)

- 140+ unique contributors
- 13k merged PRs
  - 20k commits
- 1.5M LoC (0.5M HDL)



Organizational Partners



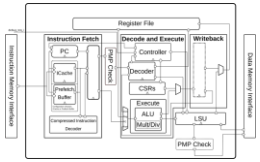
Problem: *Scalable* Open Silicon Development

one skilled engineer

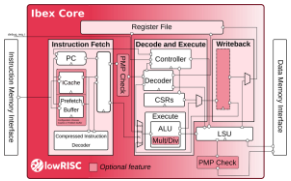
a team of engineers

multiple teams
of engineers

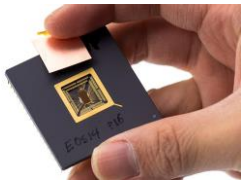
multiple organizations
with multiple teams



to develop a RISC-V core and open-source it



to verify the core and bring it to commercial maturity



to design a chip around the core and deliver it to customers

opentitan

to develop and maintain the RTL, DV, firmware, & infrastructure for a complete open silicon ecosystem

Need to get quality, collaboration and consensus right – from the start

Solution: The Silicon Commons

Collateral

- Extensive website
- Comportability
- Block documentation
- Top-level datasheet(s)
- Getting started guide(s)
- Open silicon partner training sessions and material
- How-to contribute guides
- …

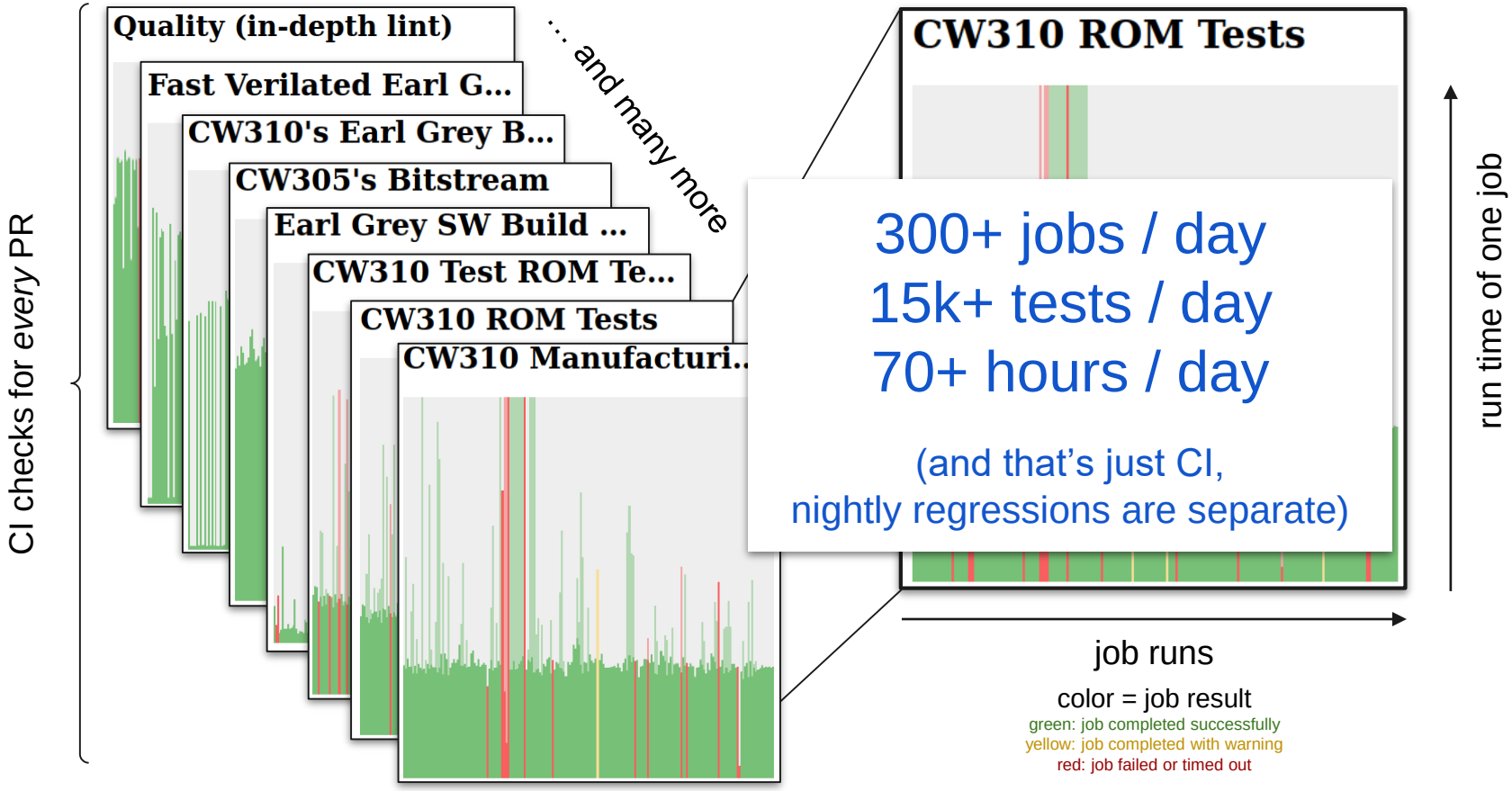
Technology

- Automated code templating and documentation generation
- Continuous integration
- Nightly regressions
- FPGA farm
- NewAE's CW310, CW340 development platforms
- Hyperdebug & *opentitantool*
- …

Processes

- Governance: SC, WGs, TC, Committers, PD
- Hardware development stages
- RFC process
- Yearly roadmap
- Tapeout Tech Leads
- On-call regression triage
- Certification-sensitive NDAs
- Trademark policy
- …

Silicon Commons: CI is a *massive* component

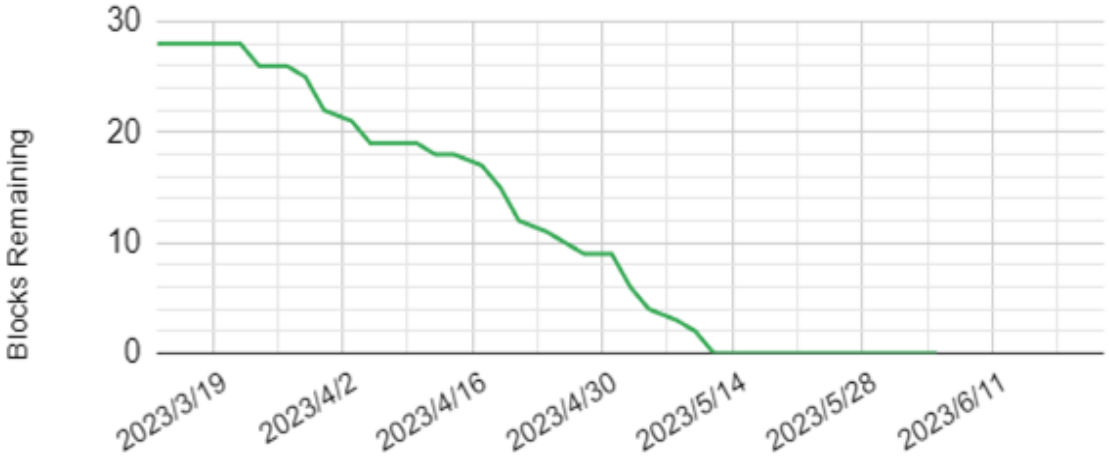


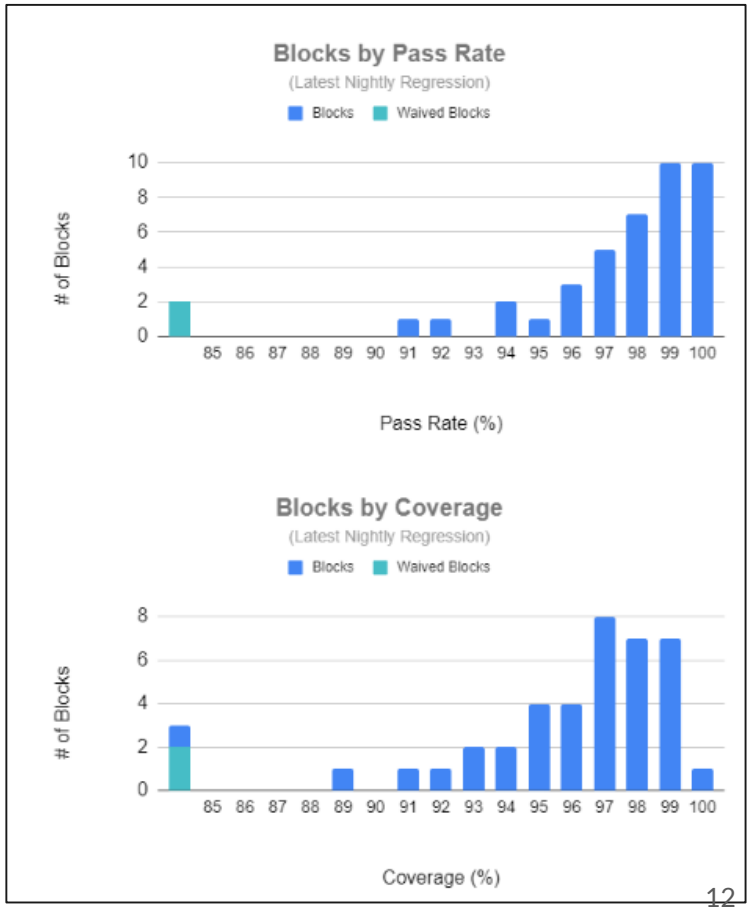
Present: Commercial Silicon

Discrete Shuttle RTL Freeze

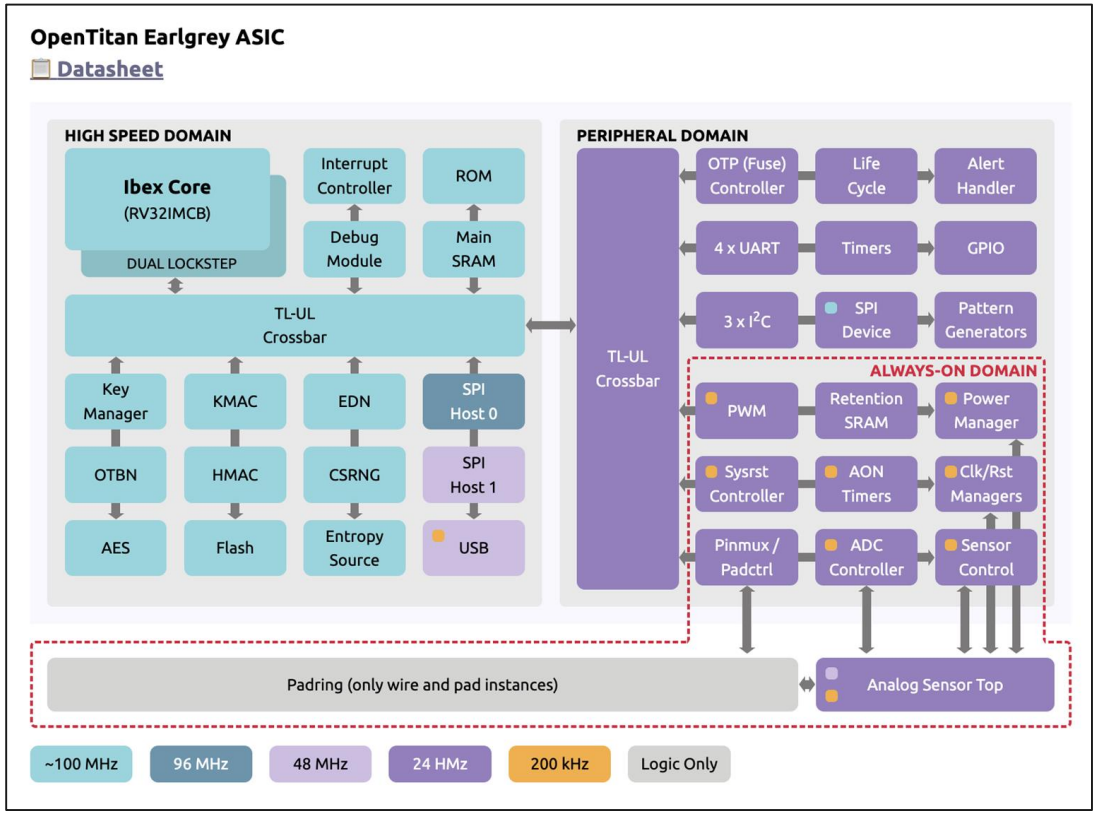
Burndown: IP Blocks to M2.5

- >90% on nightlies + >90% coverage

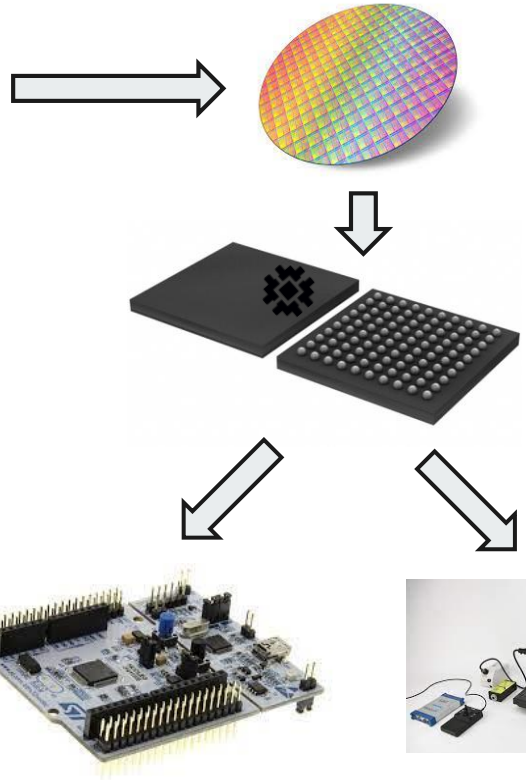




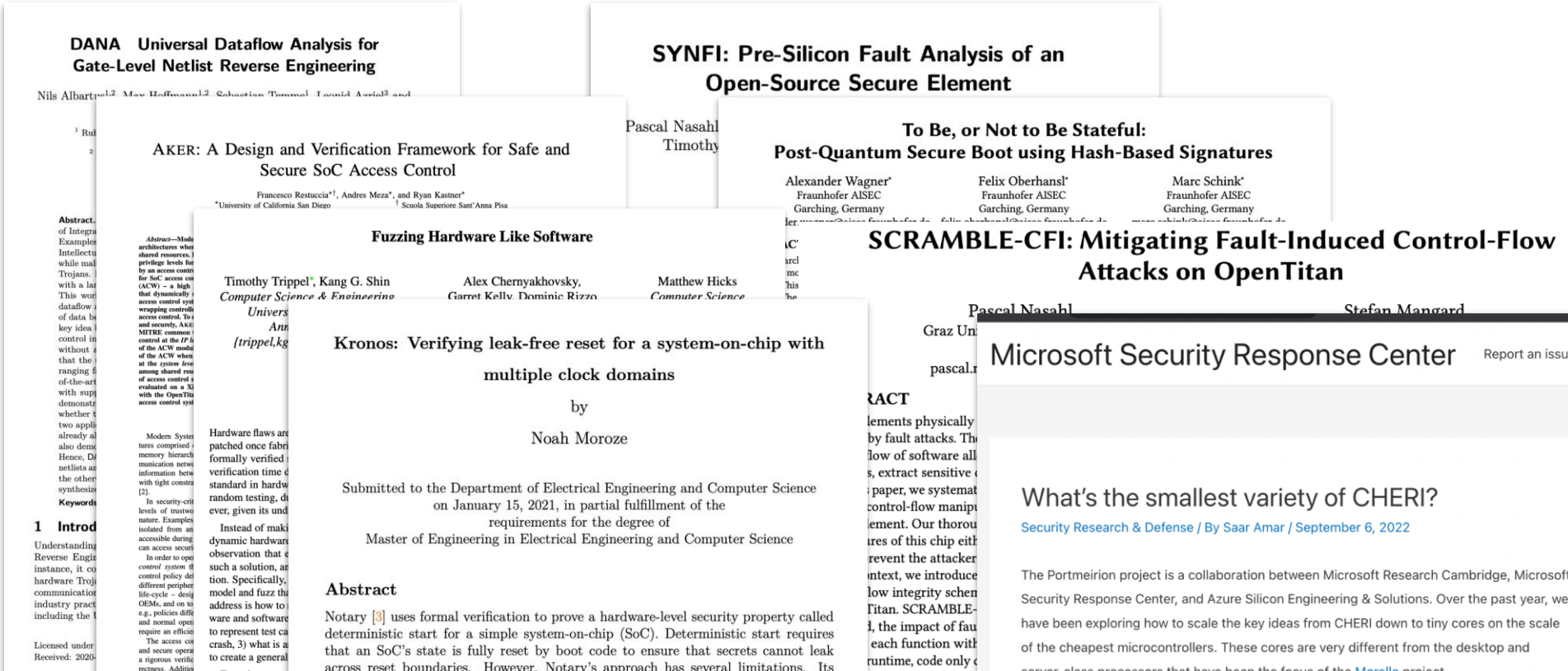
Tapeout and Engineering Sample Silicon



Discrete Engineering Samples August ‘23



OpenTitan as an Ecosystem Platform



DANA Universal Dataflow Analysis for Gate-Level Netlist Reverse Engineering

SYNFI: Pre-Silicon Fault Analysis of an Open-Source Secure Element

AKER: A Design and Verification Framework for Safe and Secure SoC Access Control

To Be, or Not to Be Stateful: Post-Quantum Secure Boot using Hash-Based Signatures

Fuzzing Hardware Like Software

SCRAMBLE-CFI: Mitigating Fault-Induced Control-Flow Attacks on OpenTitan

Kronos: Verifying leak-free reset for a system-on-chip with multiple clock domains

by

Noah Moroze

Submitted to the Department of Electrical Engineering and Computer Science
on January 15, 2021, in partial fulfillment of the
requirements for the degree of
Master of Engineering in Electrical Engineering and Computer Science

Abstract

Notary [3] uses formal verification to prove a hardware-level security property called deterministic start for a simple system-on-chip (SoC). Deterministic start requires that an SoC's state is fully reset by boot code to ensure that secrets cannot leak across reset boundaries. However, Notary's approach has several limitations. Its

Microsoft Security Response Center

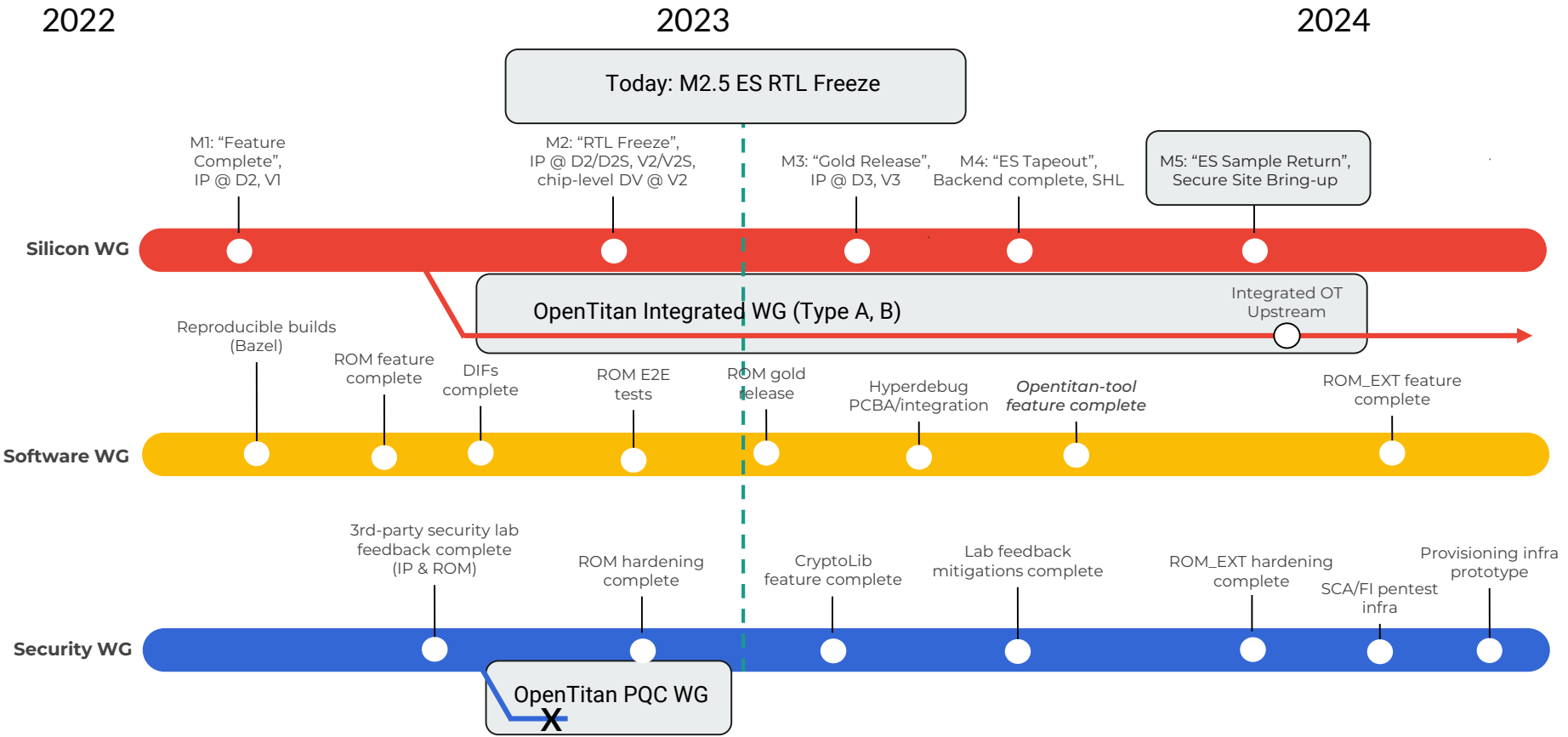
What's the smallest variety of CHERI?

Security Research & Defense / By Saar Amar / September 6, 2022

The Portmeirion project is a collaboration between Microsoft Research Cambridge, Microsoft Security Response Center, and Azure Silicon Engineering & Solutions. Over the past year, we have been exploring how to scale the key ideas from CHERI down to tiny cores on the scale of the cheapest microcontrollers. These cores are very different from the desktop and

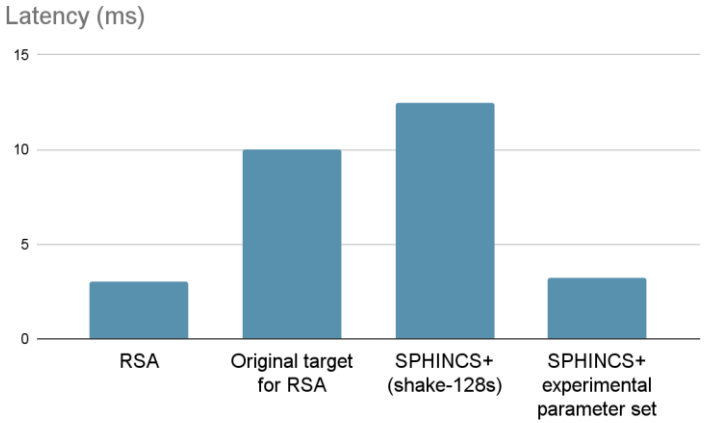
Future: A Design Ecosystem

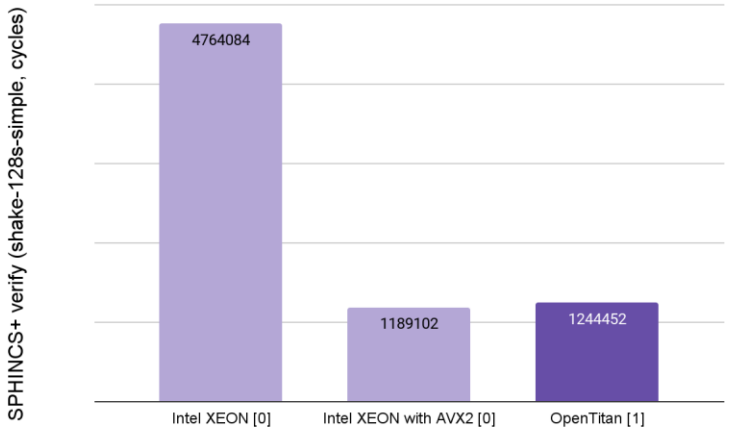
OpenTitan Project Roadmap



SPHINCS+ Verified Boot in ROM

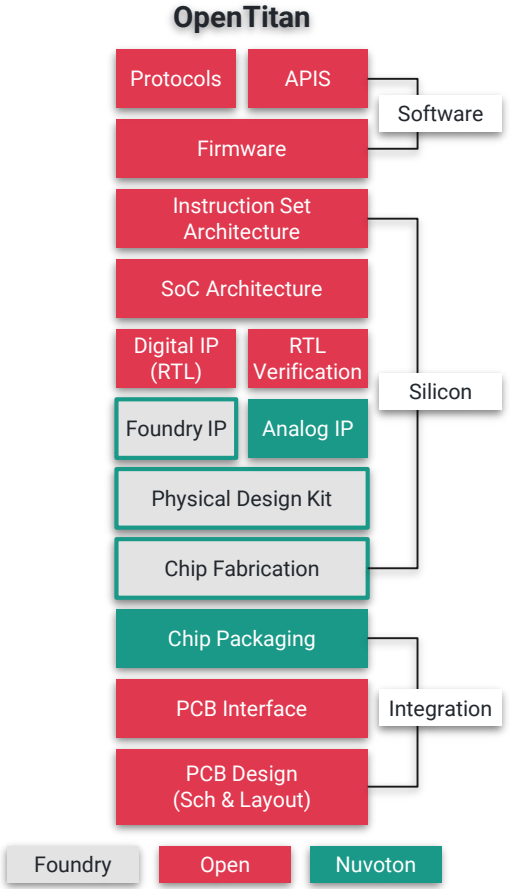
- TC approved Jan 2023, implementation complete May 2023
- HSM integration for Eng Sample discrete silicon
- Full L1 security parameters; ~12ms verification
- E2E & SPX+ reference test suites
- Hardware accelerated, hardened implementation



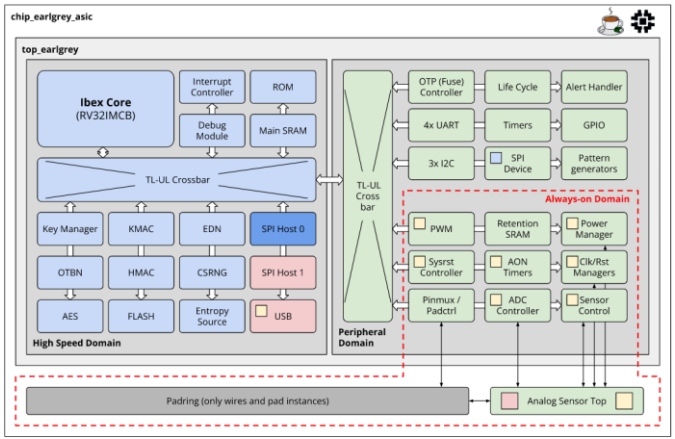


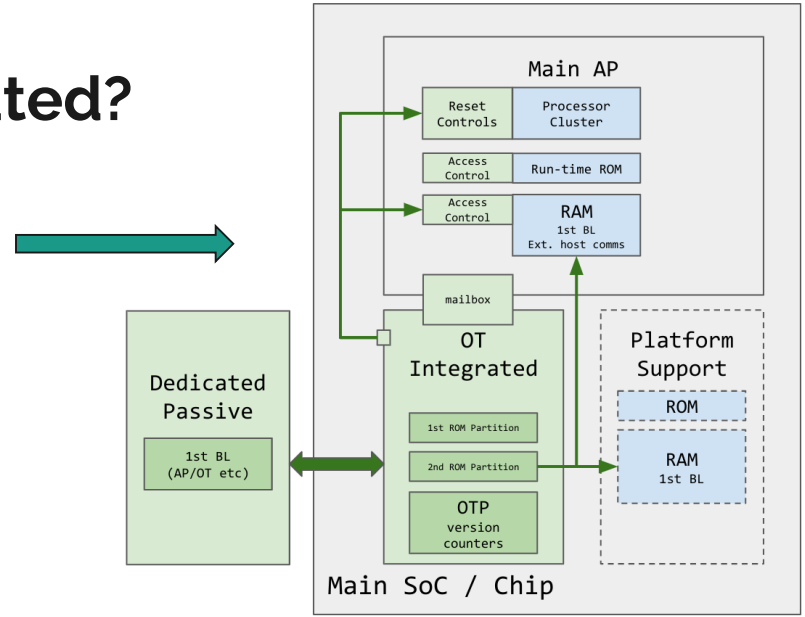
Commercial Tapeout: Nuvoton

- Experienced TPM vendor
- Responsible for turning a commercial-quality design into a commercially relevant chip: analog components, security sensors and countermeasures; abstracted through AST, secure manuf. and bring-up
- Aligned w/ certification requirements, inc. MSSR site
- Manages the tapeout process w/ the foundry
- Partners w/ OpenTitan partners like lowRISC, Google and zeroRISC on final integration and test



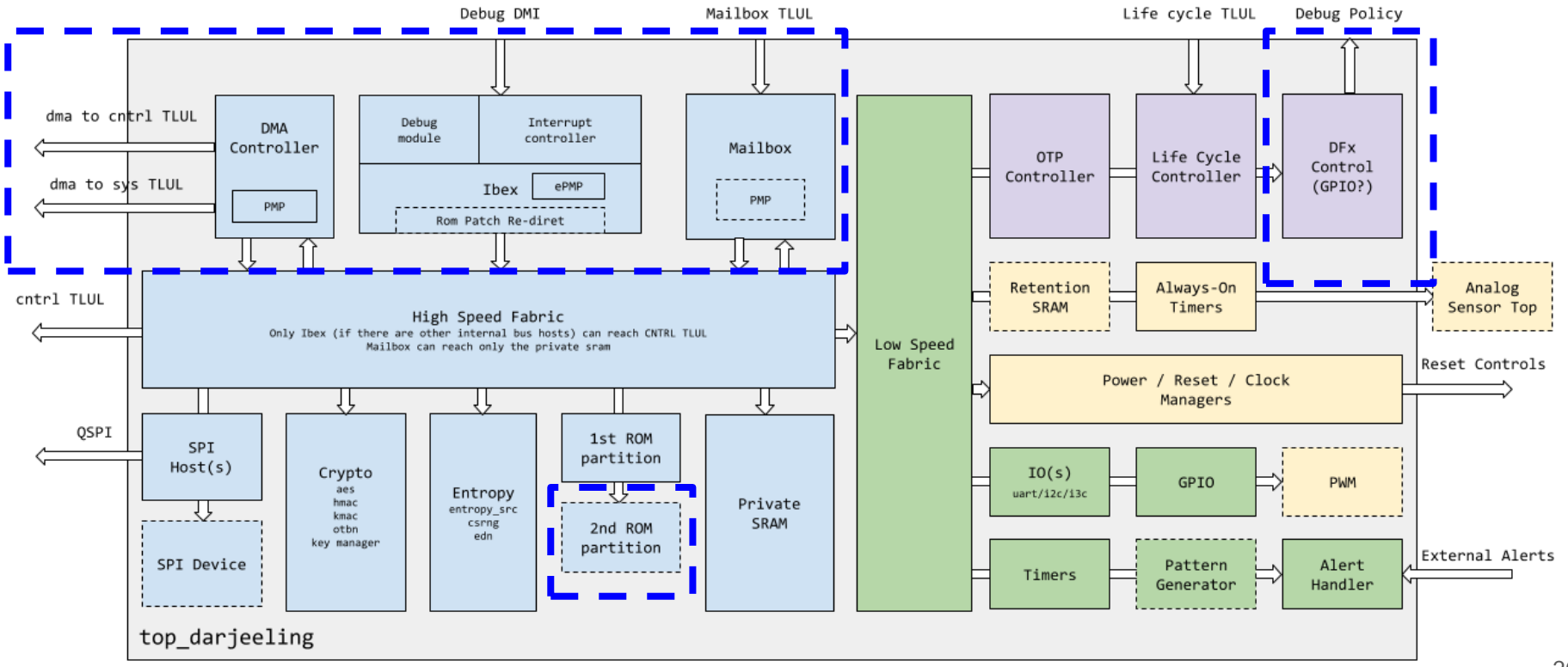
What Is OpenTitan Integrated?





- 1st new formal Working Group since project start
- Adapting the OpenTitan IP ecosystem a larger SoC's secure subsystem
- *Not a single design*; SoC integration is highly variable: chiplets, mobile, consumer, IoT, IIoT, etc.
- Certification alignment: FIP 140-3 and PP-0117

Integrated OT RoT (Type A): “Darjeeling” Top-Level



Q & A

Key Takeaways

- Discrete design is done
- Eng Sample silicon this year
- Integrated upstream this year
- Scalable development model
- Broadly adopted ecosystem of IP