barkhausen institut

M³ Platform Architecture
Fast-track Trustworthy Tape-outs

Barkhausen Institut

Michael Raitza

2026-06-22

Establishing trust

Invariants

Every system you **use forces** you to **trust** it!

Security roots in understanding

Problem

Complexity biggest **opponent** of **security**

Establishing trust

Solution

Modularise systems
Simplify communications
Isolate components

Effect

Isolation provides **relief from trust**

Consequence

Establish trust in a **large system** by isolating users into **small** trusted computing bases (**TCBs**)

Silicon-proofing IP

Suppose **you**:

- want your IP silicon-proven

You **need**:

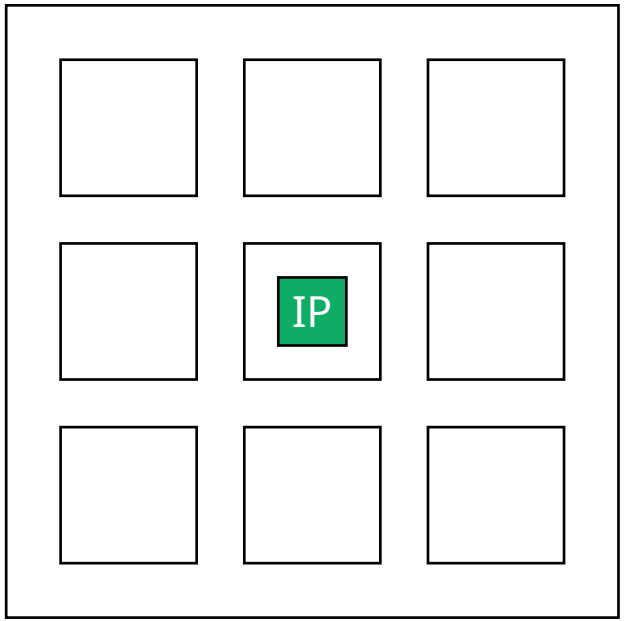
- a demonstrator / show-case

Your **expertise**:

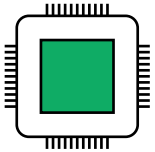
- digital front-end design (ASIC / FPGA)

Silicon-proofing IP

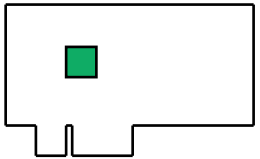
Chip



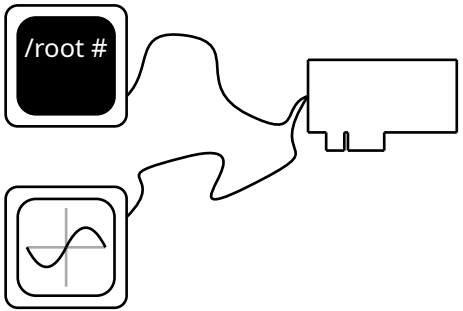
Package



Board



Demonstrator



Silicon-proofing IP

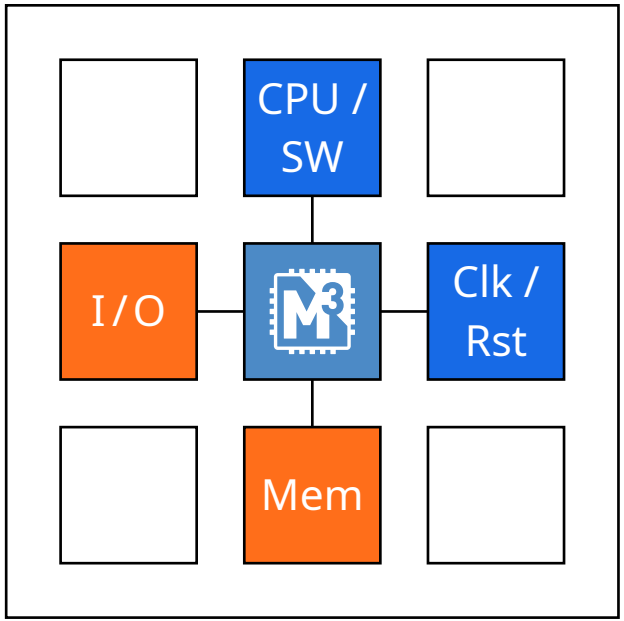
Likely not an expert in any of these!

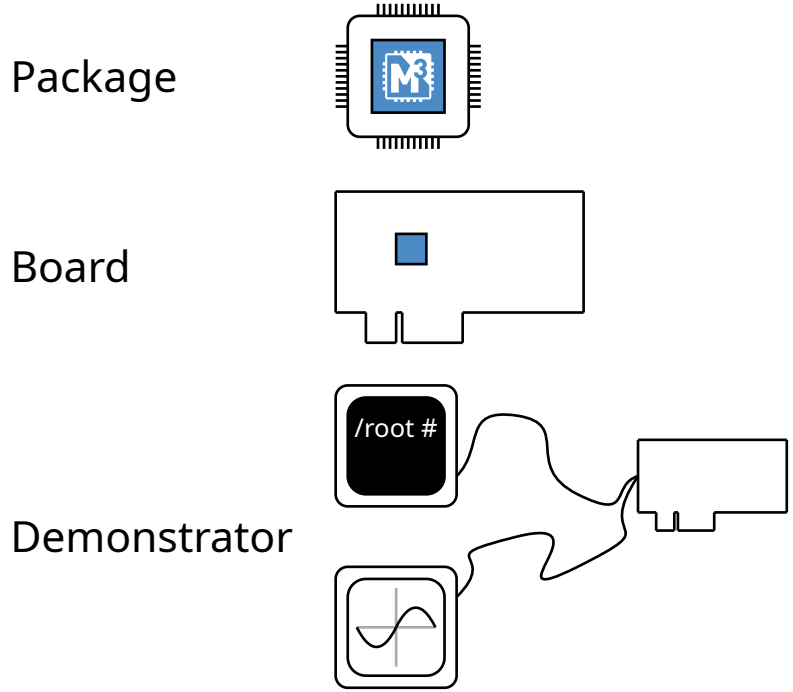
Anyhow:

Silicon-proofing IP is **time-consuming** and **expensive**.

Silicon-proofing IP

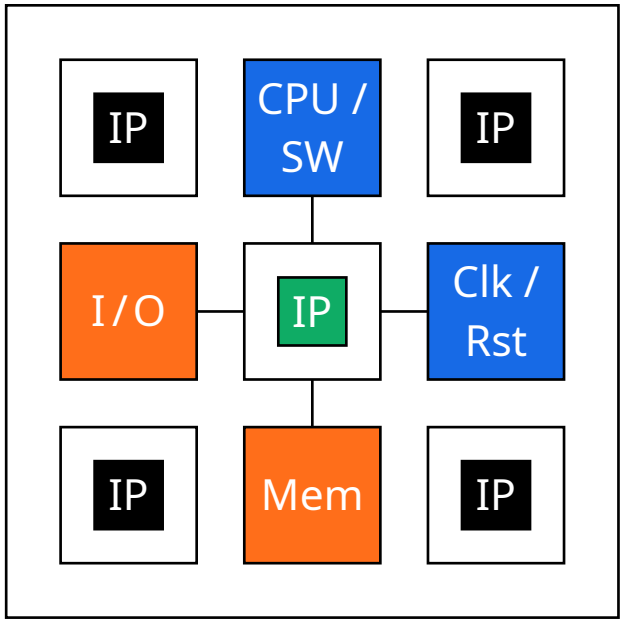
Masur tape-out platform





Silicon-proofing IP

M^3 platform architecture

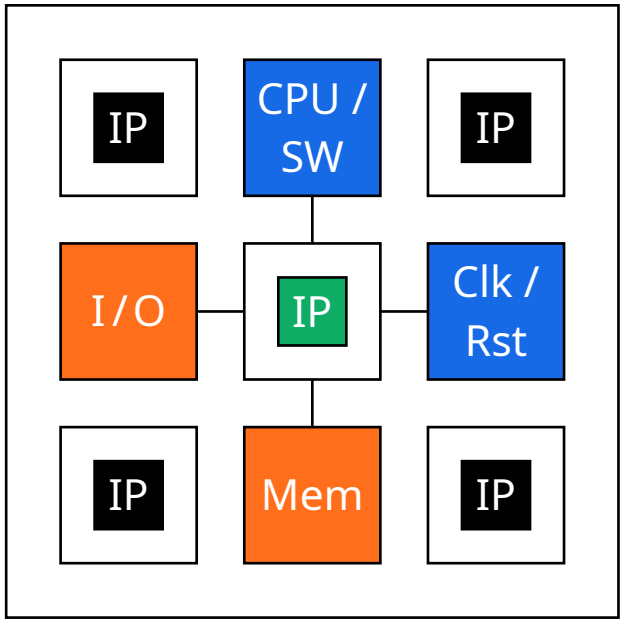


Multi-IP tape-outs
- cost sharing
- richer platform

Strong **HW isolation**
- resilience against faulty IP
- HW-enforced runtime access control

Silicon-proofing IP

M³ platform architecture



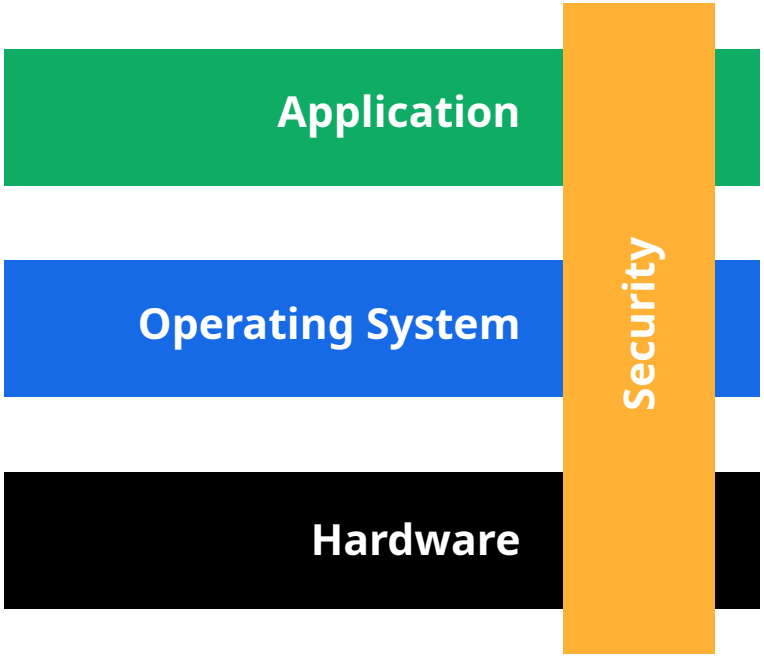
Multi-IP tape-outs
- cost sharing
- richer platform

Strong **HW isolation**
- resilience against faulty IP
- HW-enforced runtime access control

HW / SW co-design with **M³ OS**
- µ-kernel-based OS
- no runtime overhead
  (apps run bare-metal)

M³ platform architecture concept

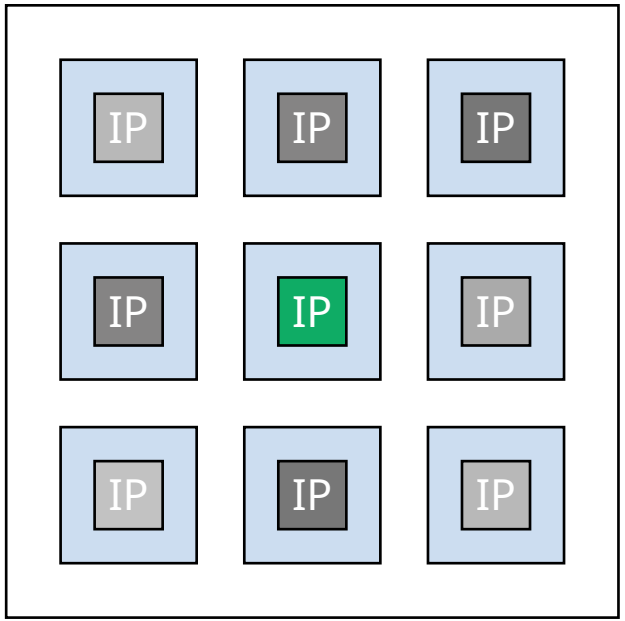
Strong isolation



Goal: Minimize HW and SW
Trusted Computing Base

M³ platform architecture

Chip topology



Fully-tiled spatial architecture

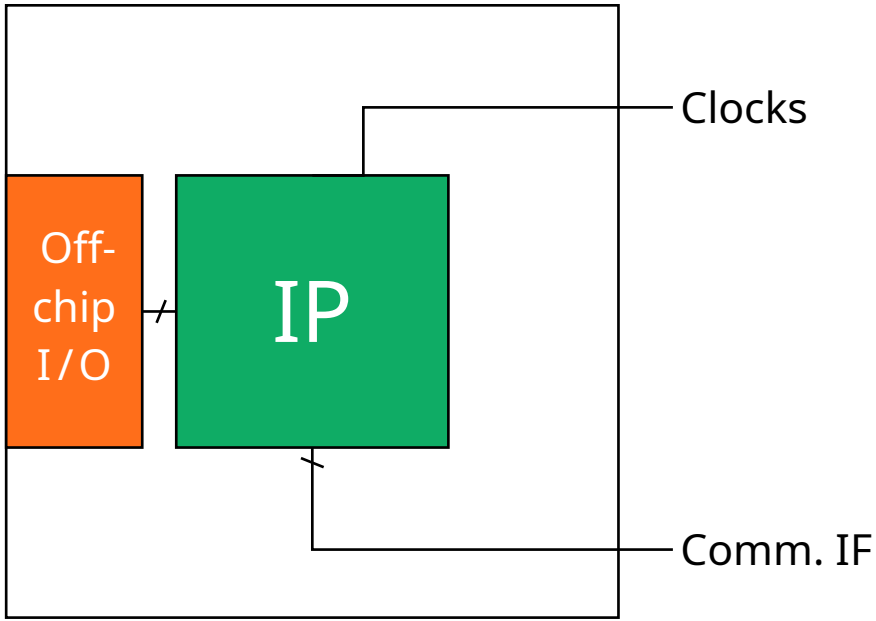
- no inherent hierarchy
- **double-tile** layout

Enables specification of:

- **clock boundary**
- interface
- communication protocol

M³ platform architecture

Tile topology



M³ defines interfaces

- clocks
- internal communication

You are controlling

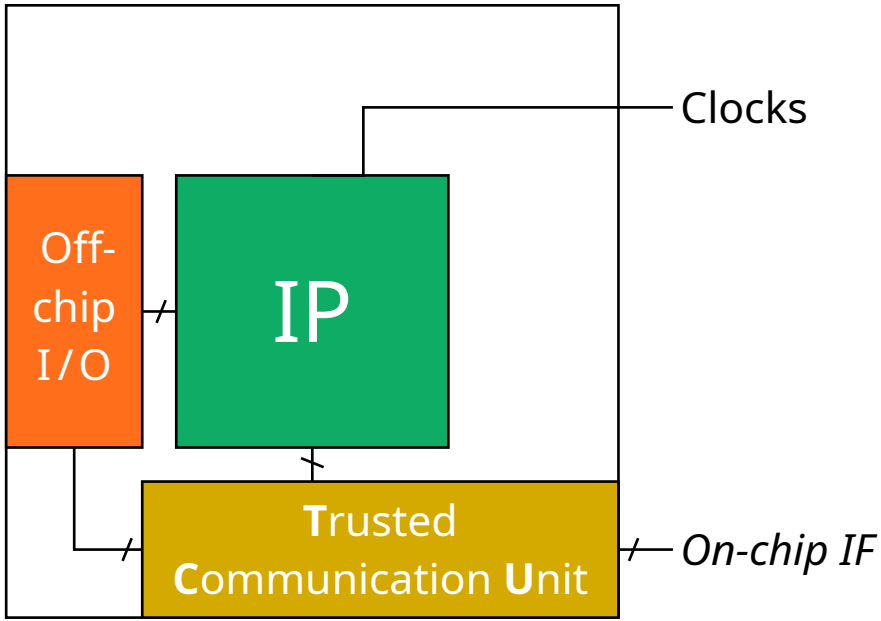
- **green box**

We are consenting

- off-chip I/O

M³ platform architecture

Tile isolation

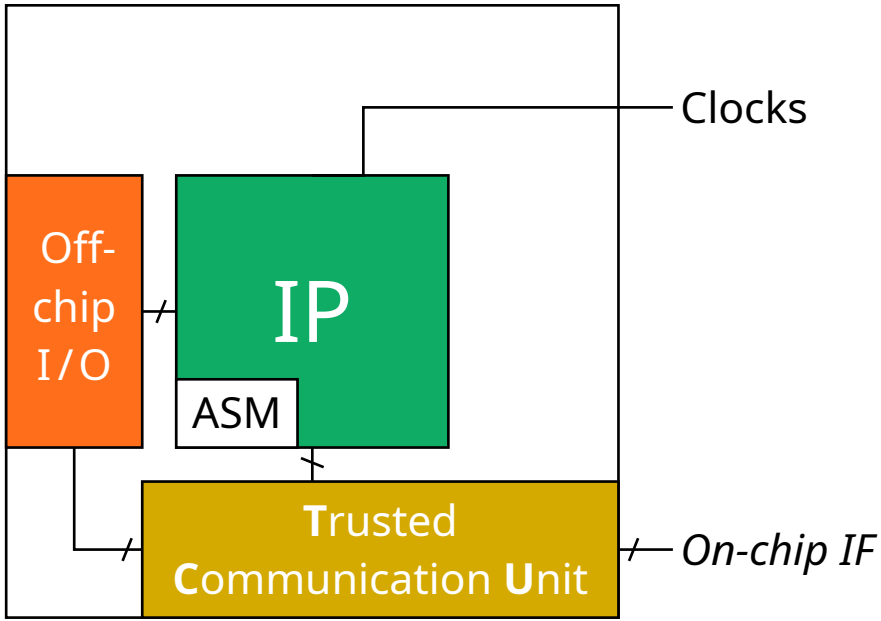


TCU – prime security IP

- sole on-chip interface
- controlling off-chip I/O
- decouples interfaces:
  - IP vs. on-chip

M³ platform architecture

Tile isolation



TCU – prime security IP

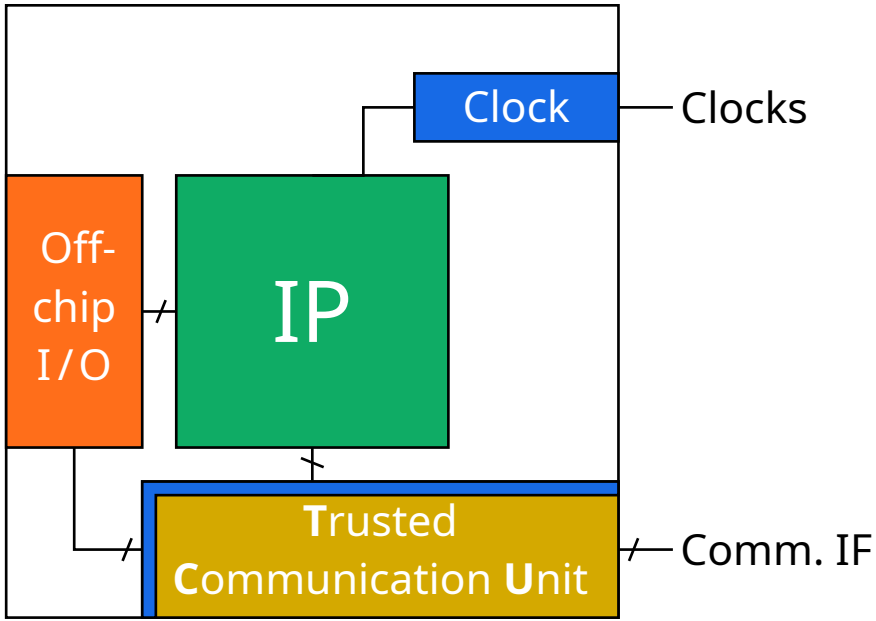
- sole on-chip interface
- controlling off-chip I/O
- decouples interfaces:
  - IP vs. on-chip

M³ convenience soft-IP

- Accelerator Support Module (pico RISC-V + SRAM)

M³ platform architecture

Clock domain separation



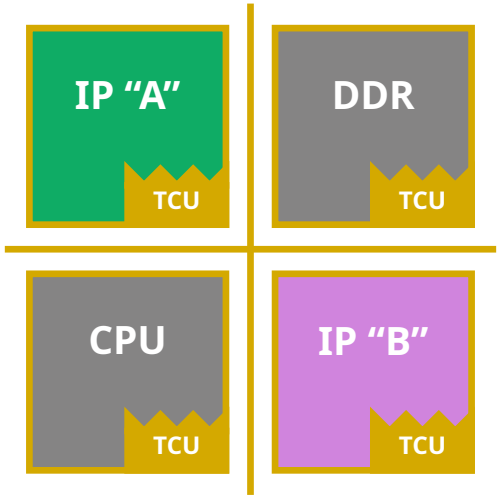
Clock separation
- use your own PLL (optional)
- CDC in IP-to-TCU IF

- failure confinement

Support for your **hard-IP**
- digital
- mixed-signal
- analog

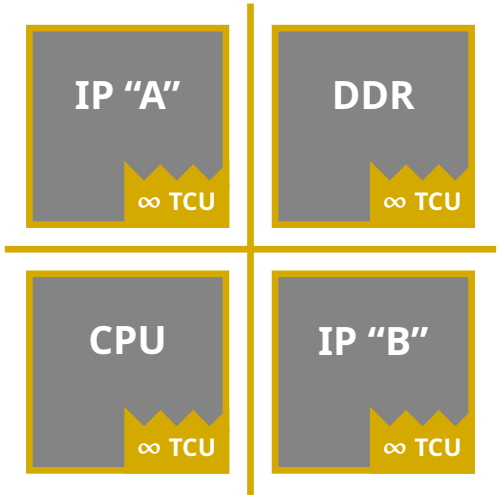
Multi-IP tape-outs

Reducing trusted computing bases



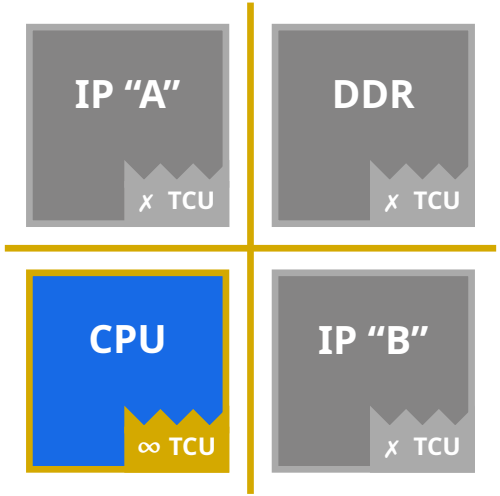
Multi-IP tape-outs

Reducing trusted computing bases



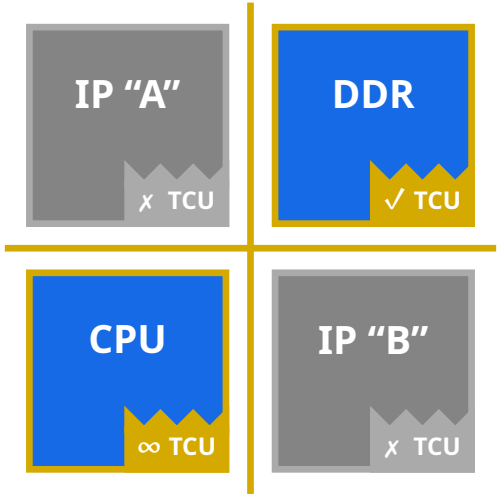
Multi-IP tape-outs

Reducing trusted computing bases



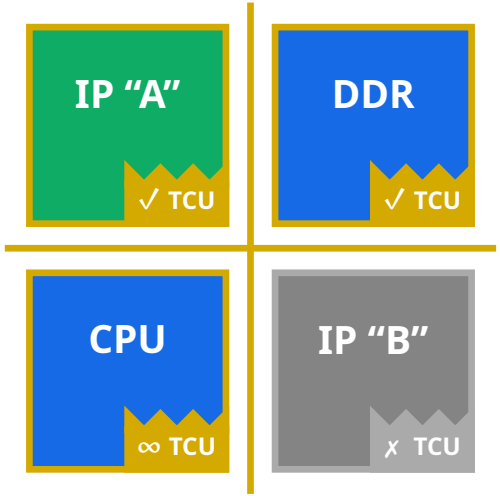
Multi-IP tape-outs

Reducing trusted computing bases



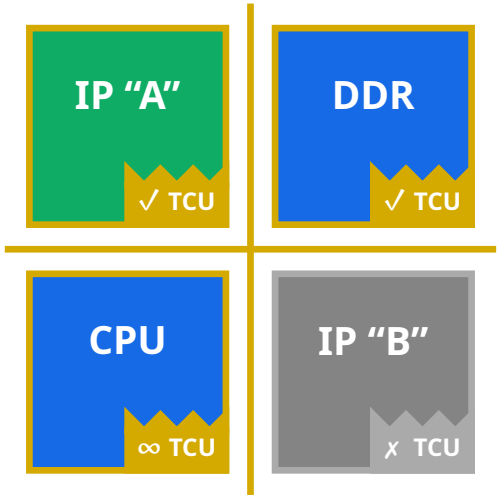
Multi-IP tape-outs

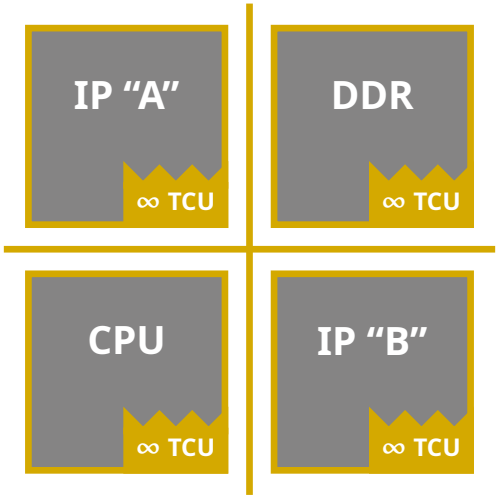
Reducing trusted computing bases



Multi-IP tape-outs

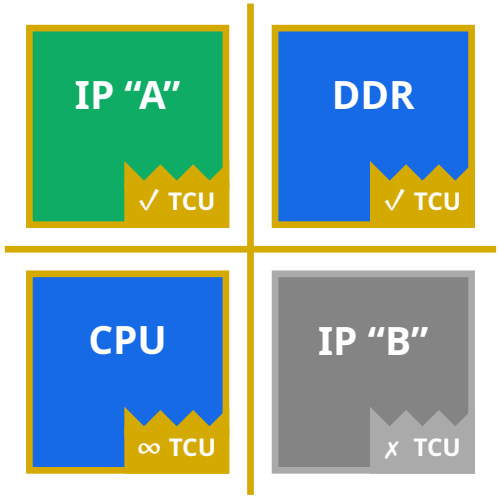
Reducing trusted computing bases

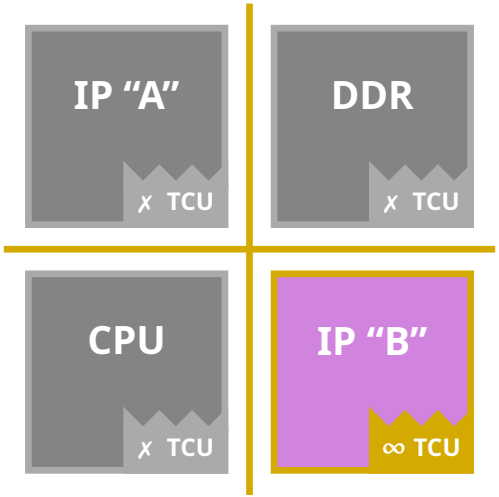




Multi-IP tape-outs

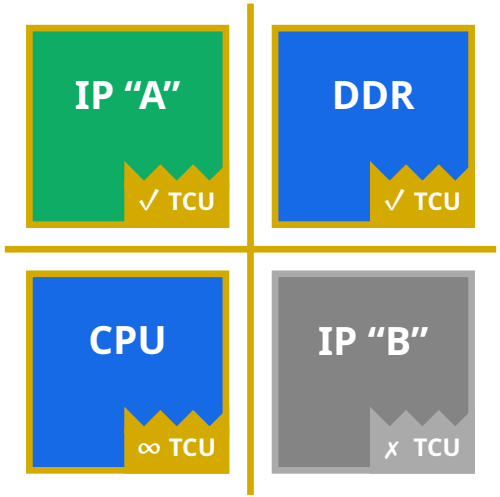
Reducing trusted computing bases

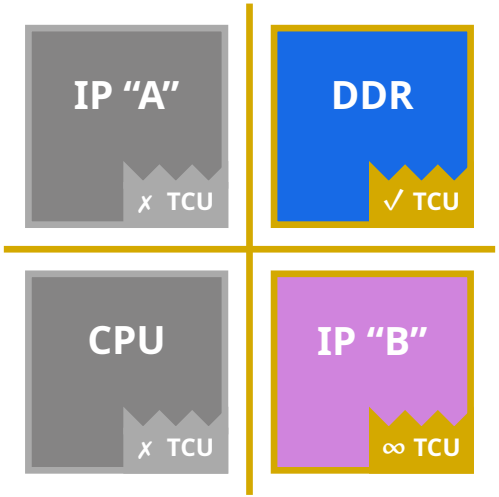




Multi-IP tape-outs

Reducing trusted computing bases





Multi-IP tape-outs

Reducing trusted computing bases

Application “A” and “B” work **without mutual trust!**

Trusted Communication Unit (TCU)

Modularising isolation

- agnostic to on-chip interface

- **M³ architecture poses some requirements**

deadlock-freedom	→ at least 1 message acceptable
no stalling	→ receiver *pays* for **timeliness**
livelocking	→ sender *pays* for **success**
size-bounded messages	

Trusted Communication Unit (TCU)

Features

HW interfaces

- in-house network-on-chip
- FlooNoC

Trusted Communication Unit (TCU)

Features

HW interfaces

- in-house network-on-chip
- FlooNoC

Transmission protocols

- message passing
- direct memory access
- virtual addressing / memory protection
- cache-coherent memory access

Trusted Communication Unit (TCU)

Features

HW interfaces

- in-house network-on-chip
- FlooNoC

Transmission protocols

- message passing
- direct memory access
- virtual addressing / memory protection
- cache-coherent memory access

Security

- source-controlled access control
- IP-independent security capabilities

Masur 26 chip (*currently in production*)

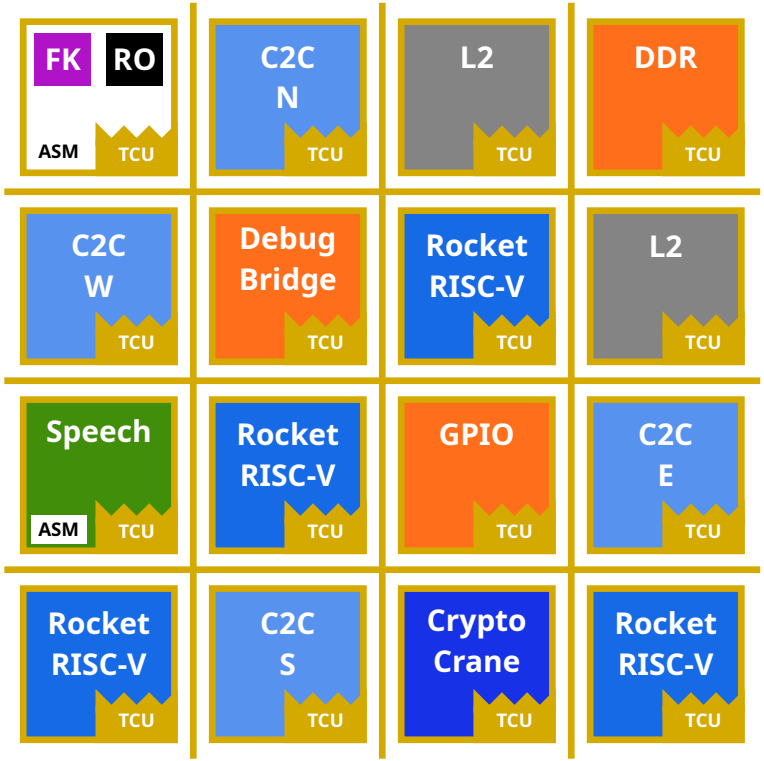
4th Masur platform tape-out

4th TCU version (open source)

9 months development

1st package re-use

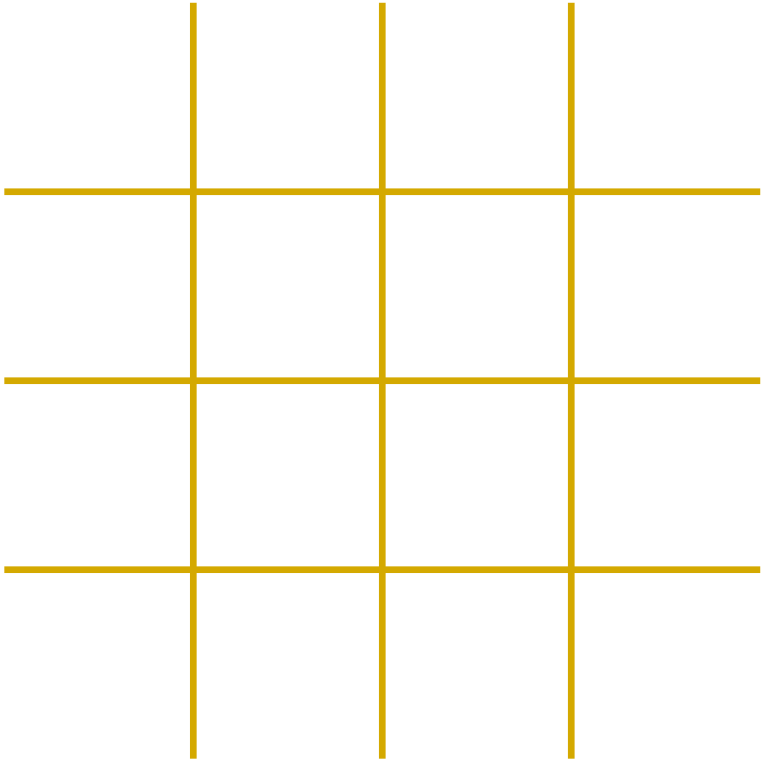
also OS research vehicle
(large mem + many CPUs)



Masur 26 chip (*currently in production*)

Network-on-chip (new)

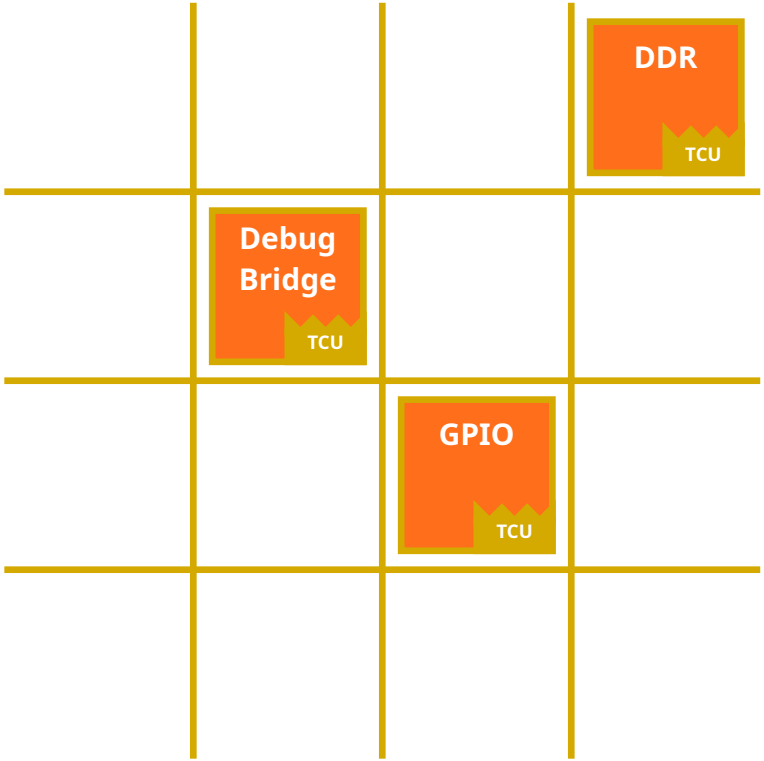
- FlooNoC (ETHZ)
- full-mesh, full-duplex
- 64 bit (ca. 280 wires)
- 4x4 grid, XY-routing
- adaptations for zoned routing



Masur 26 chip (*currently in production*)

I/O interfaces (re-use)

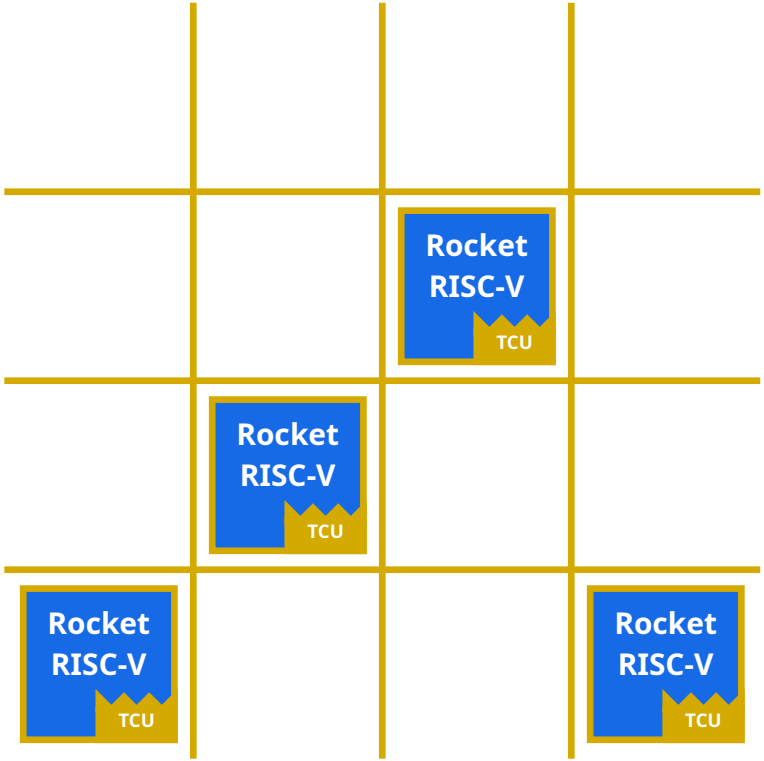
- LPDDR4 16 bit, single-channel
- JTAG
- UART
- GPIO pins



Masur 26 chip (*currently in production*)

CPUs (partial re-use)

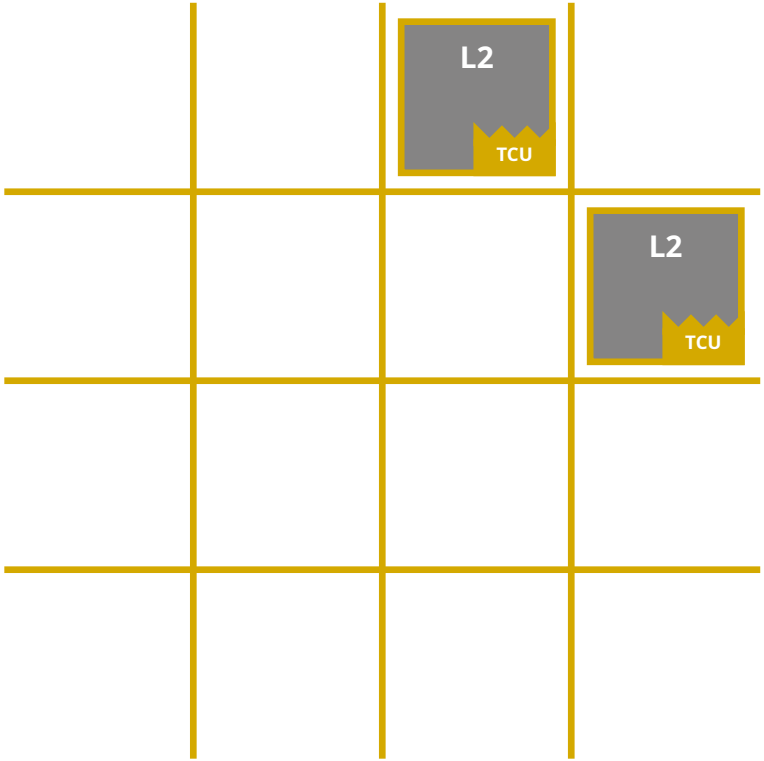
- 64 bit
- new cache interface



Masur 26 chip (*currently in production*)

Cache infrastructure (new)

- implements Bring-your-own-Core (from OpenPiton)
- 2 separate coherency regions (can be joined)
- L1.5 caches per CPU-tile

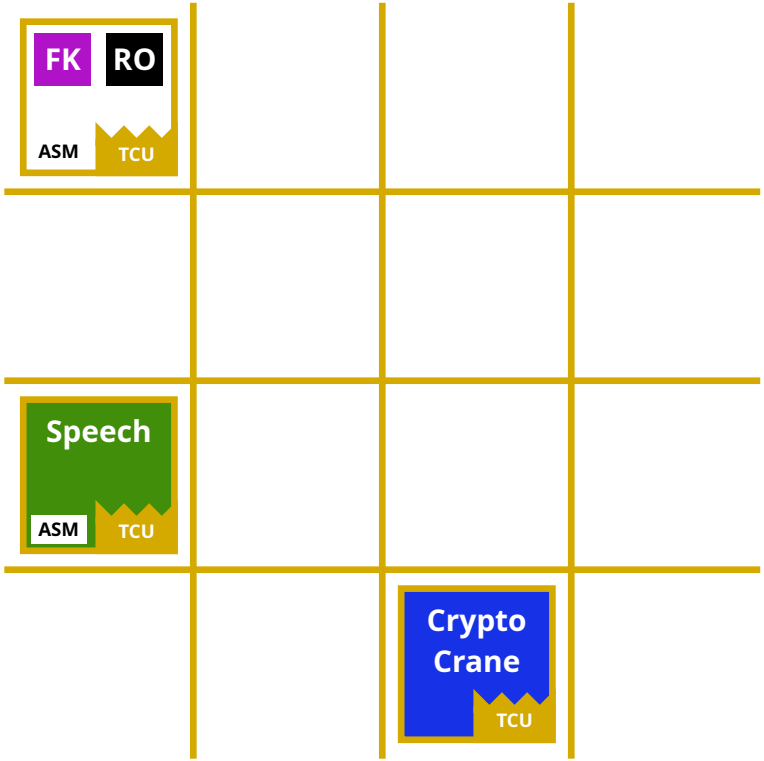


Masur 26 chip (*currently in production*)

Speech accelerator

- RWTH Aachen
- ultra low-power AI accelerator
- CPU-less IP

- soft-IP
- exclusive tile
- accelerator support module
- **minimum-effort integration**

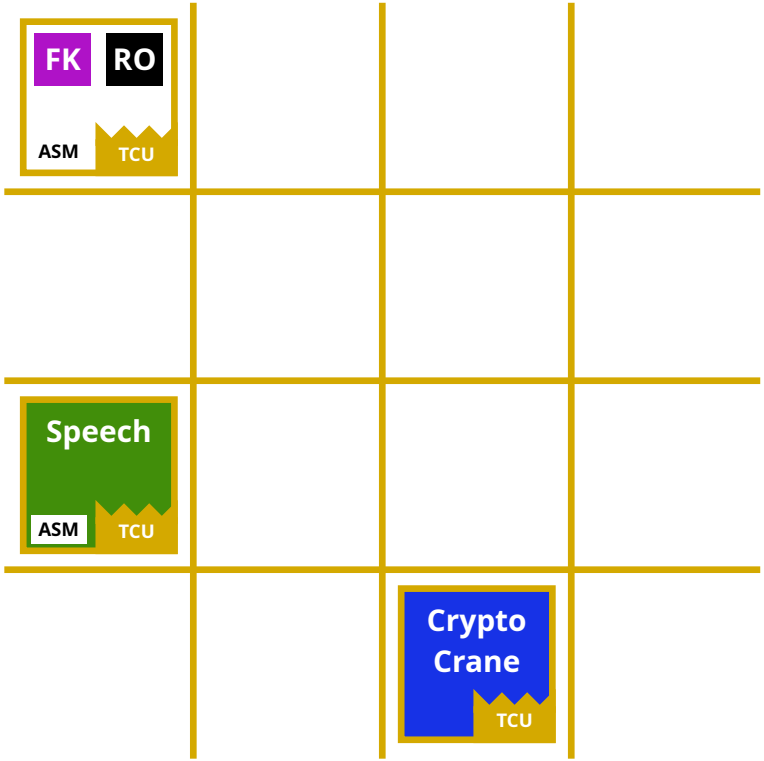


Masur 26 chip (*currently in production*)

Crypto Crane

- RPTU Kaiserslautern
- CPU + post-quantum crypto extension

- soft-IP
- exclusive tile
- full-custom (only interface)
- **customer performance constraints**



Masur 26 chip (*currently in production*)

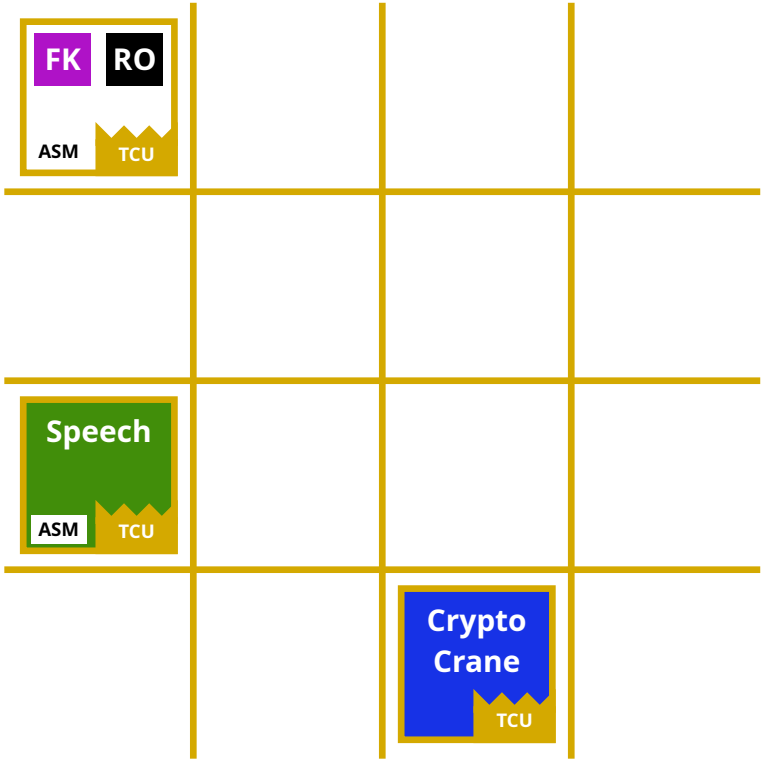
FrodoKEM crypto accelerator

- in-house PQC accelerator
  (secure digital systems group)
- soft-IP

Ring oscillator

- in-house
  (RF design enablement group)
- hard-IP

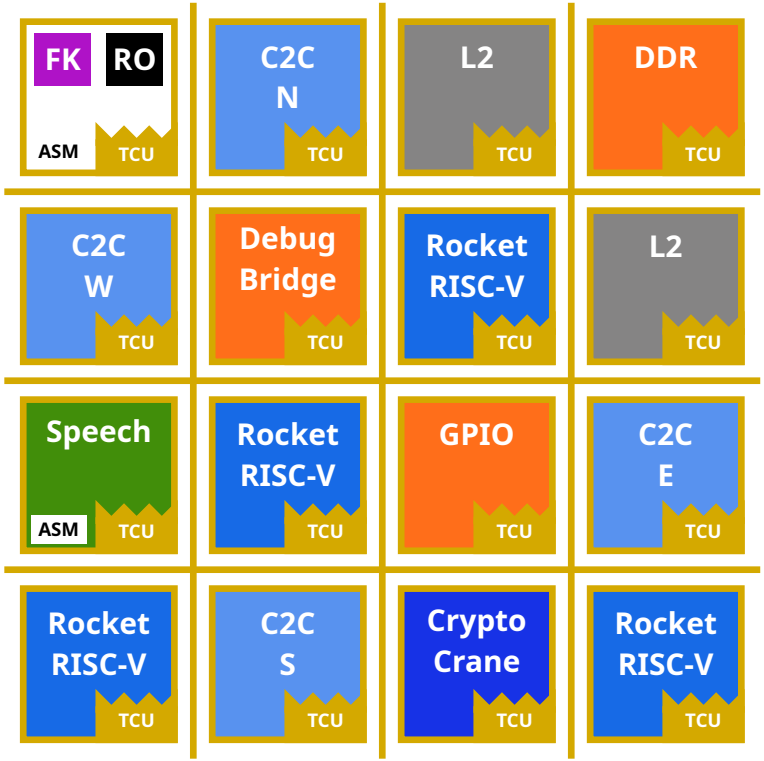
- 4 IP cores + ASM on tile
- **tile sharing**



Masur 26 chip (*currently in production*)

Design principles

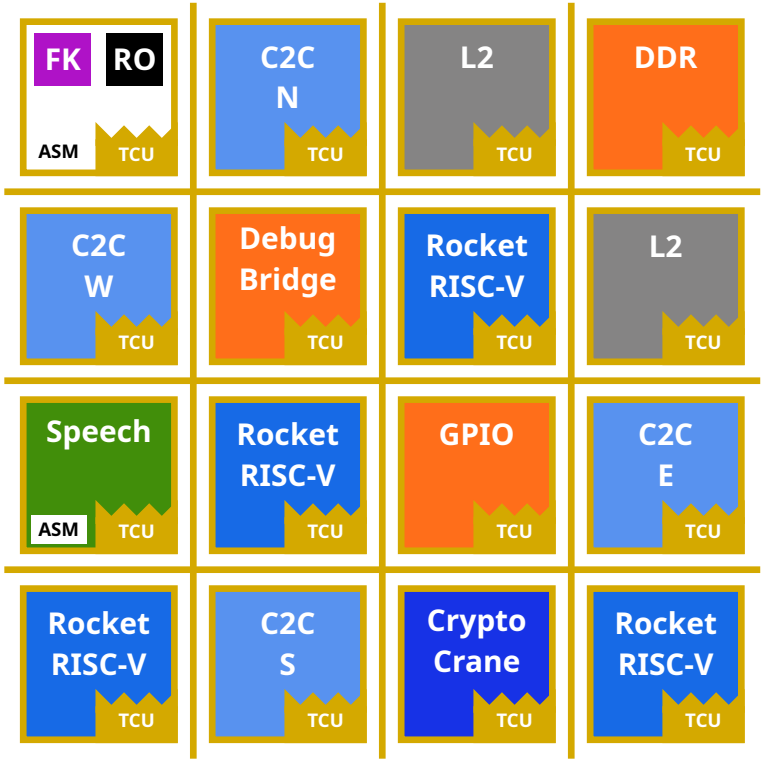
- selectivity is key
- layered configurable interfaces



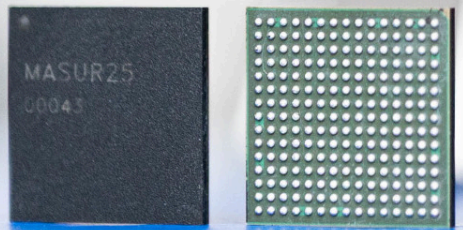
Masur 26 chip (*currently in production*)

Design principles

- selectivity is key
- layered configurable interfaces
  - IF adapters ⟶ full-custom IP
  - X-bar ⟶ tile sharing
  - ASM ⟶ CPU-less IP
  - selective cache-coherence



Only trust what you need



barkhauseninstitut.org/en/chip-design