Energy-Efficient Embedded Systems by means of a Codesign of Application Domains

Patrick Schaumont
UCLA

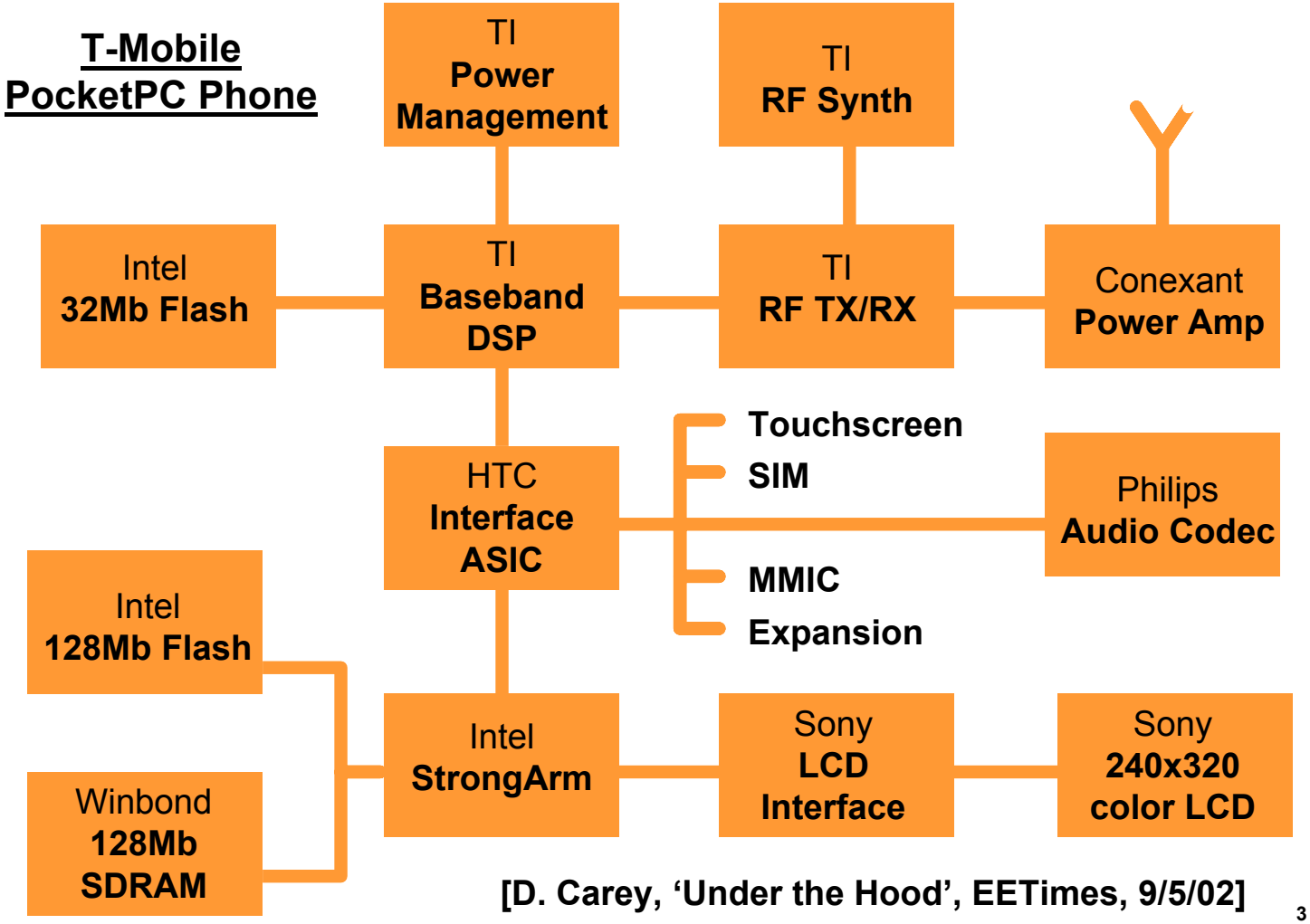
Acknowledgements:
Ingrid Verbauwhede, Doris Ching,
David Hwang, Yusuke Matsuoka

4th International Seminar on Application-Specific Multi-Processor SoC

Overview

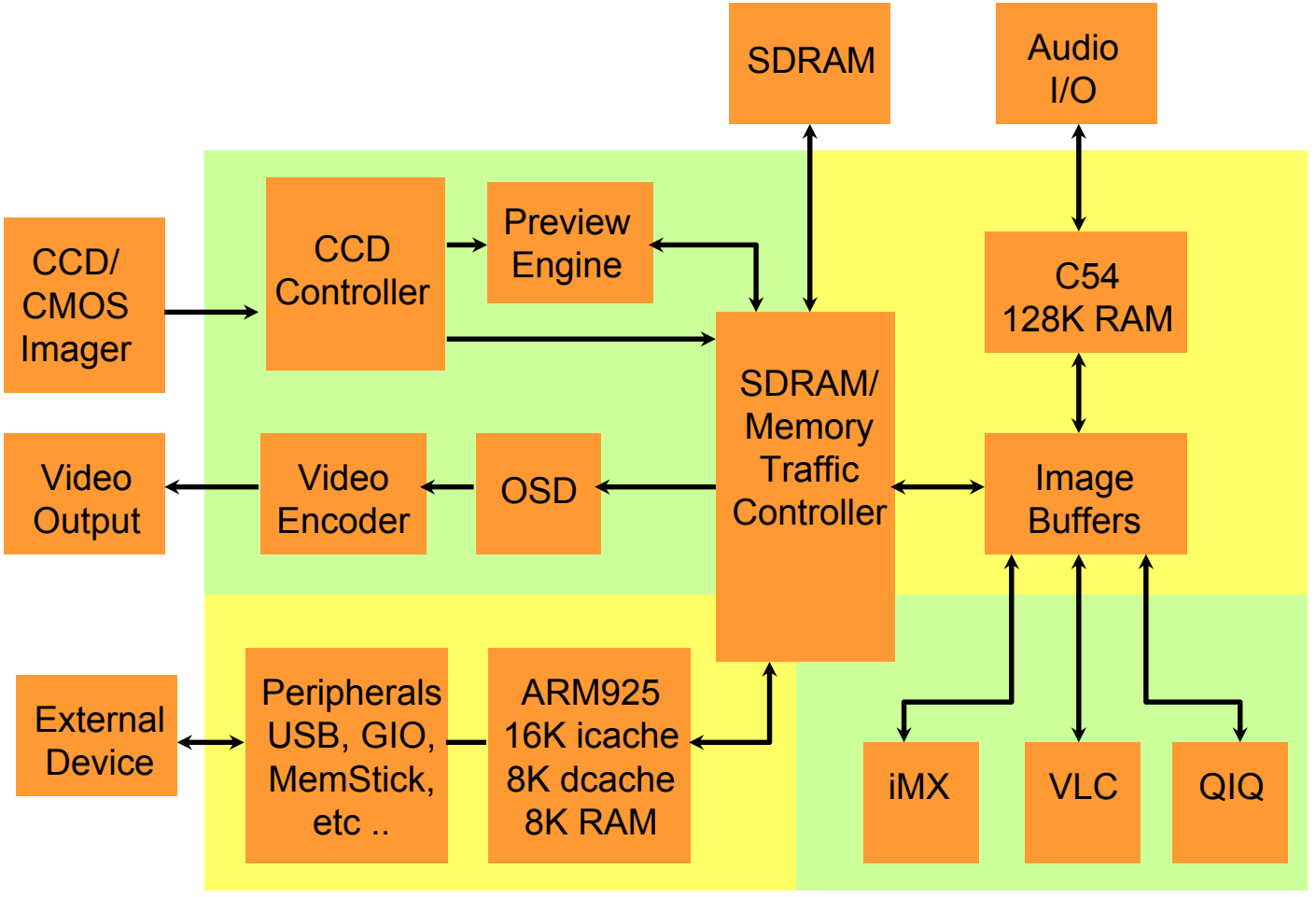
- Energy Efficient System-on-Chip
- Flexibility-Energy Trade-offs
  - Domain-Specific Processing
- Putting it all together in RINGS
  - Architecture & Software Integration Strategies
- Getting it into a tool: GEZEL
- Sample Applications

Energy-Efficient Systems are heterogeneous and distributed ...



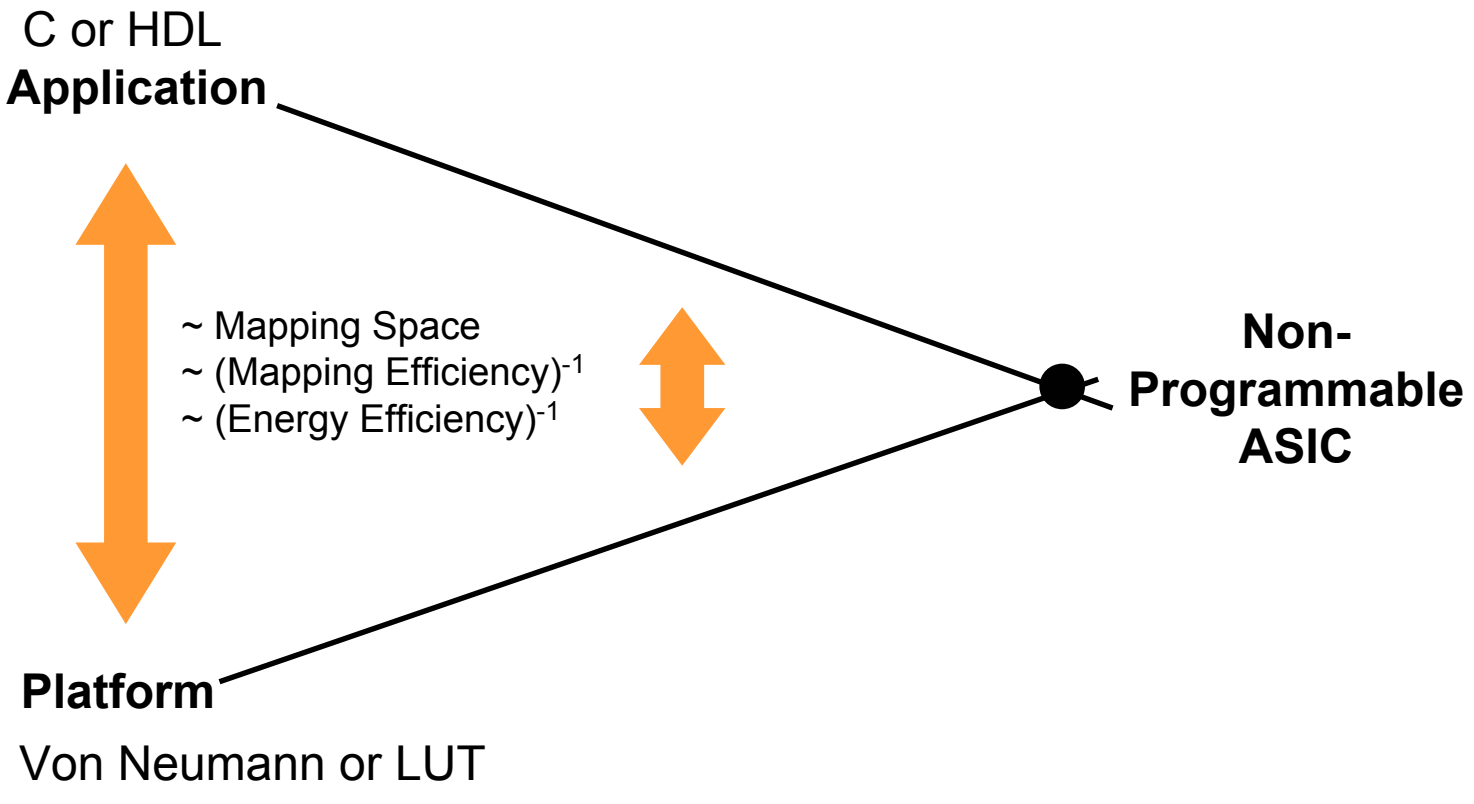
[D. Carey, 'Under the Hood', EETimes, 9/5/02]

.. and so are SoC: heterogeneous multiprocessors

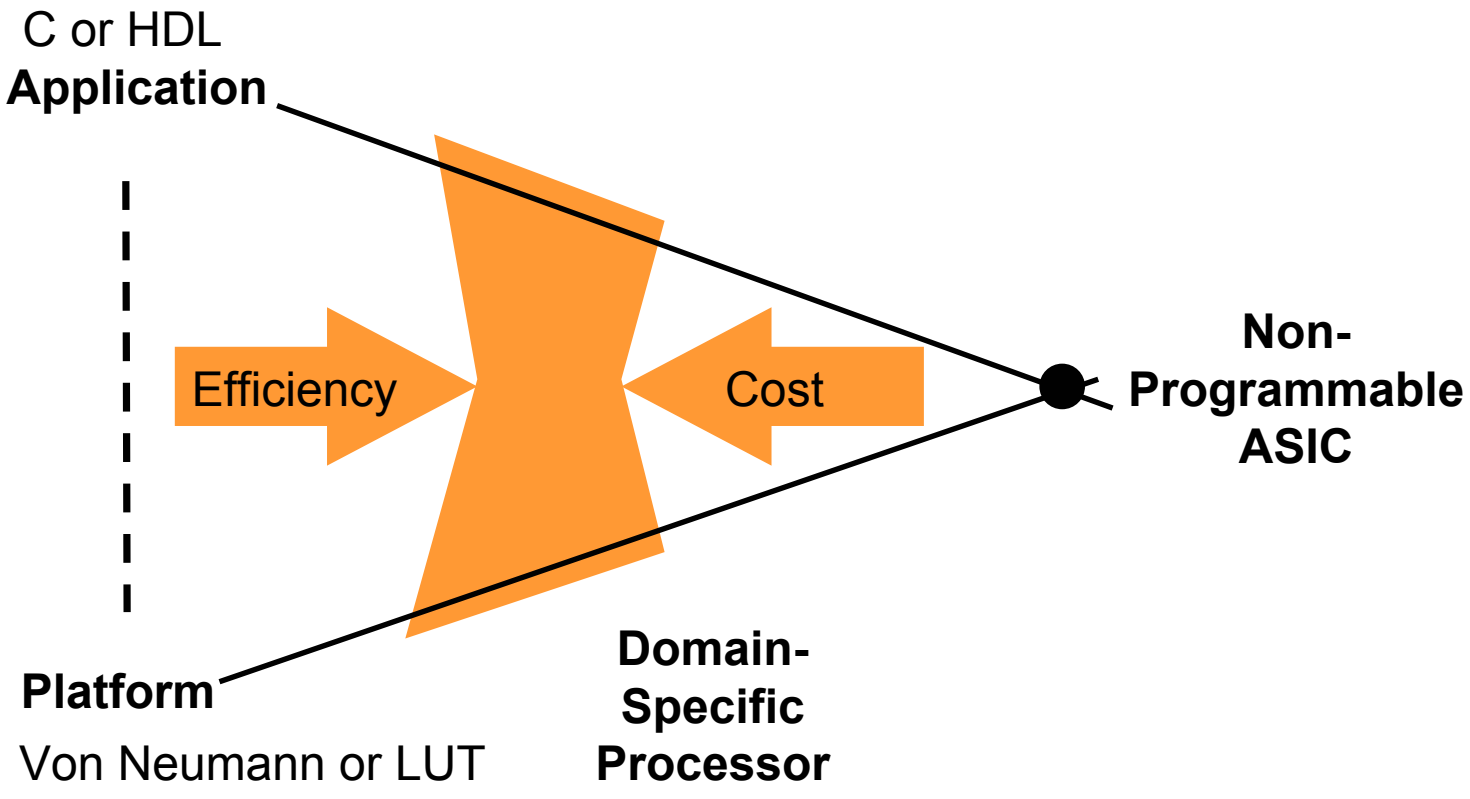


[Talla et. al, TMS320DM310 – A portable media processor, Hotchips 15, 2003]

Flexibility = (Energy Efficiency)$^{-1}$

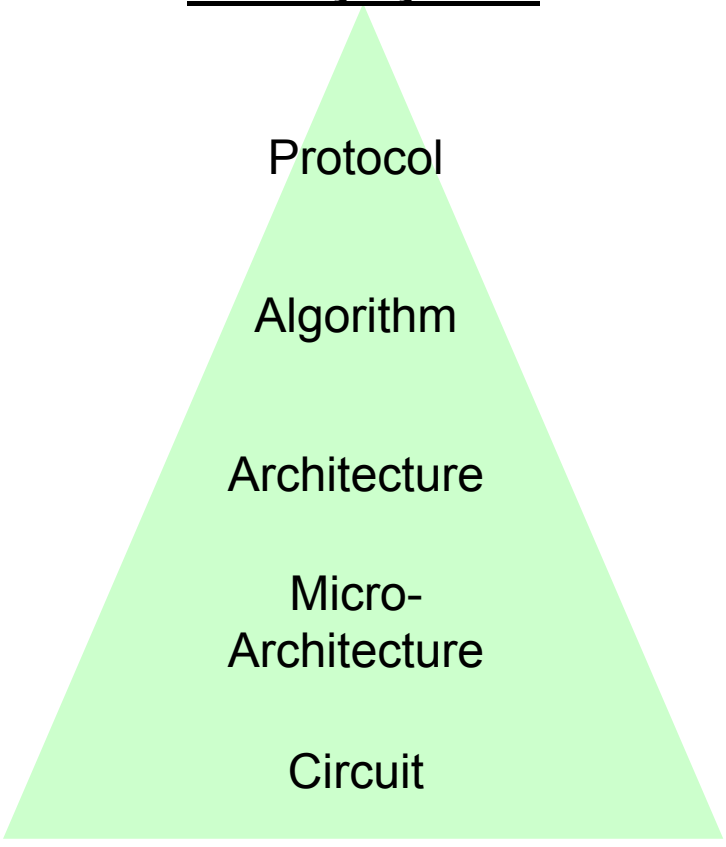


Domain-Specific Processor holds the middle



Sample Application Domain: Security

Security Pyramid



Sample Concepts

Authentication
Confidentiality

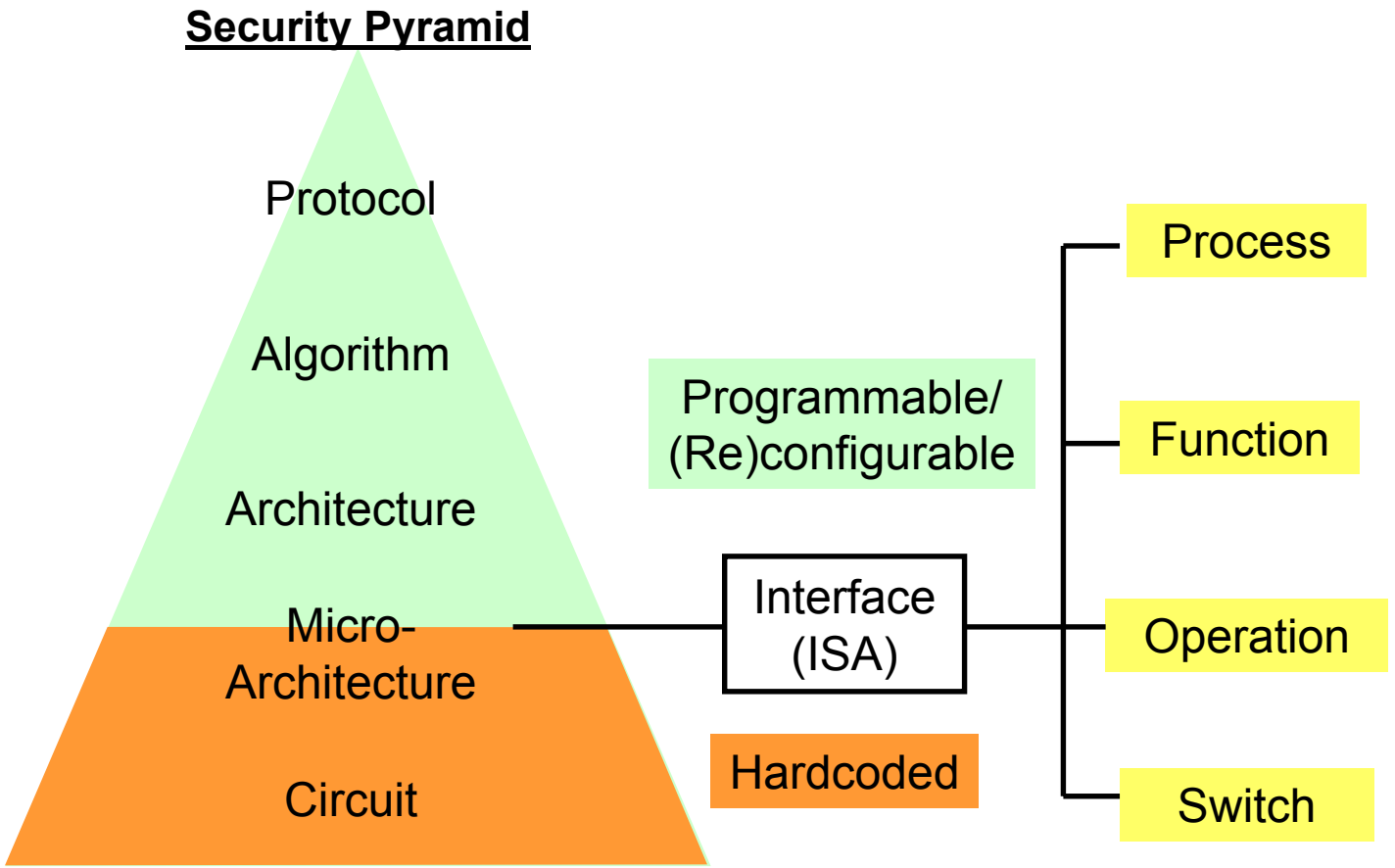
Encryption
Hashing

Sandbox
Keystore

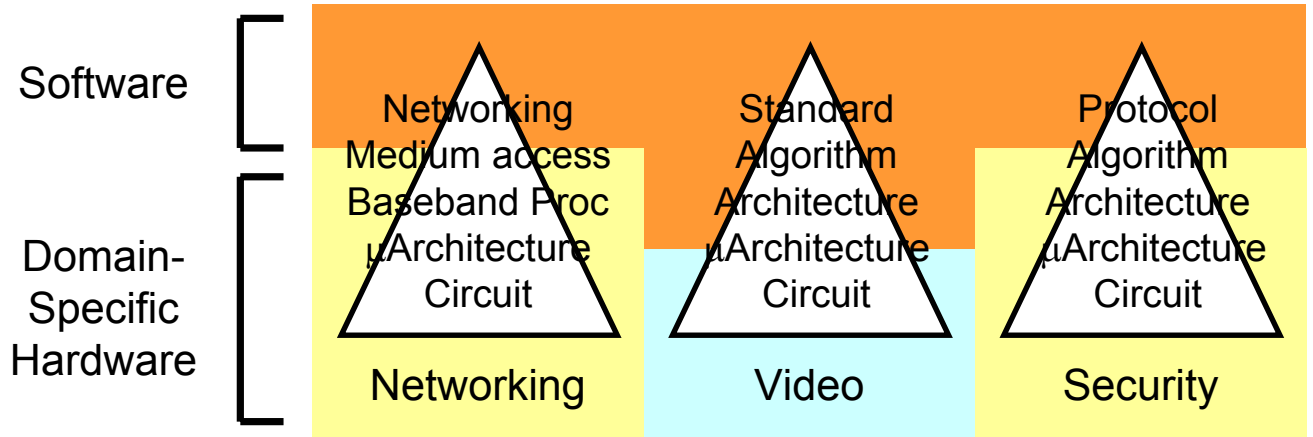
GF Operations

DPA-resistant Circuits
Secure Storage

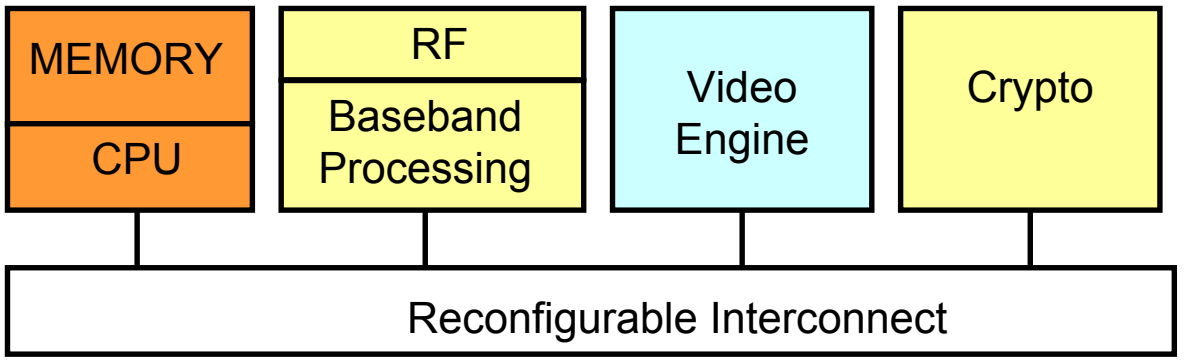
Flexibility Partitioning for Efficiency



RINGS = Combined App + Arch Model



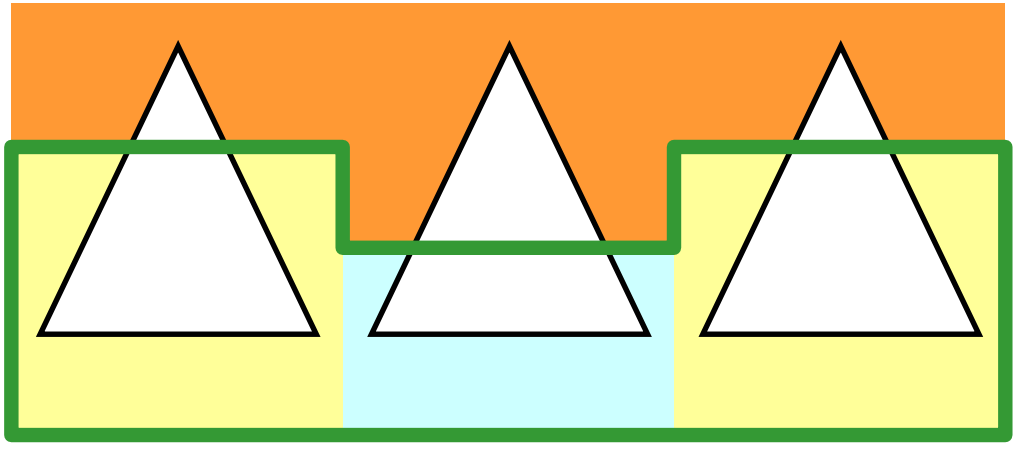
Application Model: System = Software-integrated domains

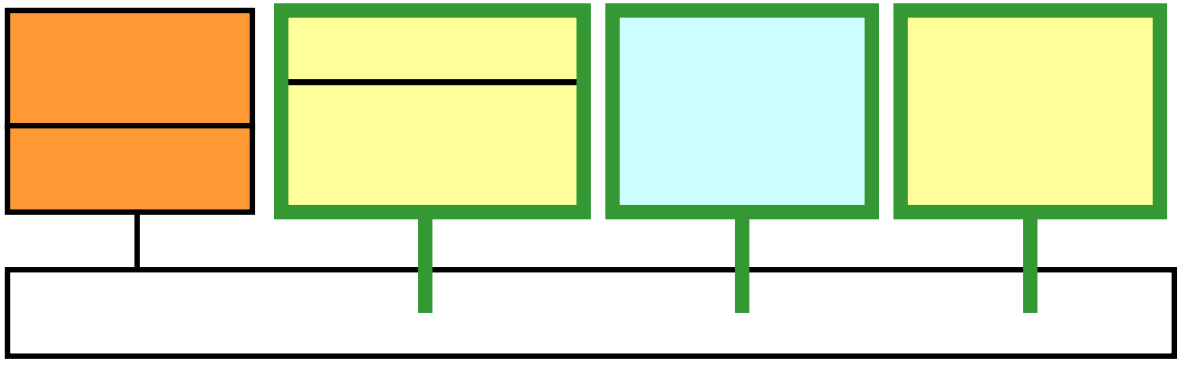


Architecture Model: System = Flex. connected processors

Strategy for Architecture Integration

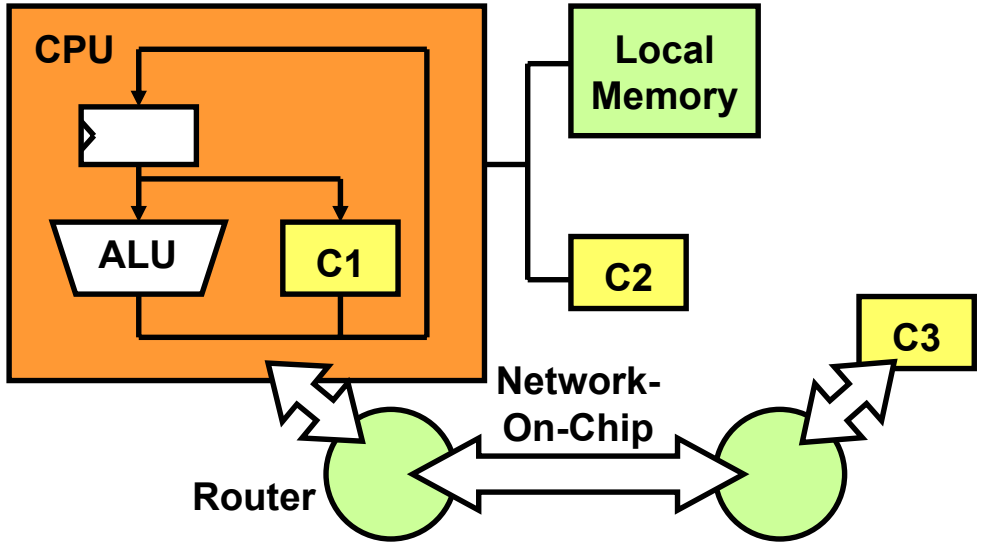
Domain-Specific Hardware





Three styles of architecture integration

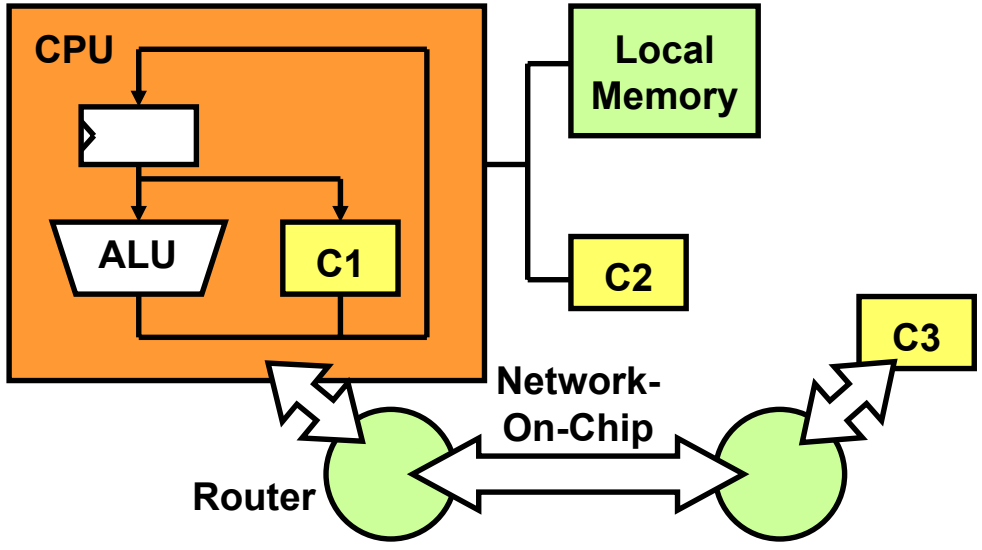
	Mapping	Granularity	Integration Mechanism
C1	**Register-Mapped**	Expression	Custom Instructions
C2	**Memory-Mapped**	Function	Memory-Mapped Instructions
C3	**Network-Mapped**	Process	Communication Primitives



Loosely Coupled has best improvement

		E_{swonly} (mJ)	E_{hwsw} (mJ)	
C1	DFT (1000 iterations)	67.6	5.76	**12X**
C2	AES (175 iterations)	89.2	3.5	**25X**
C3	TCP/IP CHK (100 packets)	13.2	0.2	**66X**

SW on LEON2 SPARCv8, Energy Estimation on Virtex2



[RAW 2004]

RINGS Basic Observation

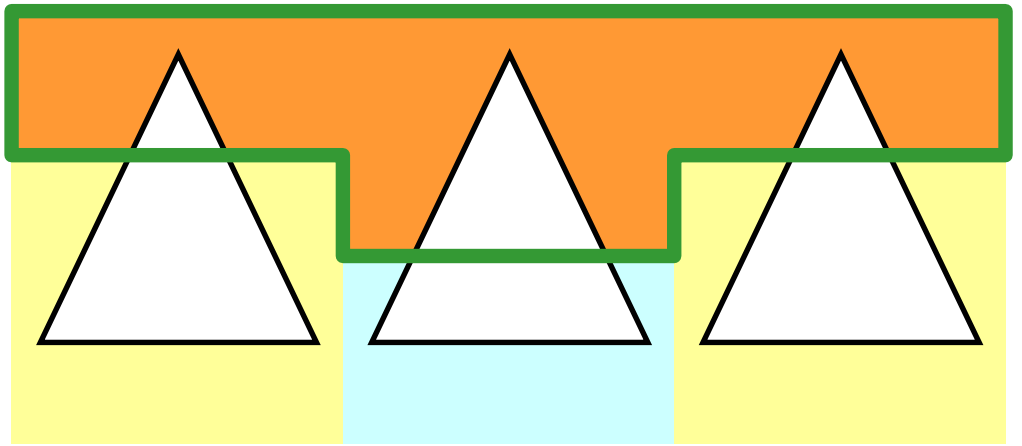
For Best Energy Efficiency:

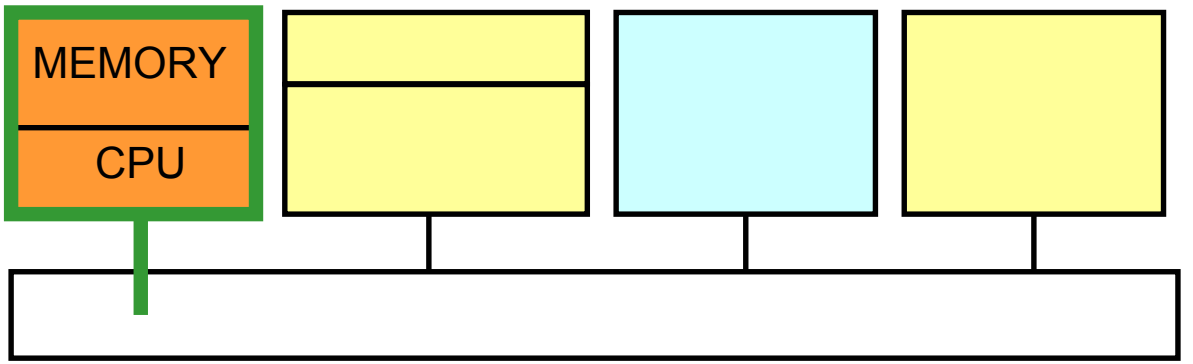
Application Flexibility

Architecture Reconfigurability

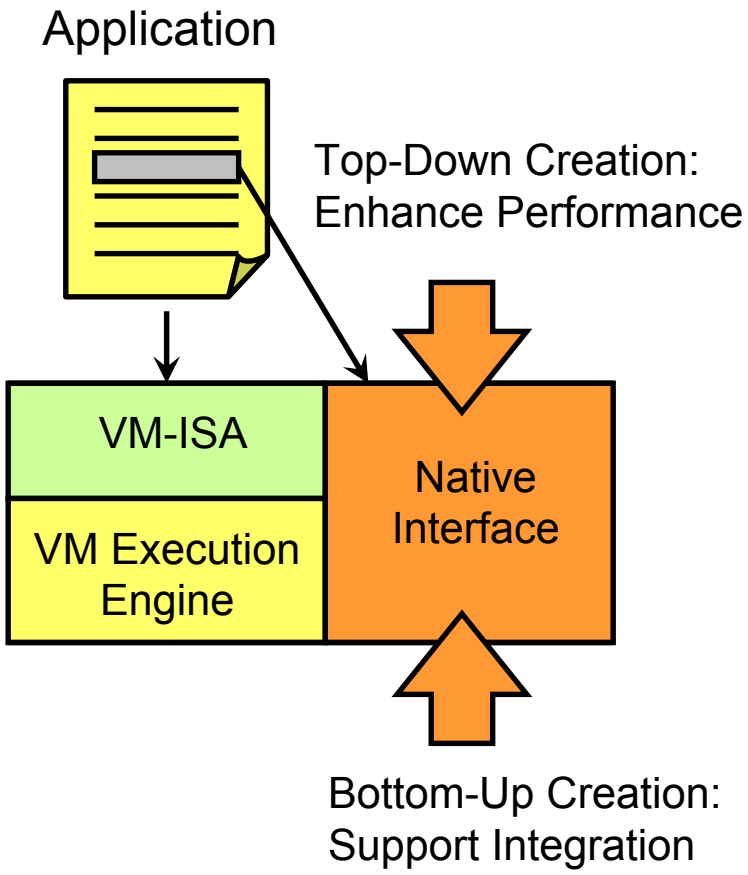
Strategy for Software Integration

Software

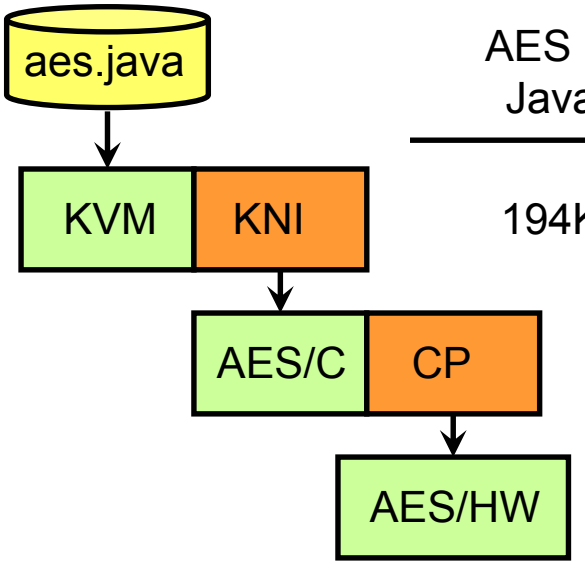




RINGS Programming Model based on Virtual-Machine Specialization



Example AES Top-Down Refinement

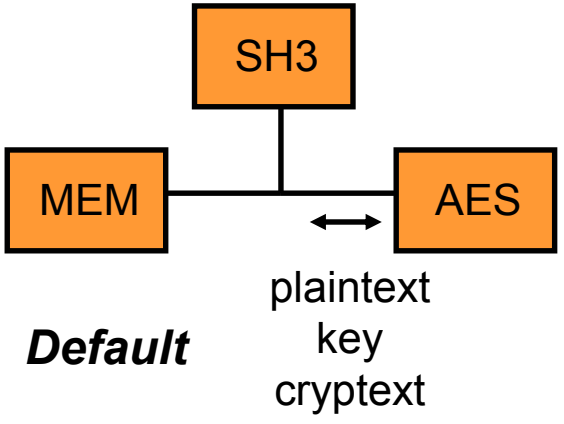


Cycle Count on KVM/LEON2-SPARC

	AES in Java	AES in C	AES in HW
	194K	10.1K	1.78K
		9.23K	797
			11
Speedup	1	19.2	109
Overhead	**na**	**1.1**	**162**

Also need to use data-level & instruction-level parallellism !

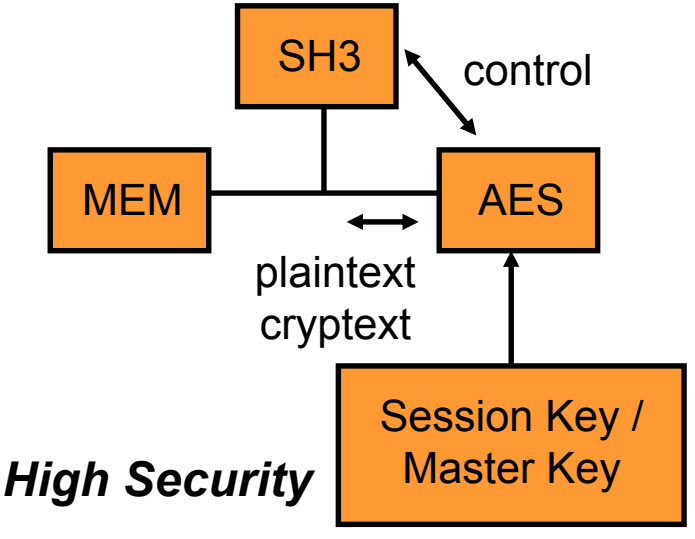
Data Parallellism: Security Example



Default

198 Kcycles (Java Only)
19.2 Kcycles (Java + HW AES)

Acceleration: 10X



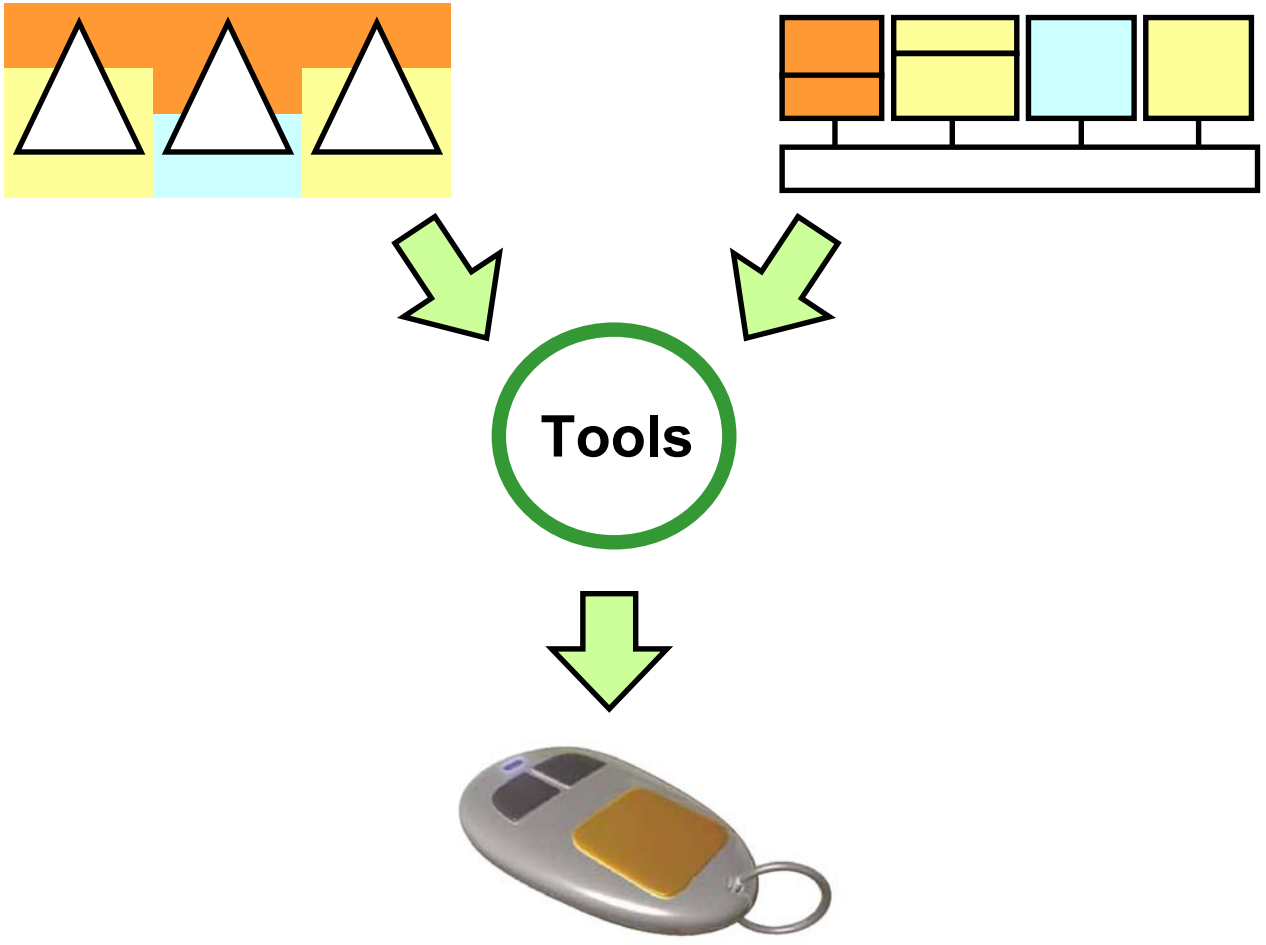
High Security

7.9 Kcycles (Java + HW AES)

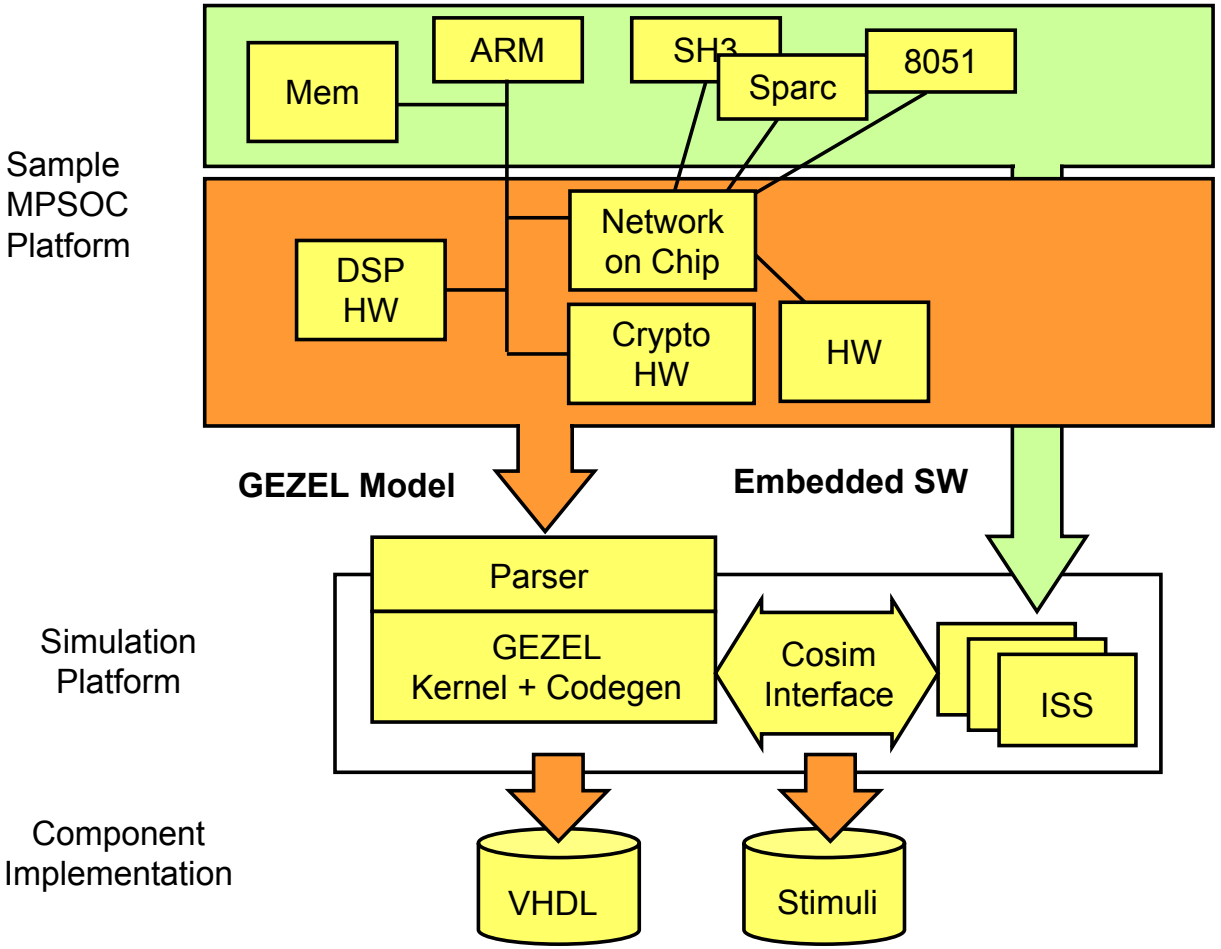
Acceleration: 25X

[by Yusuke Matsuoka]

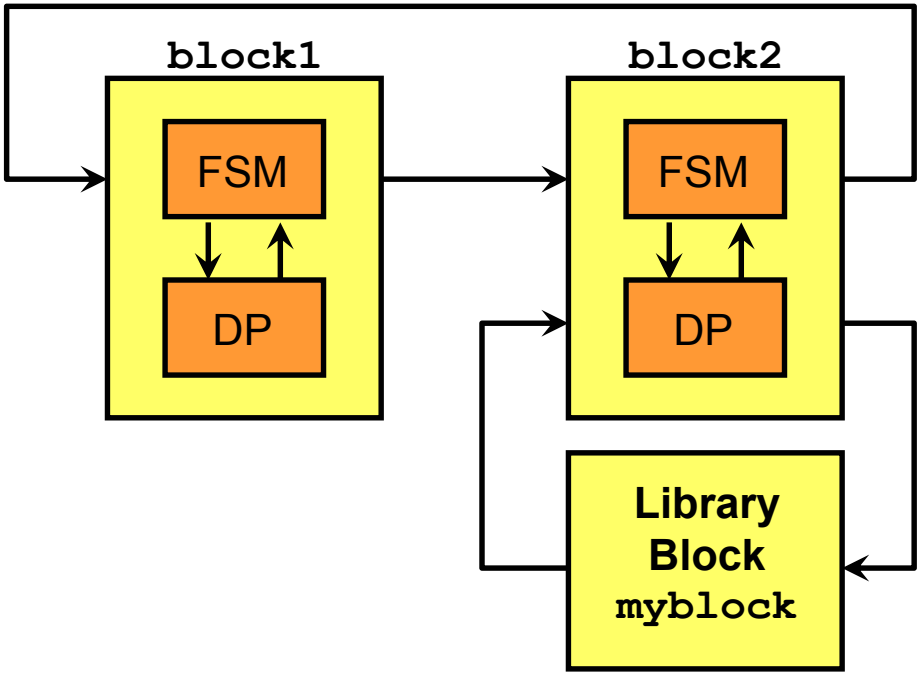
Design Technology Support



GEZEL: Design Environment for RINGS

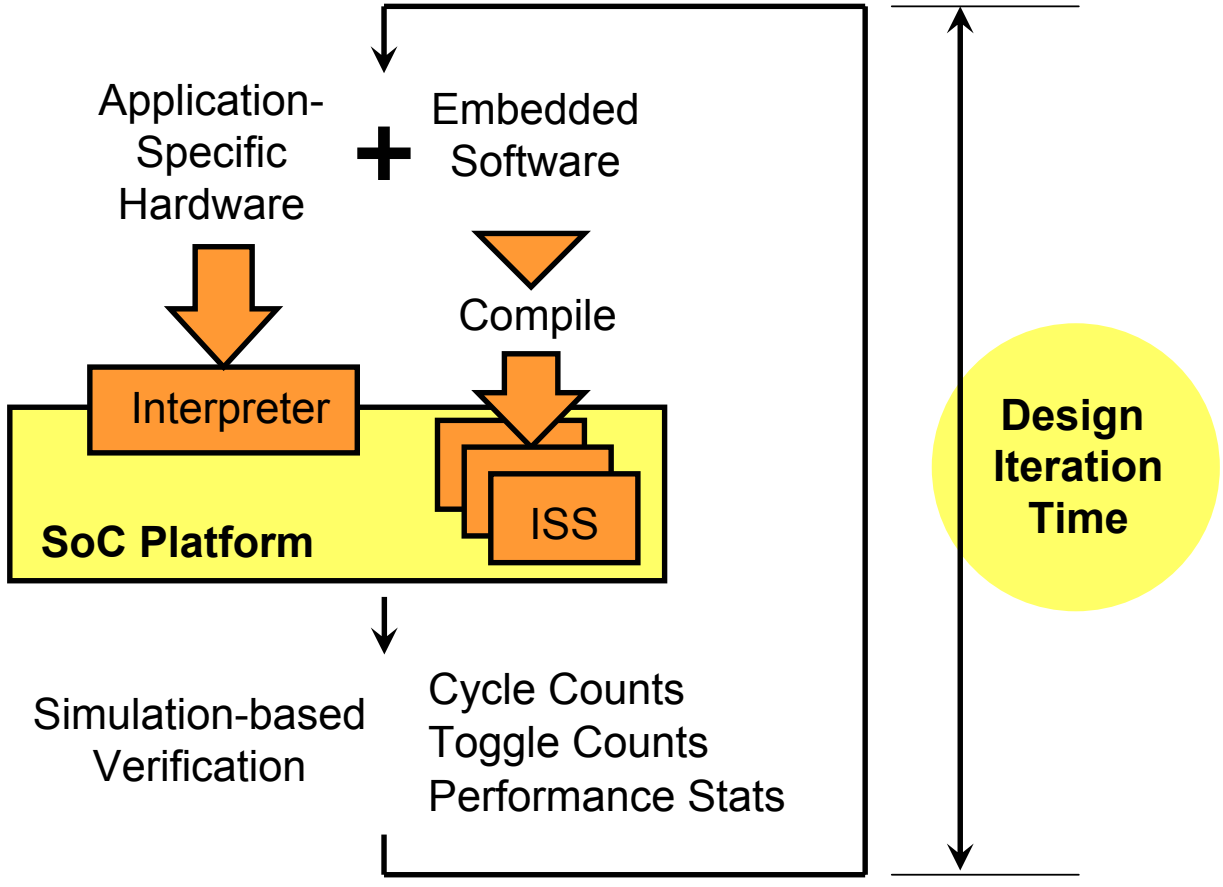


GEZEL Semantics use Comm. FSMD

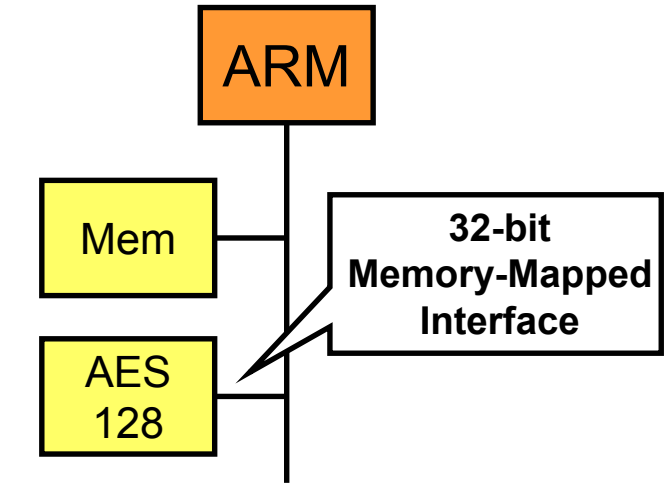


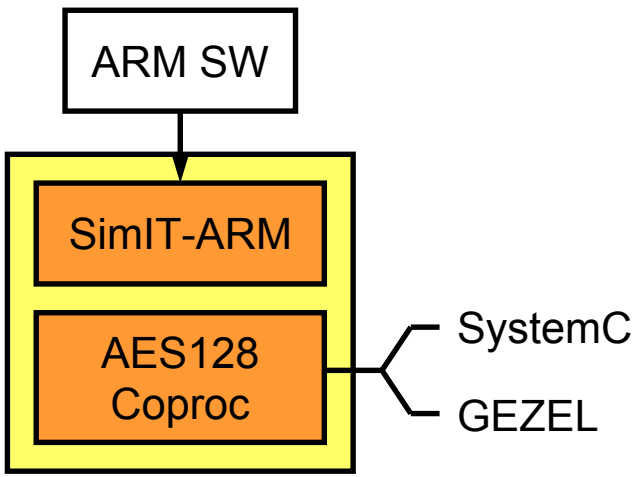
- FSMD = FSM + Datapath
- Cycle-true Hardware Model
- Library blocks (e.g. RAM, HW/SW and Cosimulation Interfaces, ..)

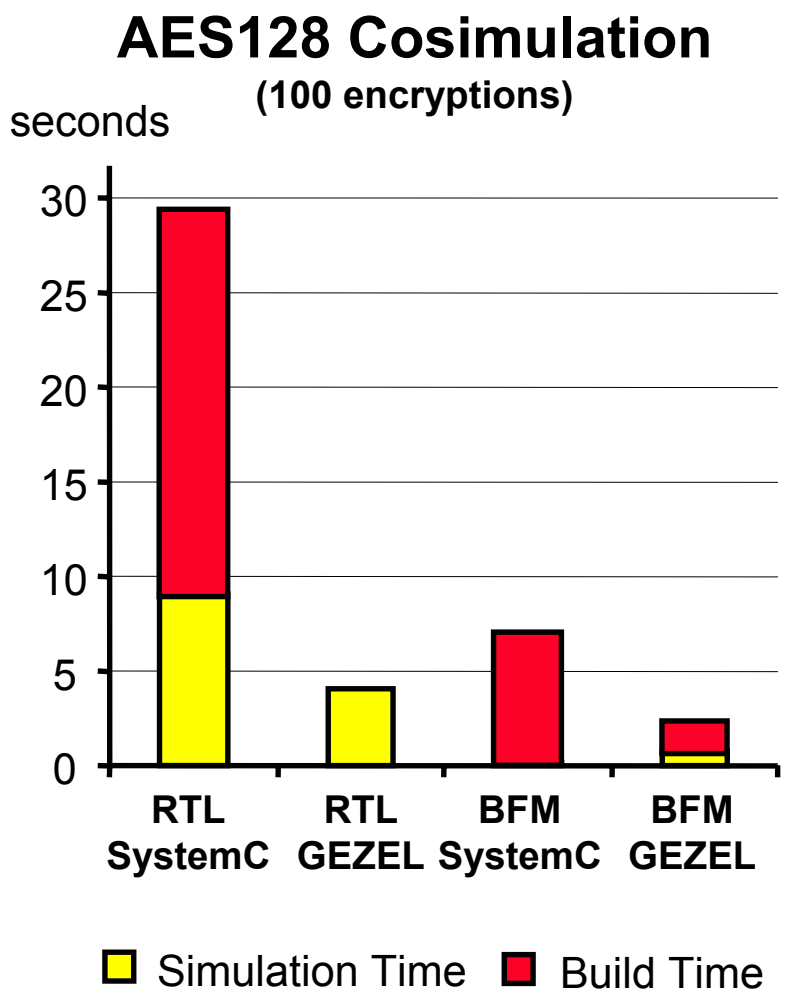
Efficient Cosimulation with GEZEL



Cosimulation Experiments







[DATE 2004]

GEZEL Applications: ThumbPod

bank

challenge

match

response

fingerprint sensor

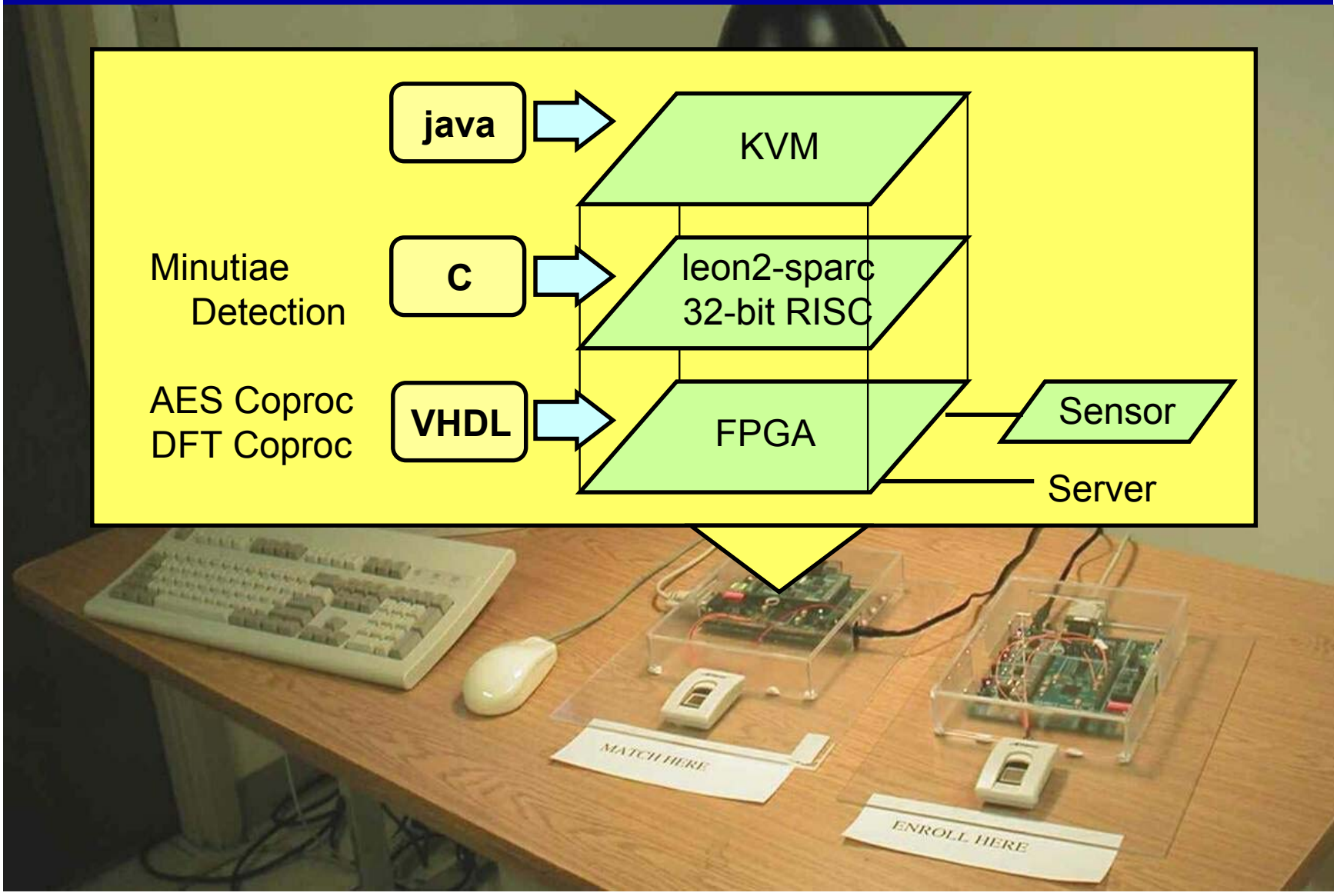
keychain

embedded processing security + biometrics

Secure Embedded Authentication

[DAC 2003]

ThumbPod Demonstrator Setup

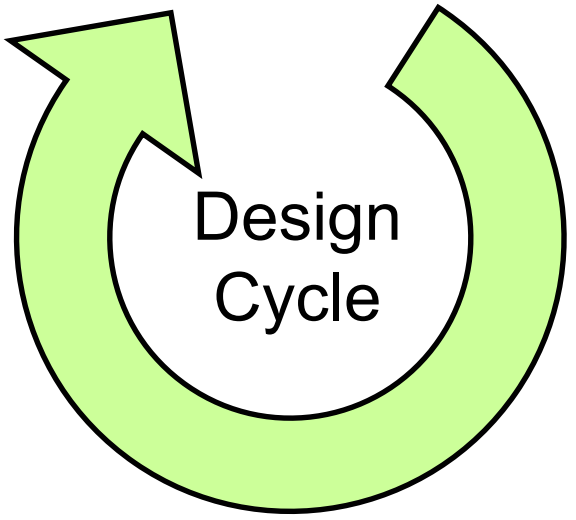


GEZEL Applications: Teaching

- **UCLA, *VLSI Architectures and Design Methodologies* (Verbauwhede)**
  - **Spring 2003: Embedded Webserver on ARM+GEZEL, LEON2+GEZEL**
  - **`http://www.ee.ucla.edu/~schaum/ee201a/`**
- **Danmark Technical University, *Introduction to Codesign* (Madsen & Steensgaard-Madsen)**
  - **Spring 2004: MIC-1 Microcontroller in GEZEL**
  - **`http://www.imm.dtu.dk/courses/02130/home`**

Conclusions

Codesign of Application Domains needs a trinity



Methods & Tools
GEZEL
& Dissemination

Applications
Thumbpod-1

Architectures
RINGS Architecture (Hardware)
Hierarchical Virtual Machine (Software)