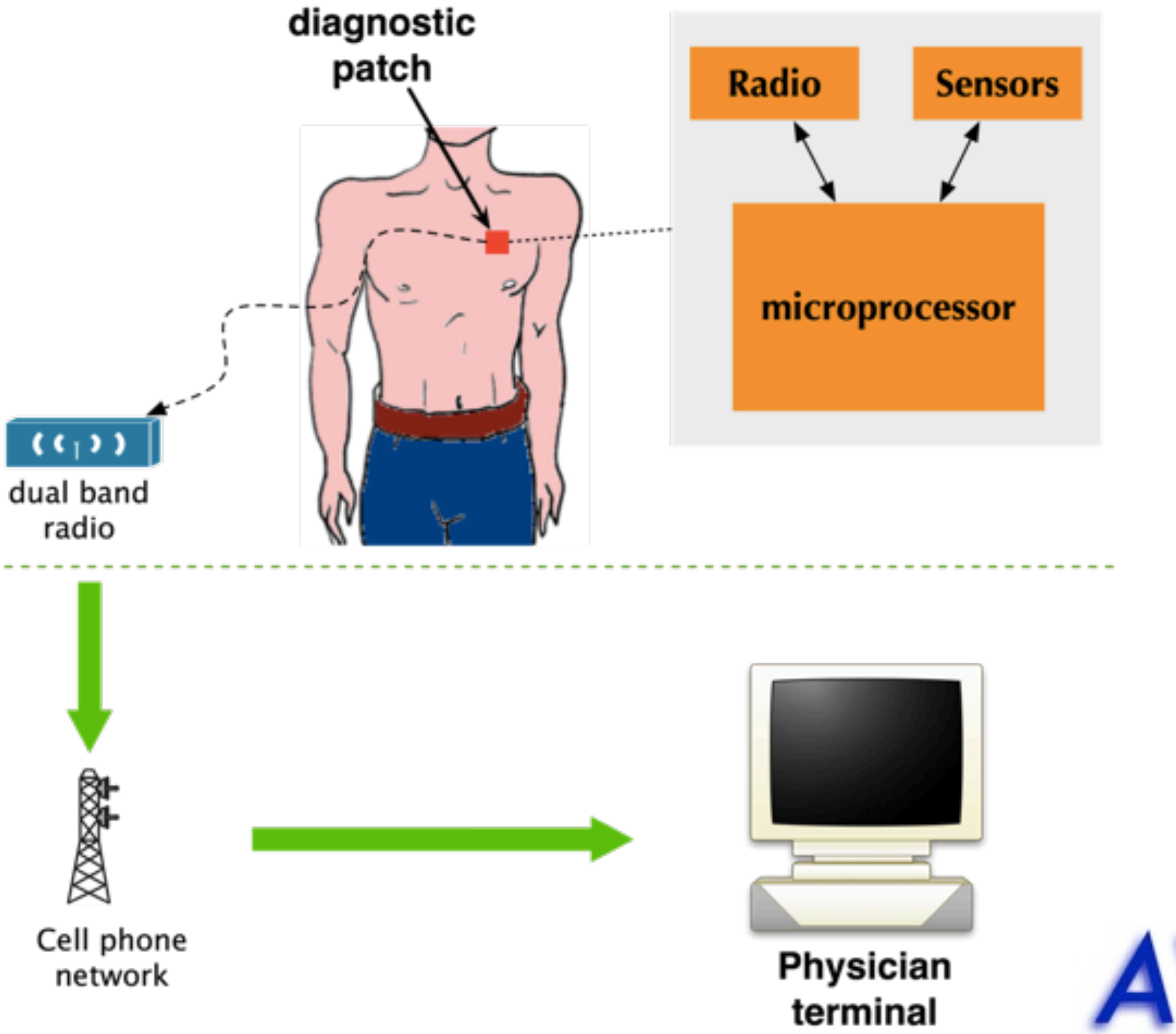
ULTRA LOW POWER COMPUTATION FOR SECURE EMBEDDED SYSTEMS

Rajit Manohar (Cornell)

Driver: wireless cardiac monitoring

- Continuous monitoring of biomedical signals
  - Eliminate wires
  - Improve quality of information

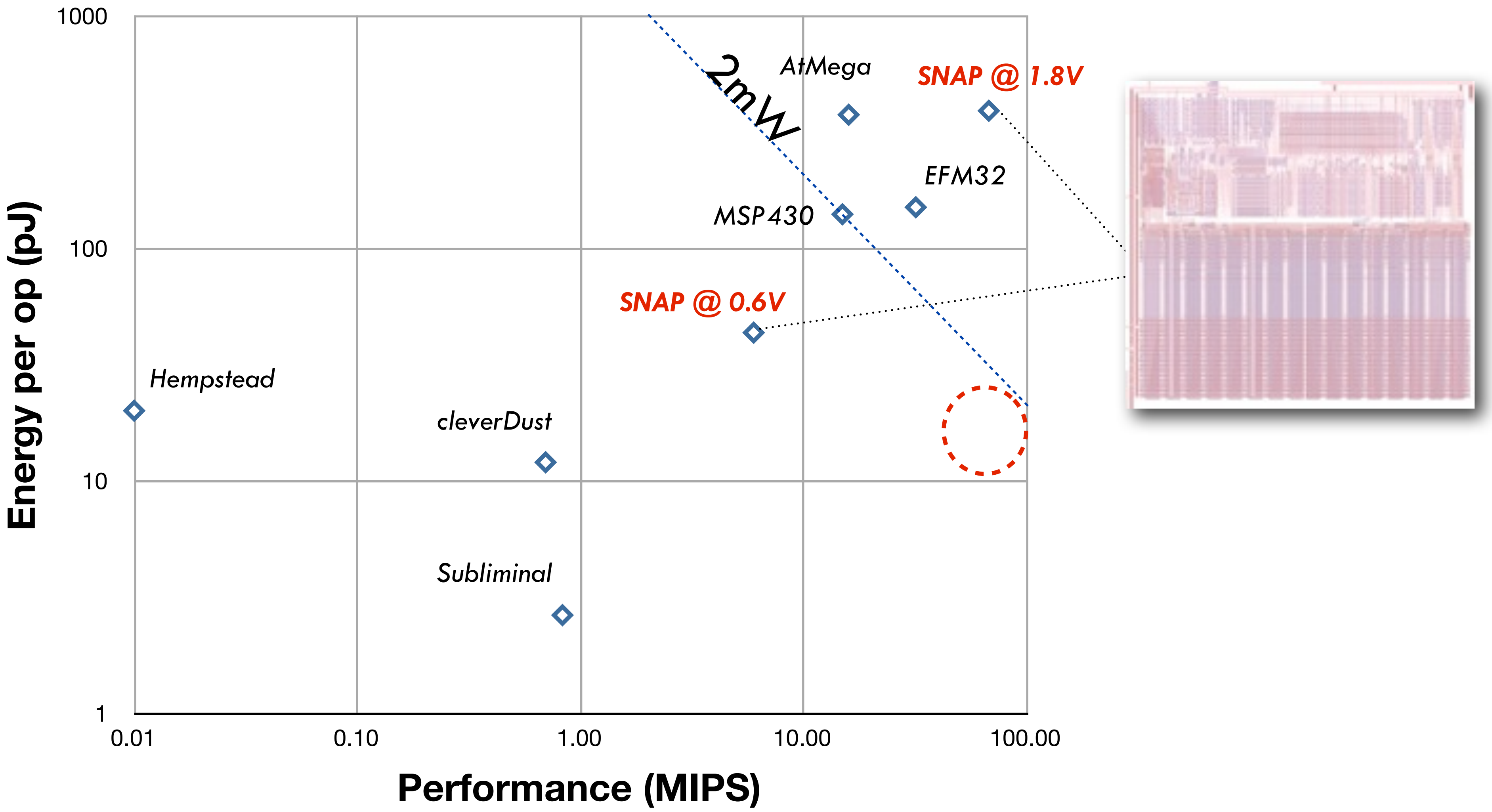


Basic requirements

- Sensing, processing, communication
  - Processing: ≈80 MIPS
  - High-fidelity cardiac sensor: ≈2mW
  - Wireless data rate: ≈10-100 Kbps (≈2mW)

- For reference
  - Li-Ion batteries: ~ 100-200 W-hr/kg

Existing embedded processors

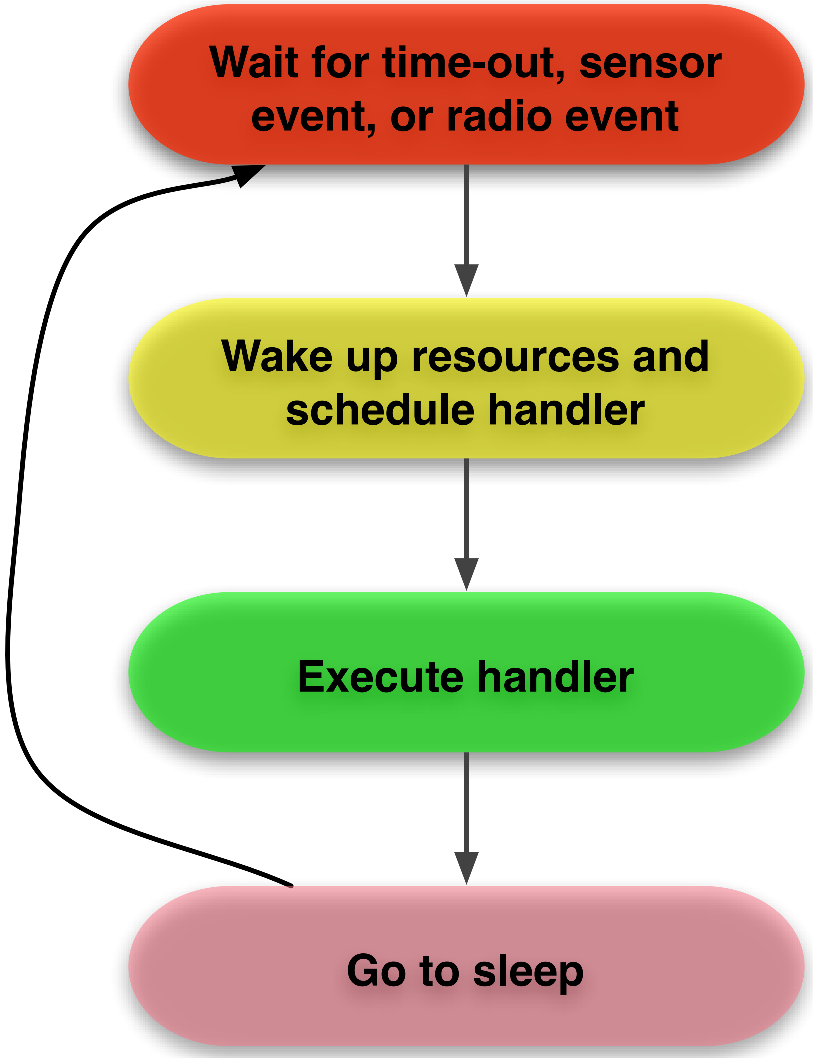


Gap: 50-100 MIPS

Hardware-software considerations

- Dynamic instruction count is low for pure monitoring apps

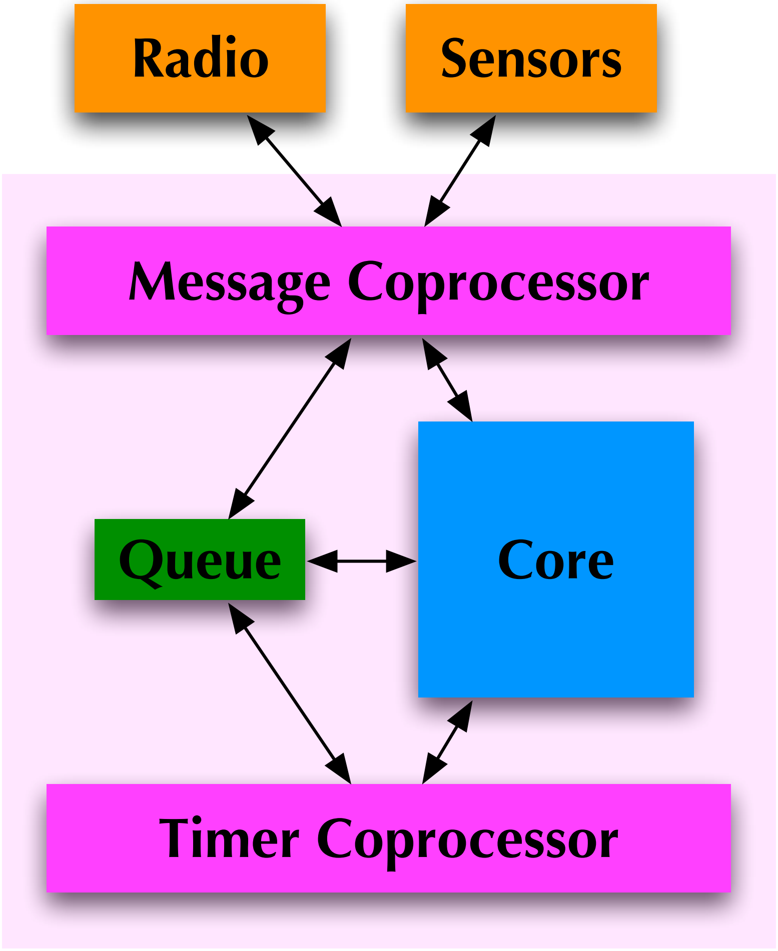
- Implications
  - Minimize run-time overhead
  - Make hardware resemble standard application structure


Wait for time-out, sensor event, or radio event
Wake up resources and schedule handler
Execute handler
Go to sleep

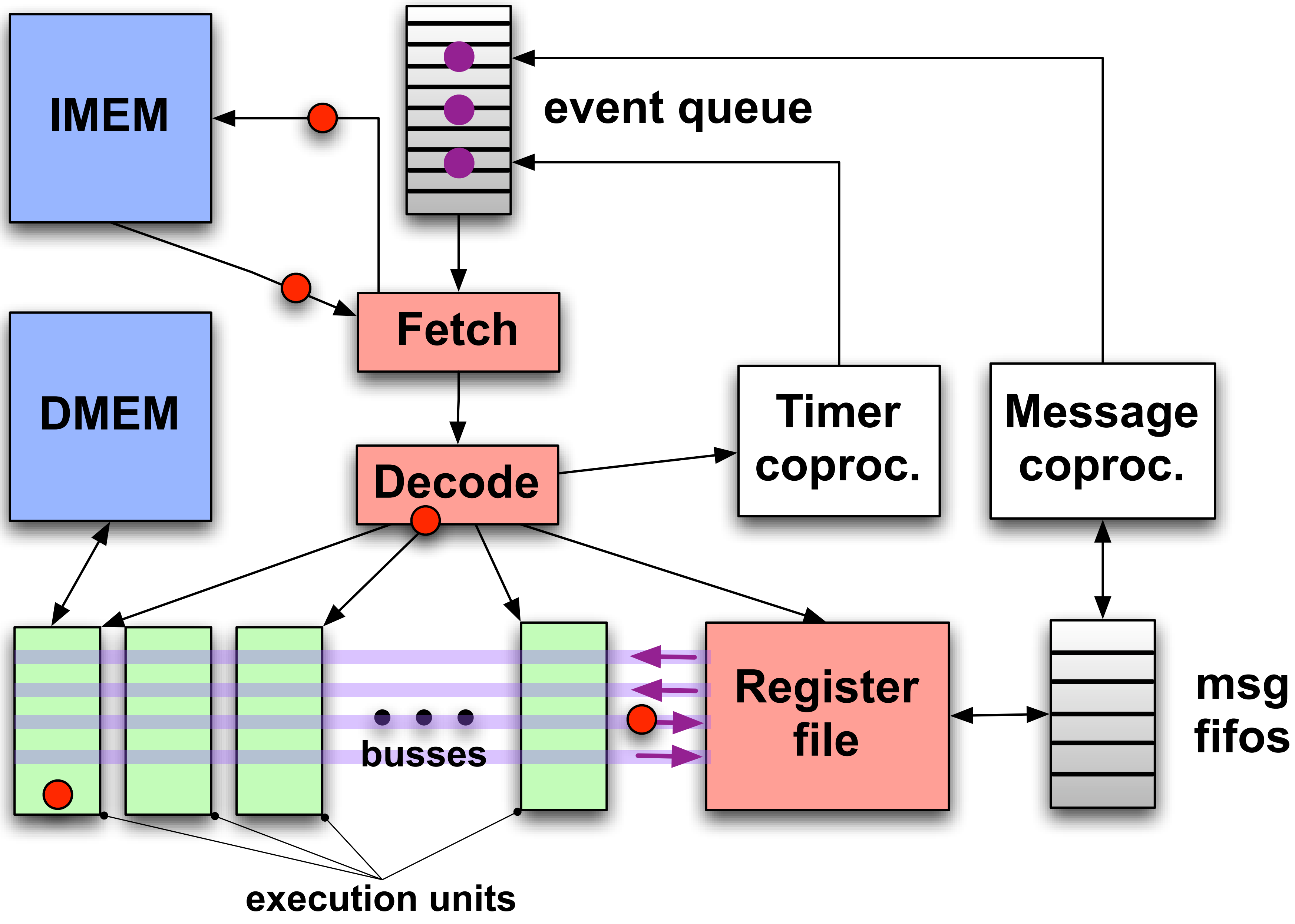
SNAP instruction set architecture

- Event-driven execution

  … all the way to the circuits!
  - Clockless logic
  - Hardware event queue
  - Hardware event-dispatch table
- On-chip timers
- Dedicated serializer/de-serializer for radio interface
- Interrupts translated into events



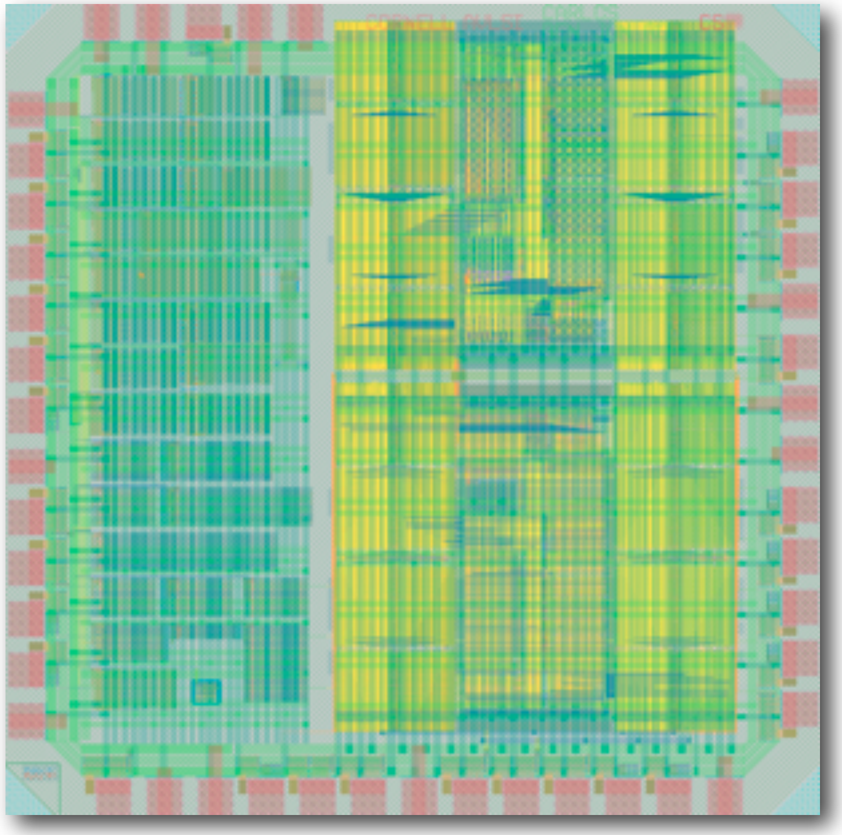
SNAP microprocessor architecture



Cornell University

SNAP2 design

- Circuit-level optimizations
  - 90nm process technology
  - Significant re-work of memory design
- Standard off-chip interface (SPI)
- In the works
  - External memory interface (designed)
  - Hardware AES (designed)



Hardware AES

- SNAP supports general co-processors
  - Message co-processor ("I/O mapped")
  - Radio, SPI uses this interface
  - … as does AES
- AES operation
  - Setup
  - Loop-back mode: encrypted data returned to processor
  - Inline mode: data encrypted to/from radio

Hardware AES

- Encrypting communications
  - Energy for communication: ≈1-10 nJ/bit
- AES-128 energy cost
  - Software: ≈1-2 nJ/bit
- Hardware AES-128 cost
  - Best previously reported: 68 pJ/bit
  - Our implementation: 16 pJ/bit
- “Free” compared to cost of communication

Future Work

- Low power secure random number generation
- Security-preserving circuit synthesis
- Low power GPS

- Thanks to…
  - Carlos Otero, Jon Tse, Nabil Imam, Rob Karmazin, Ben Hill
  - NSF and Blue Highway (Welch-Allyn)