The Internet of Things…
and Batteries, Hackers and CPU Architects, oh, and NVM

Lucian Shifren
ARM R&D
San Jose CA
What is the Internet of Things?

- Buzzword
- Trend
- Convenient Categorization
- Industrial
- Consumer
- Agricultural
- Medical
- Educational
- All of the above
Consultant says: IoT is the answer to EVERYTHING…
Things
Thing Today: Discrete Components

Will only get more embedded!

- Charger
- Host MCU (inc. Flash, RAM, ADC)
- MEMS Sensor (Accelerometer)
- Radio (inc. CPU)
Energy

PROBLEM #1
Batteries Don’t Follow Moore’s Law

1998 Nokia 5110

- Screen 47x84 B/W display
- 64K RAM, 1MB Flash
- 16 buttons
- Entertainment – ‘Snake’
- Battery 900mAh

2012 Samsung Galaxy S3

- 4.8inch 1280x720 HD display
- 2GB RAM, 16GB Flash
- Touch screen input
- 8-megapixel camera with HD video
- 2D/3D graphics acceleration
- Stereo speakers with 3D audio
- Battery 2100mAh
Use Cases Imply Power Envelope

- Smaller batteries lasting longer? All depends on usage
- Some IoT devices need to last years (e.g., distributed sensors)
- Let's all agree, more battery life is always a good thing
What’s the Real Problem?

HP >
Cost >
Top Speed >

NO
GOOD

GOOD

The Architecture for the Digital World®
What’s the Solution

More HP?

“Fix” Track?

The Chassis?

This one!
Cortex-M0 Energy/Cycle

- Cycle 10000 logic gates same energy as writing/erasing 1 bit of FLASH
- FLASH is a huge problem as it’s energy does not scale
- IoT devices need to last longer on smaller batteries
Security

PROBLEM #2
Everything Connected

Big Data
Internet of Things

Must be safe, seamless and simple

Services

- Power efficient servers
- Fast, high capacity storage
- High throughput networks
- Low power wireless networks
- Integrated sensors and computing
- Ultra low power systems

The Web

Things

Little Data
Data Ownership and Protection

My Fridge → My Data → Me, My House, My WiFi Router

My Fridge → My Data → My Gym/Dietician

My Fridge → My Data → My Bank

My Fridge → My Data → My Life Insurance Holder

My Fridge → My Data → Coupon Companies

My Grocery Store → Their Data

My Fridge → Their Data

My Fridge → Their Data

My Fridge → Their Data

My Fridge → Their Data
Oh Boy!

Belkin WeMo smart home networks in danger of hacks

Researchers warn that more than 500,000 home automation devices have vulnerabilities that would allow attackers to remotely take control of thermostats, lighting, sprinkler systems, and more.

by Dara Kerr @denkerr / February 18, 2014 6:10 PM PST

NEWSFEED BIZARRE

Stranger Hacks Into Baby Monitor and Screams at Child

Olivia O. Waxman @OBWax / April 28, 2014

- Your “things” need the same security as your bigger things, no matter how much or little they cost
- Cliché time: “you are only as strong as the weakest link”
Cost is Key in Security

- Security needs NVM and FLASH is very expensive (cost and energy)
- OTP does not allow firmware/security updates
- IoT much more cost sensitive to security requirements
Endurance
PROBLEM #3
Memory and CPU Today

- Memory hierarchy retained, levels are added (such as eDRAM) but the hierarchy is untouched

![Memory Hierarchy Diagram]

- Processor
  - eDRAM
  - DRAM
    - EDO, SD-RAM, DDR-SDRAM, RD-RAM and More...
  - CPU Cache
    - Level 1 (L1) Cache
    - Level 2 (L2) Cache
    - Level 3 (L3) Cache
  - Physical Memory
    - Random Access Memory (RAM)
  - Solid State Memory
    - Non-Volatile Flash-Based Memory
  - Virtual Memory
    - File-Based Memory
  - SSD, Flash Drive
  - Mechanical Hard Drives

- Flops
- Temporary/volatile
- Persistent/non-volatile
## Wanted: Super Memory

<table>
<thead>
<tr>
<th></th>
<th>SRAM</th>
<th>DRAM</th>
<th>NAND</th>
<th>SuperMem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area (F^2)</td>
<td>~120</td>
<td>4-6</td>
<td>&lt;4 (eff)</td>
<td>&lt;=6</td>
</tr>
<tr>
<td>Write Speed</td>
<td>&lt;300ps</td>
<td>10ns</td>
<td>50ns+</td>
<td>&lt;1ns</td>
</tr>
<tr>
<td>Read Speed</td>
<td>&lt;300ps</td>
<td>10ns</td>
<td>10ns</td>
<td>&lt;1ns</td>
</tr>
<tr>
<td>Leakage</td>
<td>High</td>
<td>Low</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active Power</td>
<td>“Low”</td>
<td>Low</td>
<td>High (write)</td>
<td>Low (1pJ/bit)</td>
</tr>
<tr>
<td>Nonvolatile</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>High Voltage</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Logic process</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Endurance</td>
<td>Infinite</td>
<td>Infinite</td>
<td>10^5</td>
<td>&gt;10^15</td>
</tr>
</tbody>
</table>

- Super Memory needs to scale
- No alternative (yet) for embedded SRAM, but nonvolatile would have big implications
- Which will win? MRAM? RRAM? TBDRAM?
Detectability is a measure of the difference between 0 and 1 (how much ECC/write/read assist needed)

Speed is indicative of read/write performance

= Super Memory
The State of the Art (Part 2)

- Retention for STT is on the order of weeks/months (depending on write), RRAM etc. is on the order of years
- Cost includes area plus processing/test
Endurance Requirements for System Memory

- Endurance is most likely limiter to universal memories
- Many IoT devices will have low enough cycling that new NVM could be universal (need at least $10^{10}$)
- This could allow ultimate power management (instant on/off with all memory non-volatile)
Wrap Up – Where We Stand

- Could we land up with a mix of flavors?
  - Charge RAM (the incumbents): Flash, DRAM, SRAM
  - Resistive RAM: RRAM, CBRAM, PCM, CeRAM
  - Magnetic RAM: STT-MRAM, FeRAM, TAS-MRAM

- For MCU/IoT NVM
  - RRAM preferred due to cost/density
  - DRAM replacement leaning towards MRAM
    - If MRAM replaces DRAM, will replace FLASH (and ReRAM) too
    - SRAM replacement is SRAM

- New NVM could influence future CPU architectures especially in the low power arena