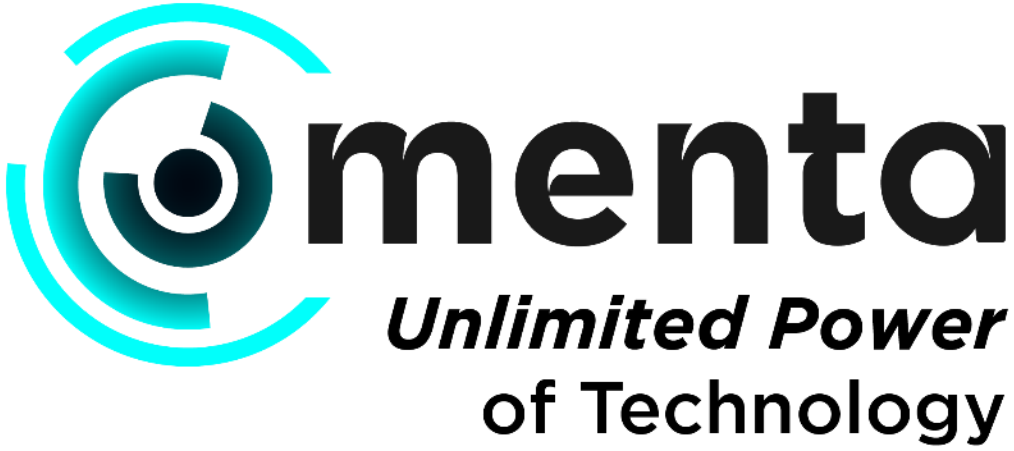
MPSoC'25



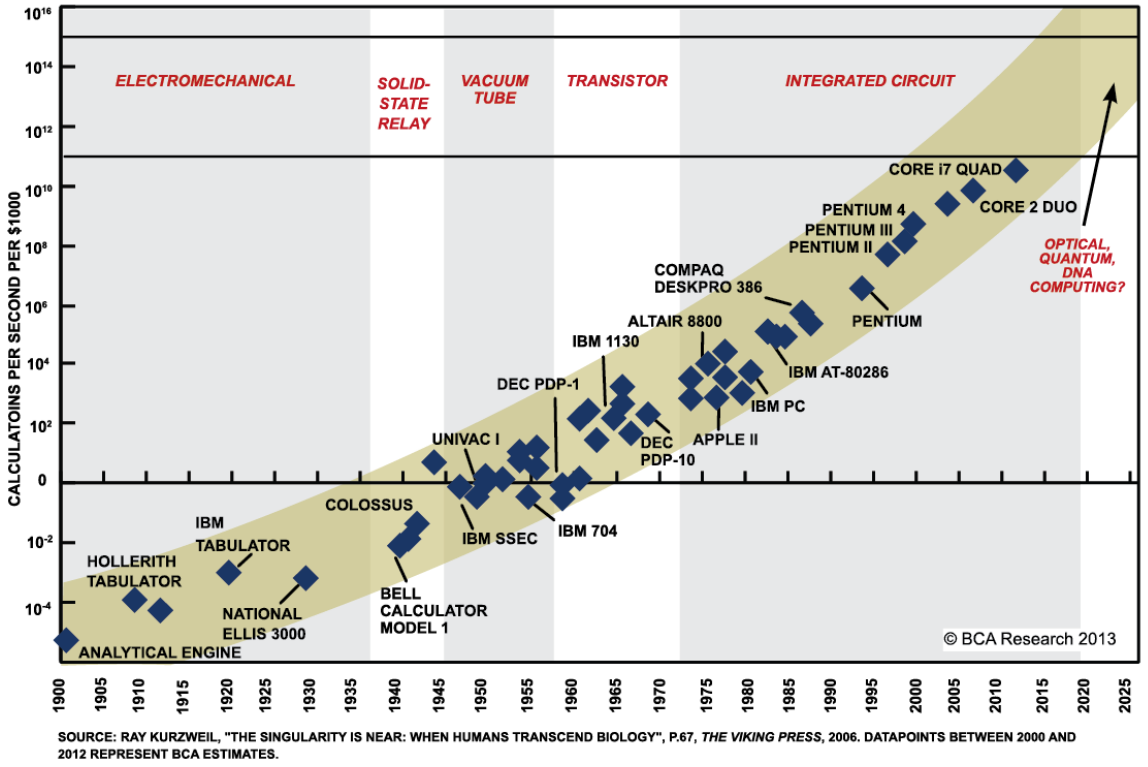
BECAUSE THE ONLY CONSTANT IS CHANGE!
Adaptable SoCs and ASICs with eFPGA

Yoan DUPRET, Managing Director & CTO

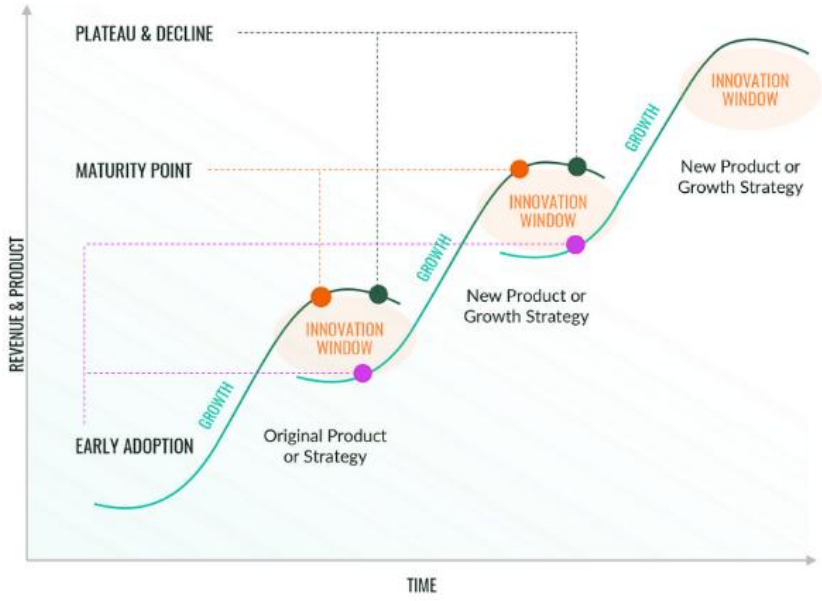
June 17, 2025

The law of accelerating returns applied to ICs

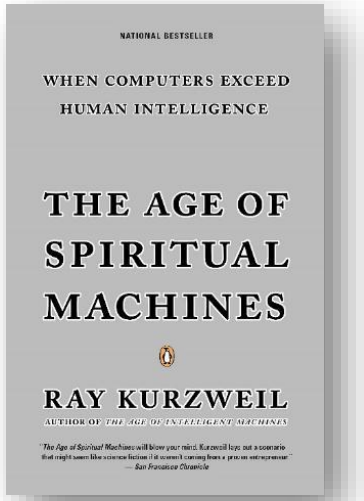
Technical innovations have the tendencies to feed on themselves, increase the rate of further innovations leading to exponential rate growth of innovations.



SOURCE: RAY KURZWEIL, "THE SINGULARITY IS NEAR: WHEN HUMANS TRANSCEND BIOLOGY", P.67, *THE VIKING PRESS*, 2006. DATAPOINTS BETWEEN 2000 AND 2012 REPRESENT BCA ESTIMATES.



From: Grove Ventures, 2022
https://medium.com/groveventures/technologys-favorite-curve-the-s-curve-and-why-it-matters-to-you-249367792bd7



3 structural megatrends imply an exponential requirement for adaptive ICs

1 Growing demands for long lifetime ICs

2 End of Moore's law

Importance of custom compute

3 Enabling changes in a design

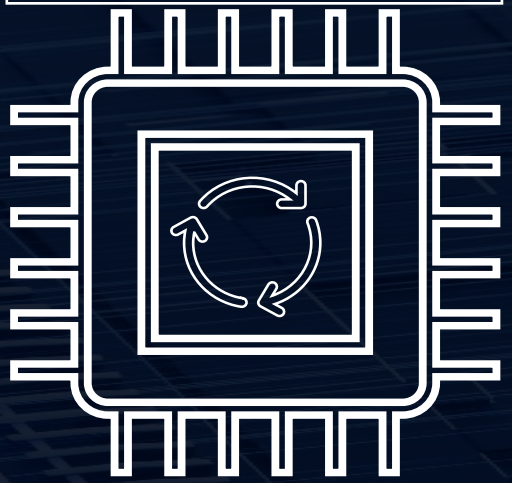
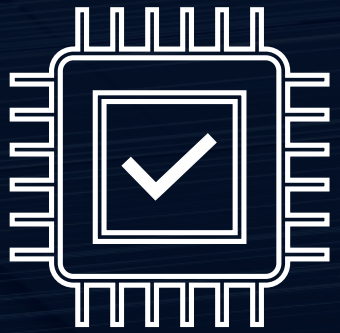
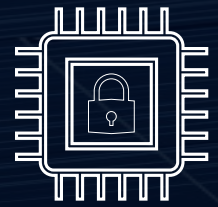
Better TTM, less verification and solving HR issues

New growing requirements

- Adaptation during chip lifetime
- Adaptive accelerators /**Custom** compute
- Lower design cycles with automation
- Pushing design decisions to after tapeout
- Waste reduction

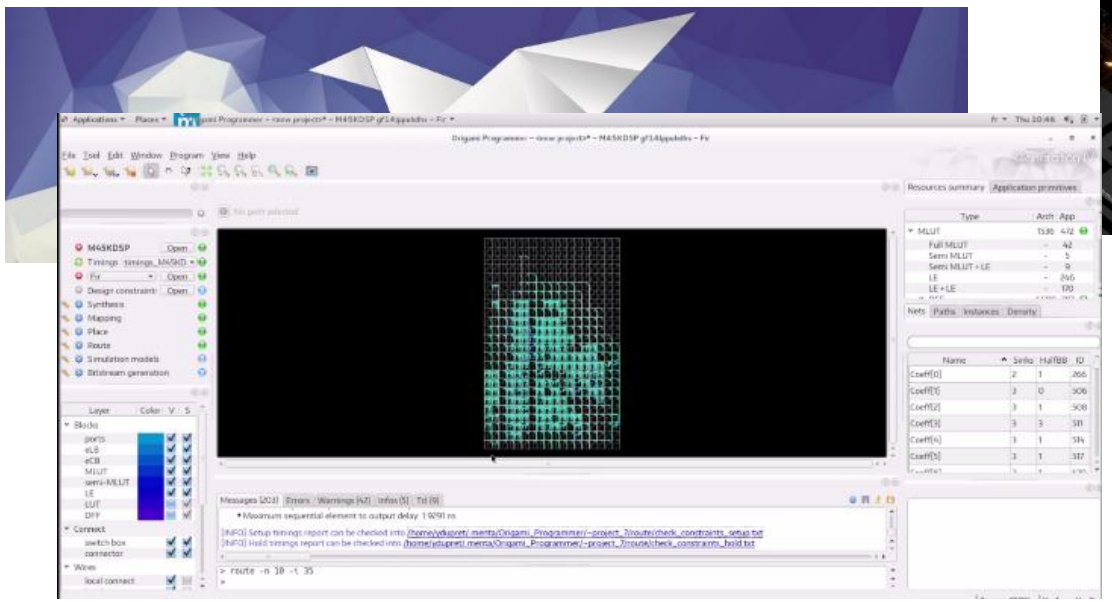
Evolving Solutions to Complex Algorithms

Solutions today are implemented in either FPGAs or ASICs/SoCs, **but Hybrid offers Best of Both**

	FPGA	HYBRID	ASIC
			
PROS	Flexible, Adaptable	Adaptable Hardware High Performance Low Cost & Power Lowers Design Risk	Highest Performance Lowest Cost & Power
CONS	High Cost & Power Supply Chain Trust Cloneable/Mutable Side Channel Attacks Hard to Design	RTL design knowledge for highest performance	Lacks any HW adaptability or flexibility High Design Risk Only SW upgrades

eFPGA IP and Software

Combine ASIC/SoC and FPGA	Pure digital eFPGA IP
Enable SoC lifetime re-programmability	Configuration Software Origami Programmer



Pioneers of eFPGA IP

15+

YEARS

ADVANCED ARCHITECTURE

ADAPTABLE

LUT6

Adaptive DSP

3rd-Party Memory

Any Hard Macro Integration

CUSTOMER SUCCESSES

AI, Security / Cryptography, RF

Digital Front End, FSMs, Bridging

Multiple Customers

Many Markets

5G, Aerospace, Consumer, Defense, IIoT, Mobility

menta

ANY FOUNDRY

ANY NODE

100%

3rd-party Standard Cell

IP DELIVERY

< 2

WEEKS

Highest Yield & Reliability

99.8%

Test Coverage

Standard Scan-Test

PARTNERS

SEMI FIVE

PQSecure

TRUSTED Semiconductor Solutions

PRESTO Engineering

TIEMPO SECURE

Fraunhofer

Codasip

IC'ALPS

KIT

imec

cea

SYNOPSYS

CIPHERA

SIEMENS

ANDES

cadence

SECURE-IC

NAGRA KUDELSKI GROUP

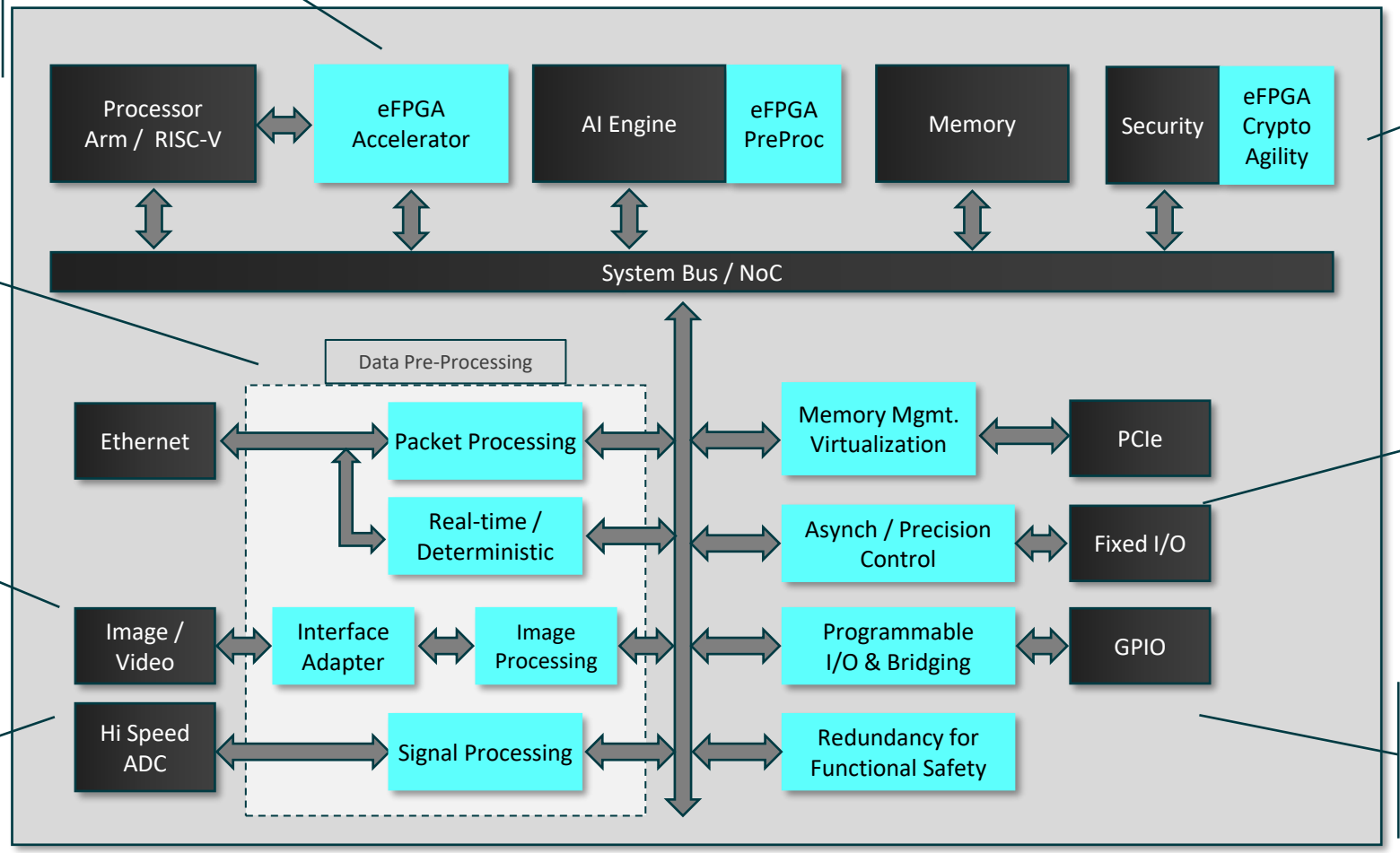
eFPGA Adds Value Across the Chip

Accelerate complex algorithms with custom ISA Instructions

Programmable Data Plane Processing Deterministic Industrial Networking

Adaptable Image Signal processing adapts to more sensors, increasing SAM

DSP Filtering Transforms



Protect against evolving threats & quantum computing

Obfuscate secret IP

Enable security autonomy

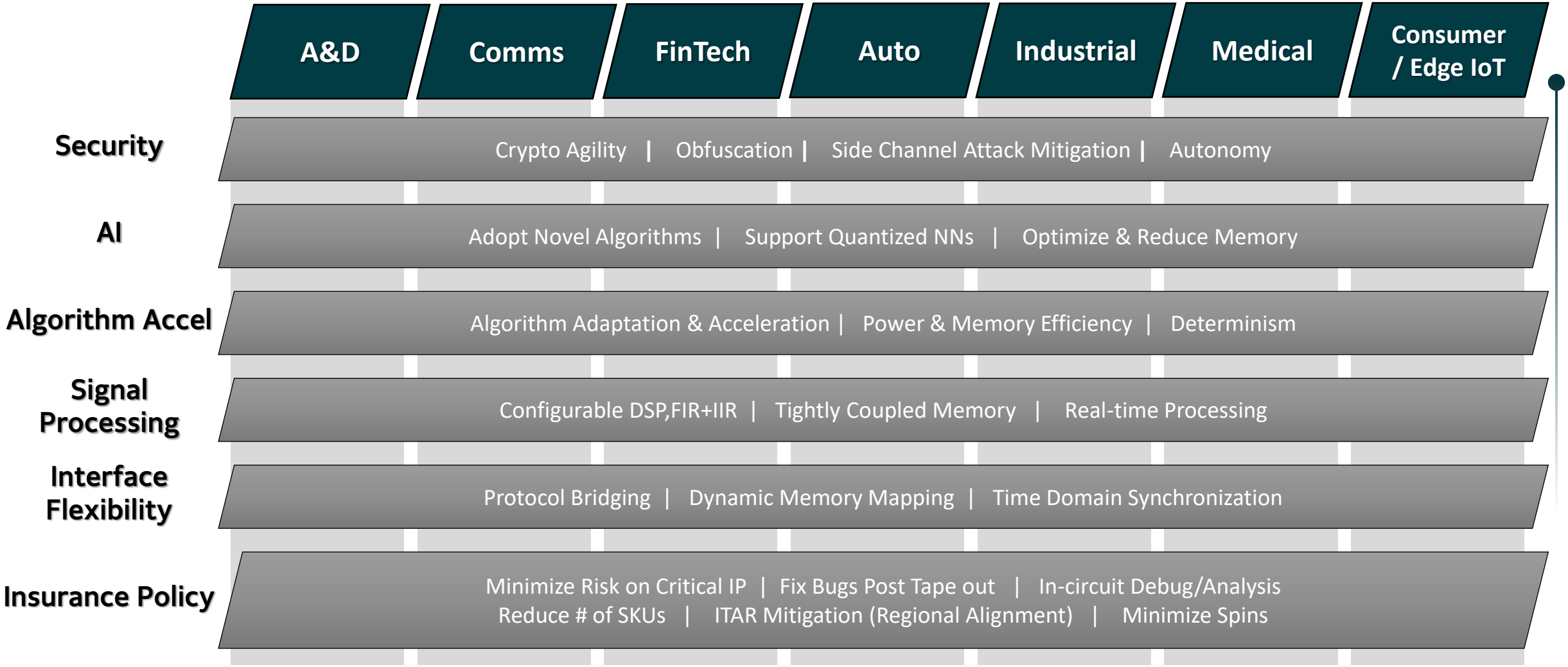
Expand Physical and Virtual functions Bridge & DMA data

Interface Flexibility – Adaptable to different markets & applications

Eliminate unused ports – minimizing surface attack exposure

Menta eFPGA IP

Horizontal eFPGA Values Across Multiple Markets



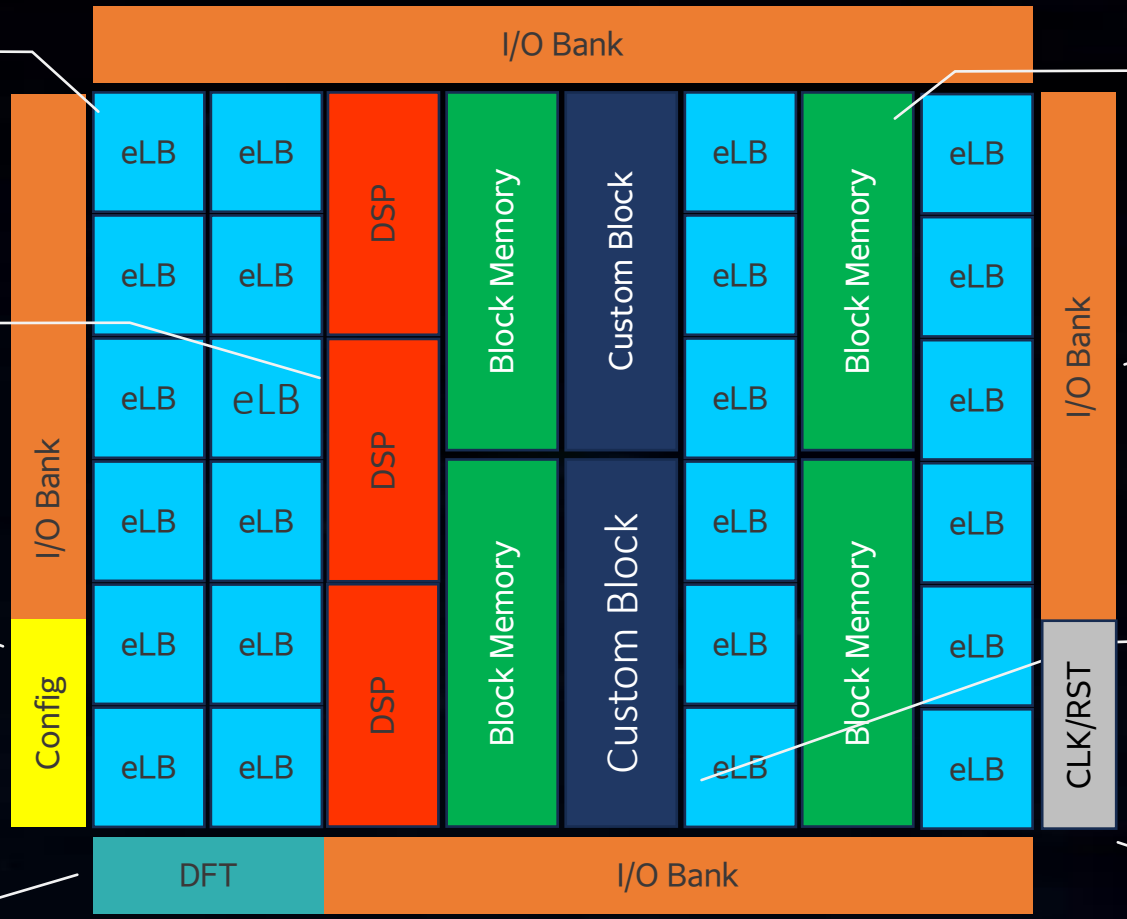
5th Generation
DESIGN ADAPTIVE eFPGA IP

Embedded Logic Blocks
Menta 6-input LUT

DSP Blocks
Customer Defined

Configuration
SPI | AXI | JTAG
AHB | Custom

DFT
Standard ASIC test scan chain interface



Embedded Memory Blocks
Any 3rd-party RAM

I/O Block
Define # of pins

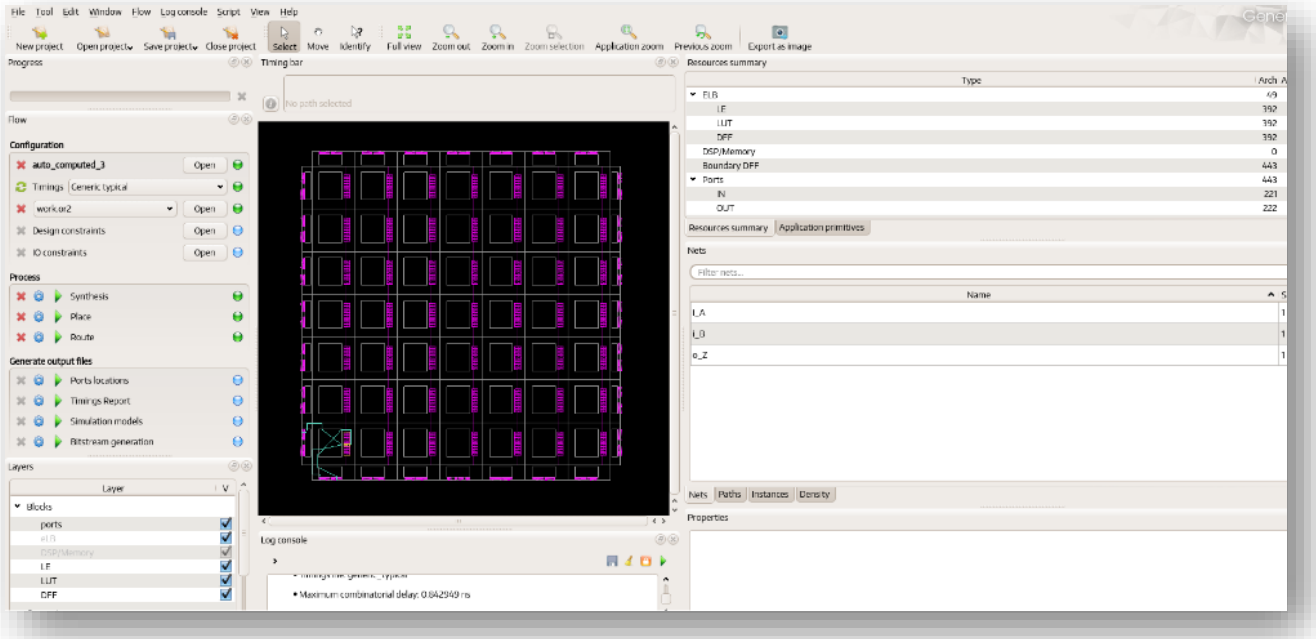
Embedded Custom Block
Customer or 3rd-party IP

Clock / Reset
Control Input Block

Origami Programmer

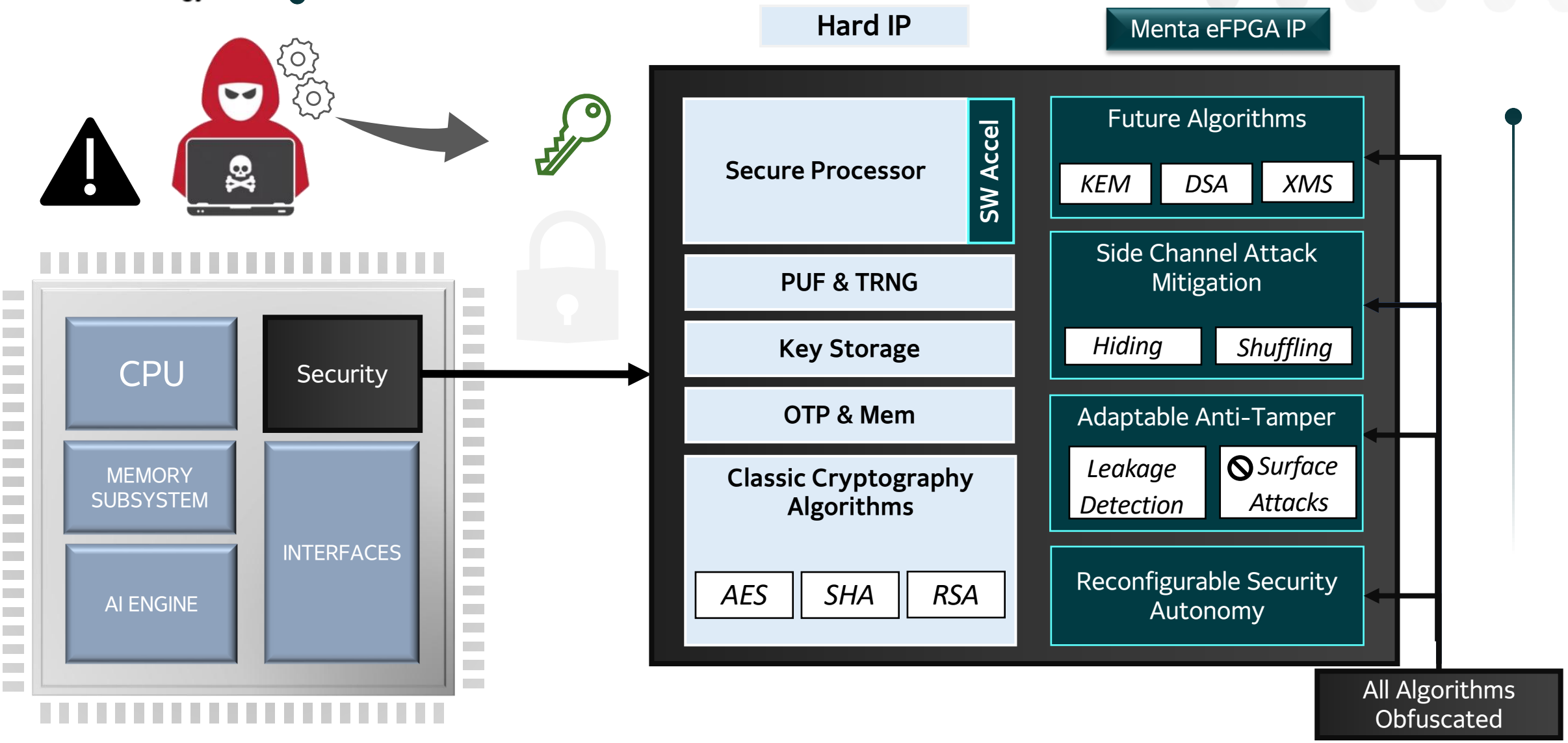
FROM RTL TO BITSTREAM GENERATION

- **Inputs:**
  - Application RTL
    - IEEE Verilog / SystemVerilog / VHDL
  - Constraints: timing & IOs
- **Outputs:**
  - Bitstream
  - Simulation model
  - Timing reports
- **GUI interface:**
  - STA
  - Resources visualisation
  - Congestion maps
  - Move and reallocate resources



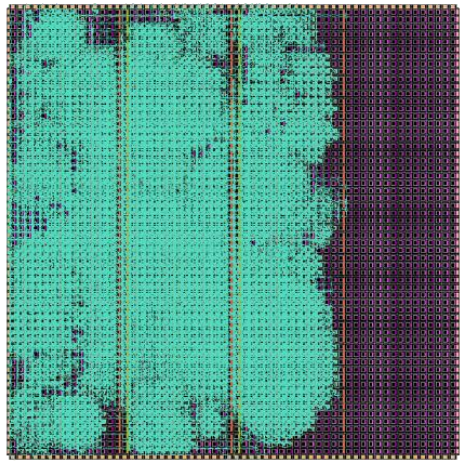
- **From synthesis to bitstream generation: Menta development**
- **No external tool required**
- **Full Command Line/Scriptable**
- **Redistributable**

Agile Cryptography Controller Architecture



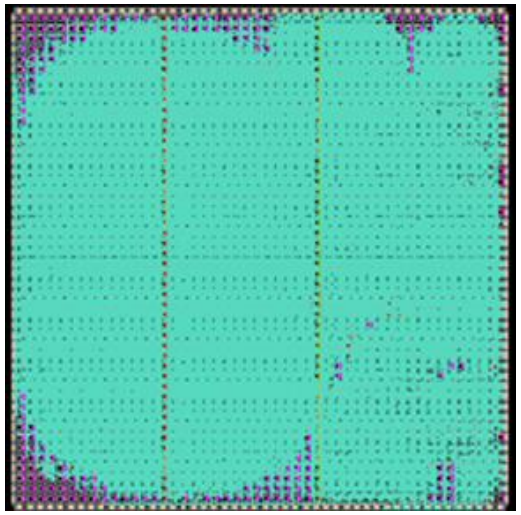
PQC Algorithms Implementations on Menta eFPGA IP

Fmax*	LUTs	Flops	DSP	Memory
64	13,814	5,344	3	36



PQSecure

PQSecure-CRYSTALS-1000: A unified hardware IP for CRYSTALS-KYBER and CRYSTALS-Dilithium with protection against Simple Power Analysis (SPA) and First-Order Differential Power Analysis (DPA) attack protection achieved through masking and shuffling. Timing attack protection through constant-time operation.



CIPHERA

ML-KEM (XIP6110B)

The xQlave® ML-KEM (Kyber) Key Encapsulation Mechanism IP core provides quantum-resistant key exchange, offering a secure solution against the growing threat posed by quantum computing.

Resources usage: <10K LUTs
Resources utilization: > 91%
Frequency*: 112 MHz

* TSMC 28HPC+

Software Acceleration with Custom ISA Extensions

HW/SW Co-Design tightly couples adaptable & reprogrammable hardware to the processor and provides the following benefits

Increased Performance

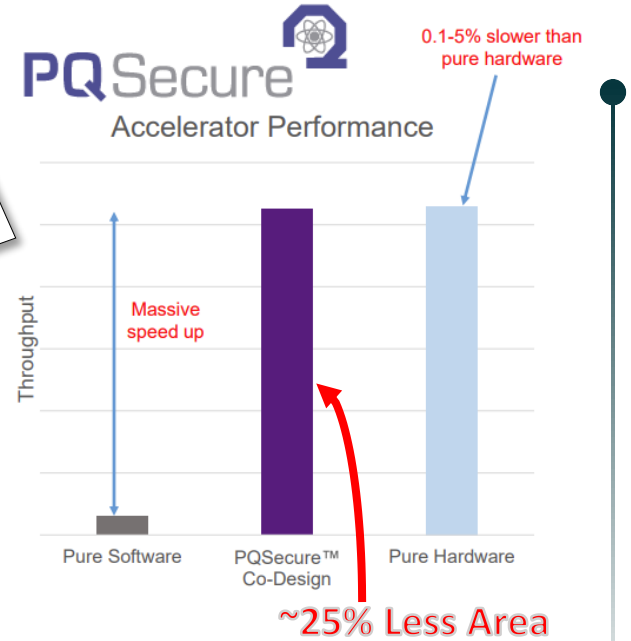
Lowers Latency

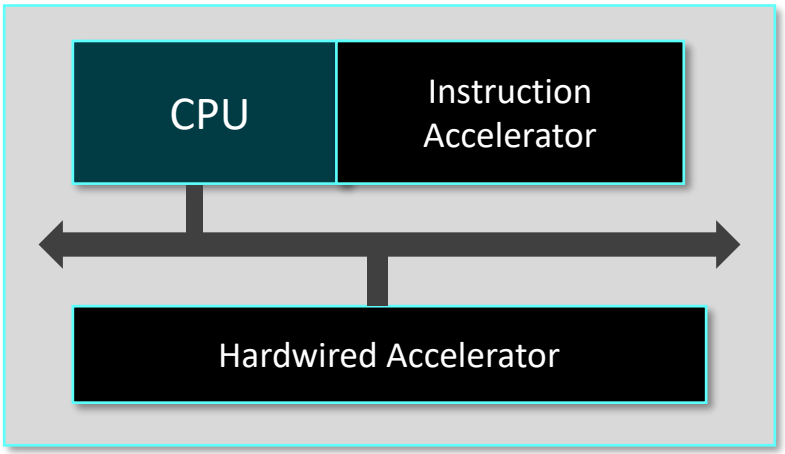
Reduces Power

PQC Algorithm with Hash function accelerated in FPGA

Other popular fxn's:

- Vector Math
- Floating Point
- Convolutions
- MAC Accel.
- DGEM
- Filters





Two Implementation Strategies

1. Tightly coupled to CPU for custom instruction extensions
   - Balance of performance and IP area impact
2. NoC connected accelerator
   - Highest performance & flexibility

Many Processors support Custom Instruction Extensions

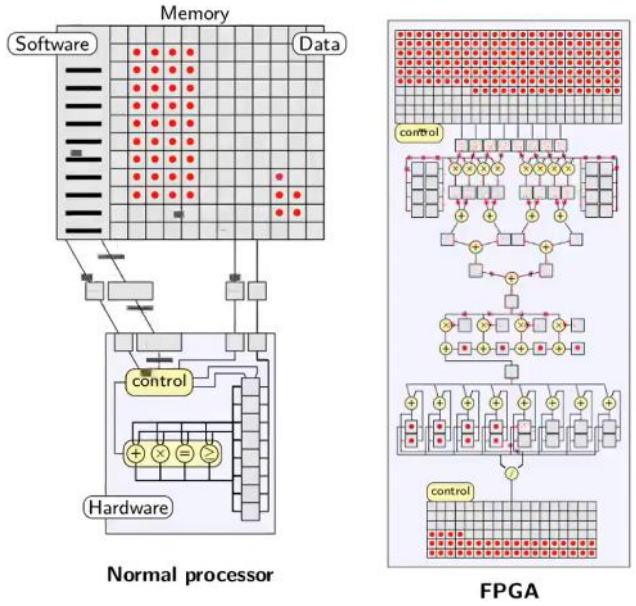
Where Do I Execute My Algorithm?

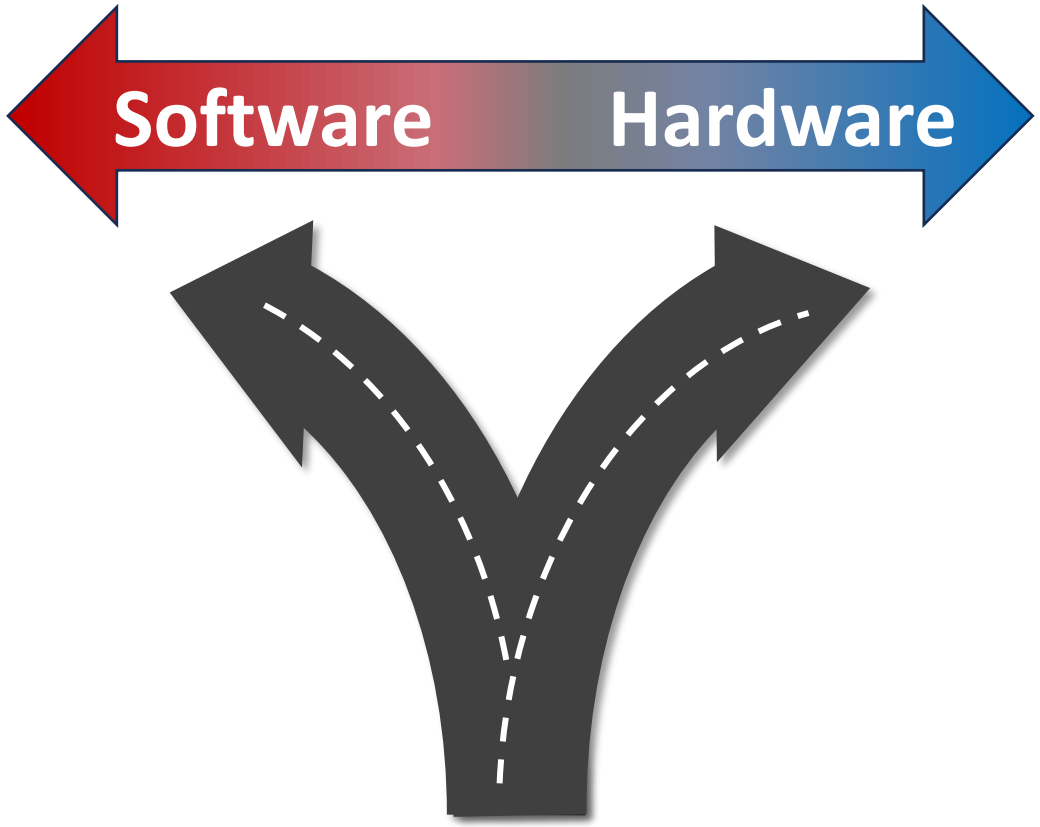
Processors or microchips offer ease-of-use, but in industries like Space, Communications, FinTech and others, the need for high performance, flexibility, and reliability makes FPGAs the great choice

Common User Interfaces

Non-time-sensitive task

Complex state machines with many branches





1 **High-Speed, Low Latency**
HW Built to match exact needs of the application

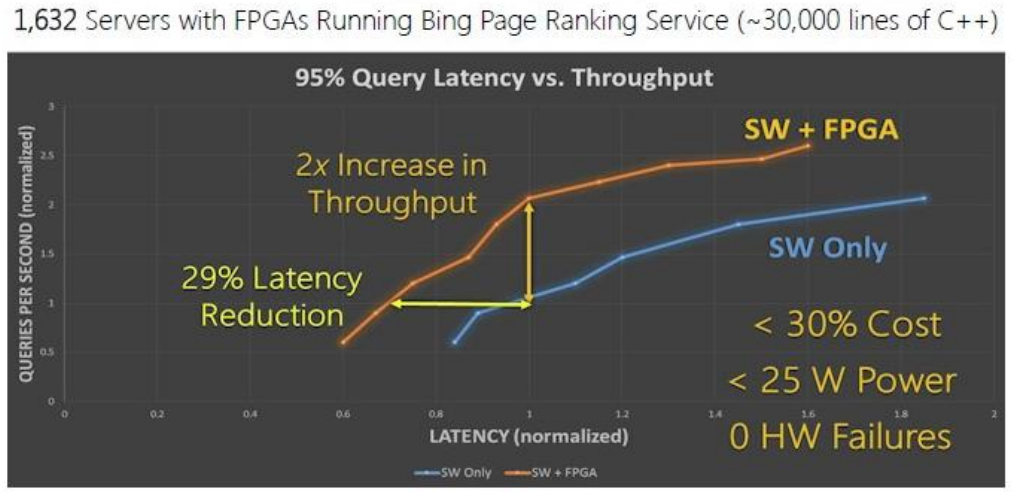
2 **Parallel Processing**
Simultaneous processing of multiple tasks & instructions

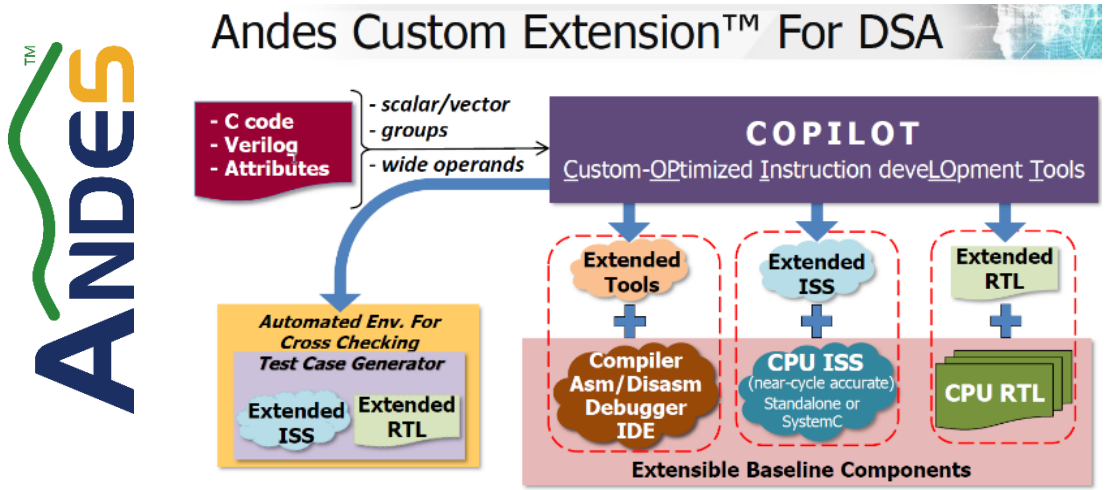
3 **Deterministic Processing**
No cache latency & tightly coupled memory, pipelining

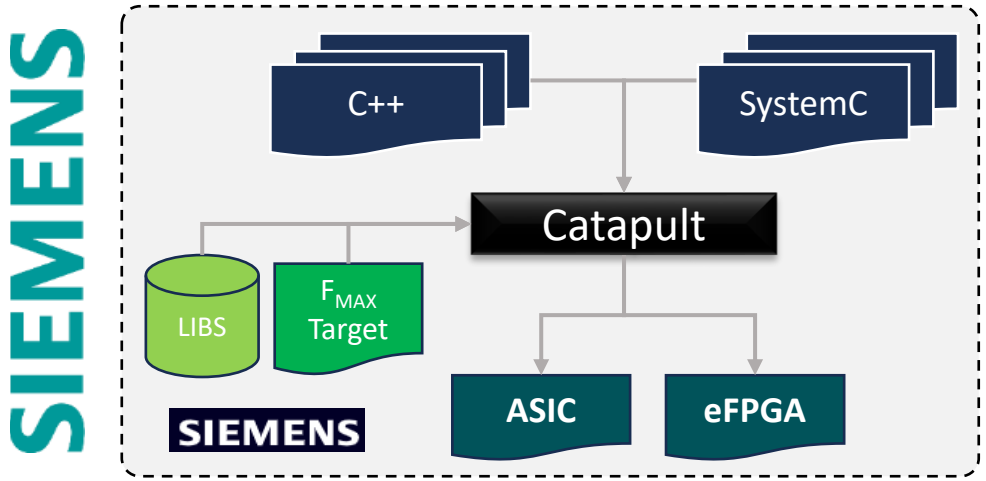
4 **Energy Efficiency**
Optimized execution in HW reduces power consumption

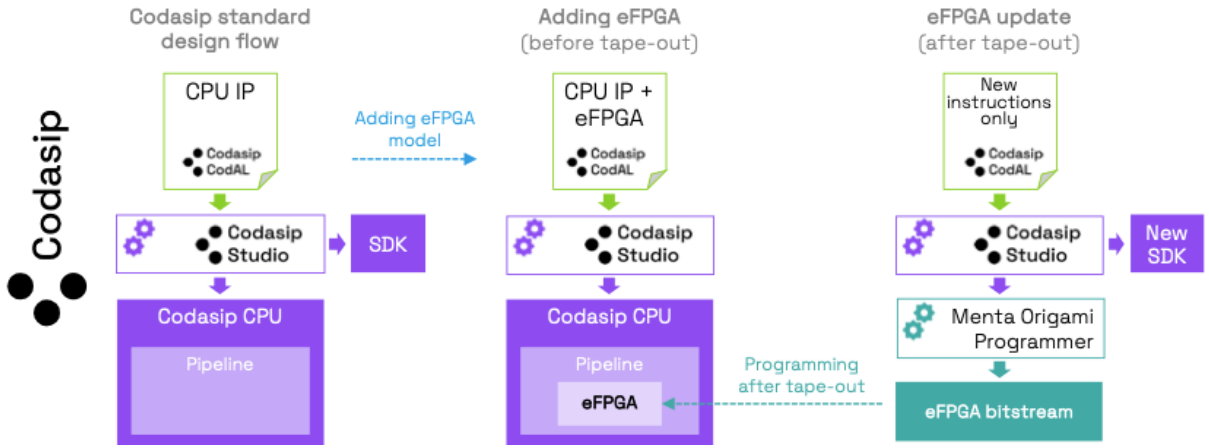
5 **Enhanced Security**
Safer key storage & threat mitigation, obfuscation

Proven HW/SW CoDesign Tools with Menta eFPGA IP









Enables Post Silicon Reconfigurability

Menta: the Clear Choice for Embedded FPGA

Performance, Control, Speed, and Support – in one IP.

Lowest Overall Cost

- Small die area
- Competitive licensing & royalty fees
- Highly efficient standard cell scan test (99.8%)
- Projected highest yield with 100% standard cell flow (no custom)

Fastest Time To Market

- IP (RTL + SW) delivery in less than 2 weeks
- Rapid ECO at any time
- Lowest risk - Foundry sign-off standard cells & flow
- Adaptability to any standards (automotive, industrial, defense)

Superior Support

- High-level of dedication
- Quick support turnaround
- Full IP and EDA ownership
- Global technical resources

Full Architectural Control

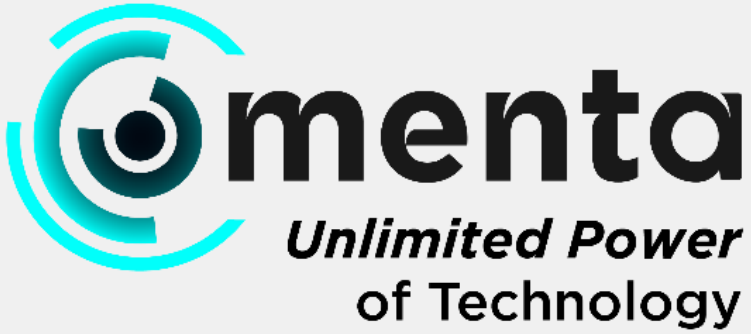
- Unlimited HW & SW definition / flexibility, hard macro
- Full control of physical implementation
- No reliance on 3rd-party tools - access, NRE/licensing cost

Full EDA Ownership & Customization

- 100% Integrable
- Easily Redistributable

Dedicated IP Partner

- Focused on IP and EDA solution
- No product or competitive conflict
- Planned R&D & support expansion


menta
Unlimited Power
of Technology