Networked Embedded System Platforms in the Post-Mote Era

Pat Pannuto†, Michael P Andersen‡, Tom Bauer§, Bradford Campbell† , Amit Levy§
David Culler‡ Phillip Levis§ and Prabal Dutta†

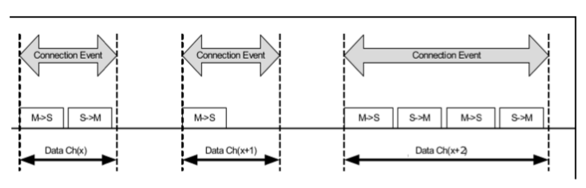
†Computer Science & Engineering
University of Michigan

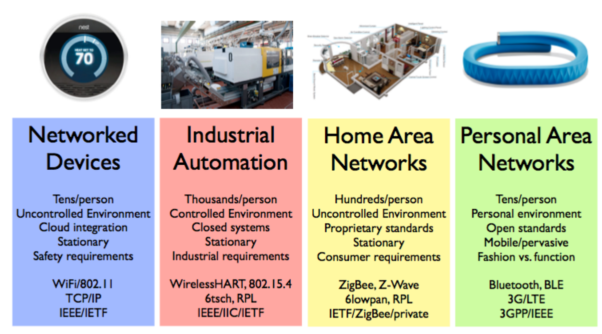
‡Computer Science & Engineering
University of California, Berkeley

§Computer Science & Engineering
Stanford University

Technology Transformations

New Networks: Integrating TinyOS and Bluetooth Low Energy





BLE provides highly efficient beaconing, bidirectional communication, fast device discovery, authentication, and optional pico-network formation and management [3]. BLE explicitly incoporates ideas of periodic beacons and duty cycles, such that a device with a wakeup latency of a second can have an average current draw of < 40 μA.

Integrating an event-driven OS with manufacturer-provided software is a challenge that a post-mote platform must address.

New SoCs: Cortex M0–M4

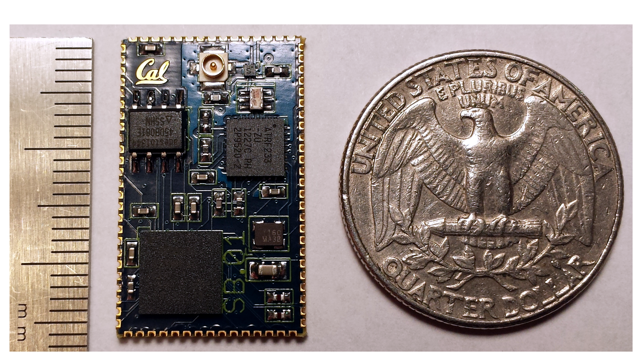


Table 4: A small sample of available Cortex-M4 processors

Vendor	Device	f_{max}(Mhz)	SRAM(KB)	Flash(KB)	Sleep(μA)	Wake(μS)
NXP	LPC408x	120	96	512	550	240
STMicro	STM32F372xx	72	32	256	1.32	42.7
Silabs	EFM32WG990	48	32	256	0.95	2
Freescale	K20Dx	50	16	128	1.3	130
Atmel	SAM4L	48	512	64	3	1.5

Table 5: Key metrics for select radio transceivers

Year	Vendor	Device	TX (dBm)	RX (dBm)	Wake (μs)	Sleep (mA)	TX (mA)	RX (mA)	CCA	AES	Auto ACK	Auto RE-TX
2013	Atmel	RF233	+4	-101	450	0.02	13.8	11.8	Y	Y	Y	Y
2007	Ti	CC2520	+5	-98	500	¡1	33.6	24.8	Y	Y	Y	N
2013	Freescale	MKW24D512V	+8	-102	-	-	18	19.5	Y	Y	-	-

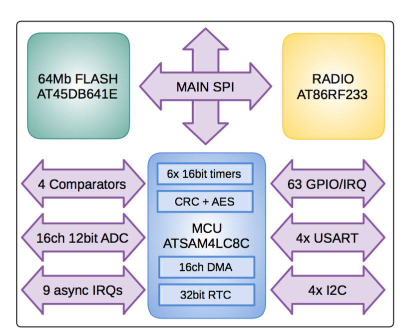
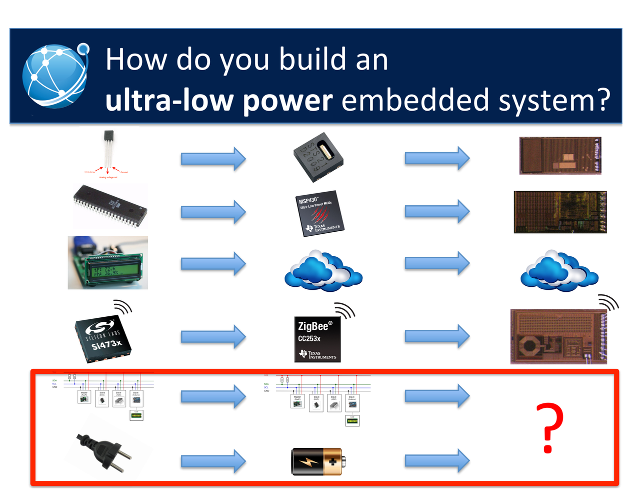


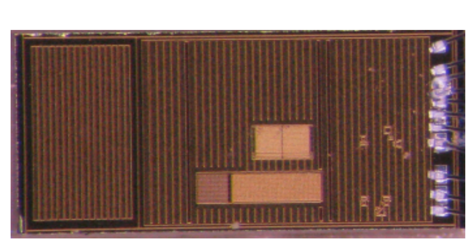
Figure 1: The Storm platform architecture

Advancement in MCU technology has widened the field of low-power processors which now ranges from highly performant cores such as the 1 μA–30 mA, 0.5– 120 MHz Atmel SAM4S with a Cortex M4, 2 MB flash, and 160 kB SRAM to highly efficient cores such as the 5 nW– 10 μA, 1–8 MHz M3 research chips [4] with a Cortex M0 and 16 kB of memory.

The post-mote OS will need to devise new means to efficiently abstract optimal power management for these more complex chips and leverage the new features when available without sacrificing its utility for less feature-rich, constrained systems.

Impact of Energy Harvesting

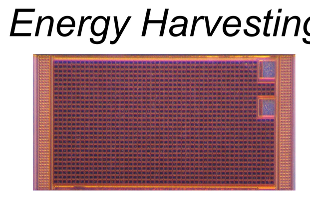




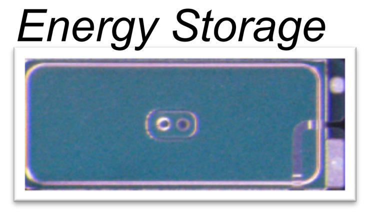
Temperature Sensor:
~10 pW standby, < 1 μW active

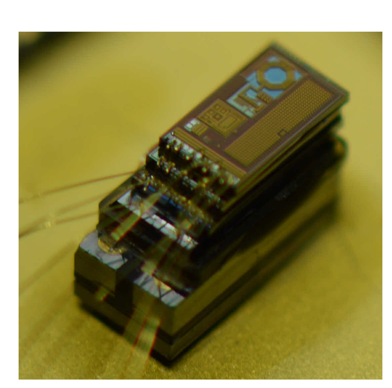
MCU
~1 nW sleep, ~1 μW active

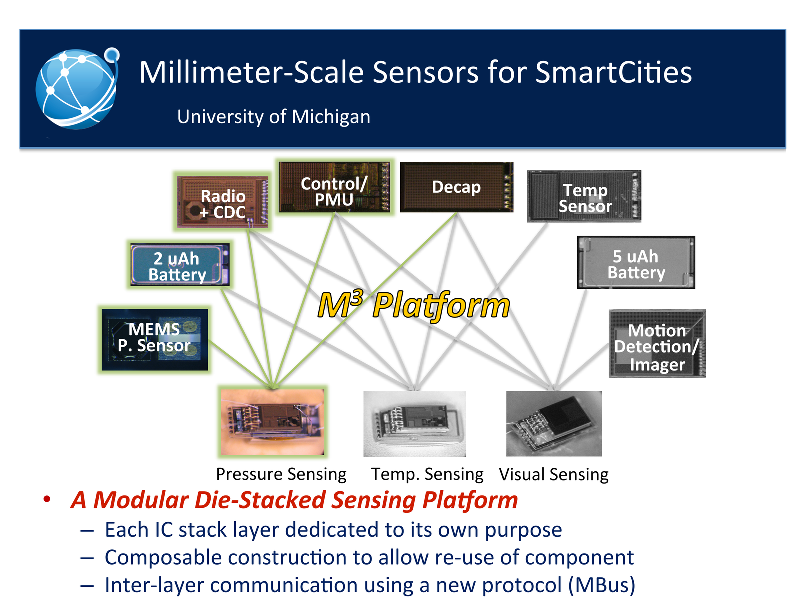
Energy Harvesting



Energy Storage



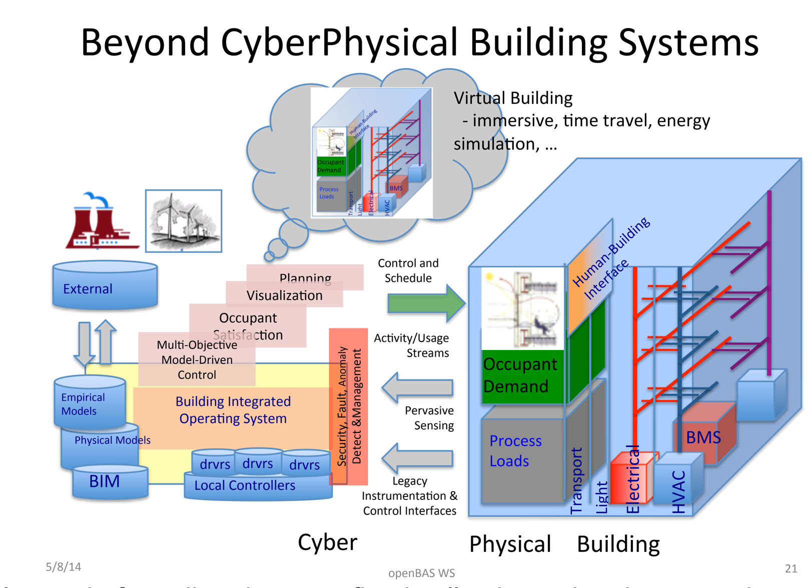




A decade of research in energy-harvesting transducers, efficient power electronics, and compact energy storage technologies, coupled with reduc- tions in the idle and active power of radios, instant-on/instant- write phase-change memory, and the efficacy of modern MCUs make compact energy-harvesting sensors that can run perpetually, even in indoor settings, a reality

Applications Transformations

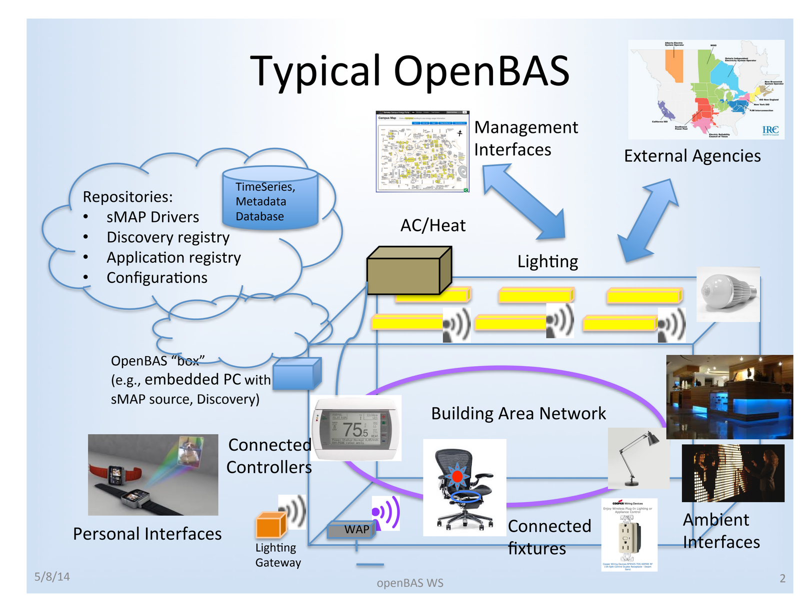
Human-centric

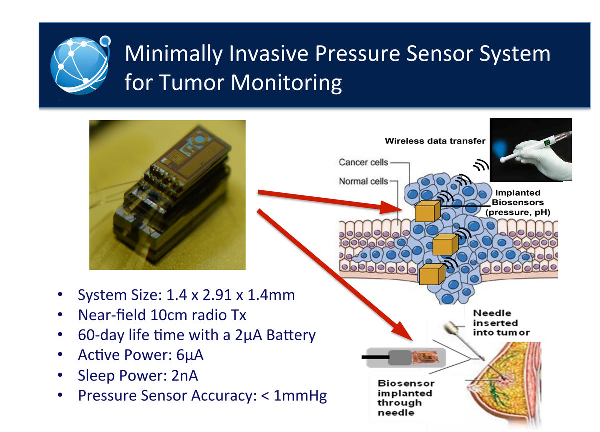


The mobile device is a gateway to an embedded network. Instead of sending data to a fixed collection point, the network can send directly to a mobile device, on demand.

These new application requirements will force us to rethink the tradeoffs between latency, storage, energy, snooping, and how an OS will support them.

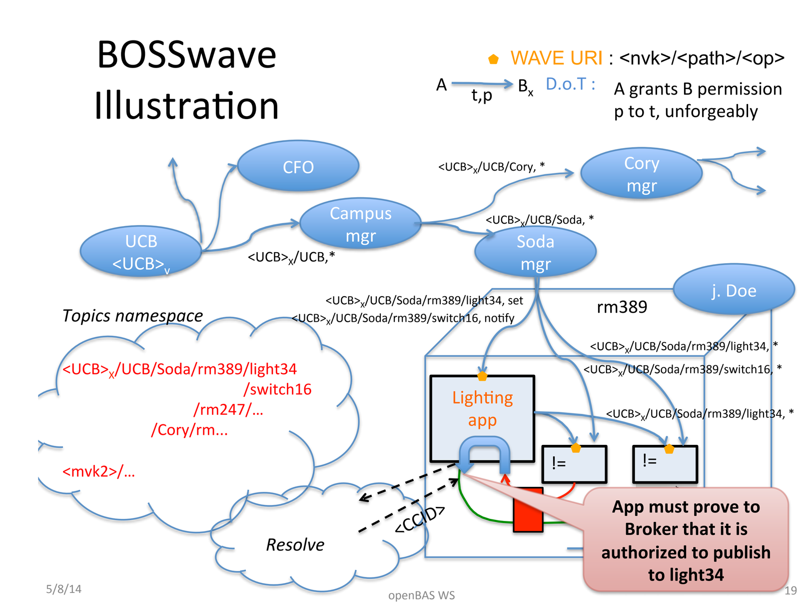
Perpetual Networks.





Energy harvesting and low-power pe- ripherals will finally enable a long-term goal of sensor networks: perpetual networks. Imagine iBeacons and smoke detectors that need no battery replacements. If the world will be filled with thousands of smart objects per person, energy must recede to be a non-issue for almost all of them.

Privacy and Proximity in Networks



Interactions between PANs (centered around a users mobile phone) and proximity applications such as iBeacons happen in public, with never-seen-before peers. This presents a dual security and privacy problem. On the one hand, connections between the PAN and proximity device must be confidential and authentic – e.g. payments. On the other hand, casual interactions with proximity devices must not enable ubiquitous tracking of users. Unfortunately, confidential and authentic communication and anonymity are difficult to achieve simultaneously. Operating systems can play a role in addressing these issues, for example by coordinating security features in the BLE stack with application specific knowledge.