Anatomy of modern cell phones

the 2012 update of the 2010 paper about 2005 phones ;)

Harald Welte <laforge@gnumonks.org>

gnumonks.org
hmw-consulting.de
sysmocom GmbH

August 8, 2012 / OSmocom Berlin User Group

Outline

1. Classic GSM phone architecture
2. Evolution to Smart Phones
3. Current situation and trends
4. Smart Phone on a Chip

About the speaker

- Using + toying with Linux since 1994
- Kernel / bootloader / driver / firmware development since 1999
- IT security expert, focus on network protocol security
- Former core developer of Linux packet filter netfilter/iptables
- Board-level Electrical Engineering
- Always looking for interesting protocols (RFID, DECT, GSM)
- OpenEXZ, OpenPCD, Openmoko, OpenBSC, OsmocomBB, OsmoSGSN

The classic GSM phone design

- Classic GSM mobile phones didn't really change much for 10 years from 1992 to 2002
- RF circuitry for analog RX and TX (mixers, filters, PA)
- DSP for radio modem, mostly Rx side, hardware modulator
- Microcontroller (often ARM7TDMI) for protocol stack + UI
- VCTCXO for clock generation
- Serial Port with AT-commands over RS-232

Improvements in classic GSM phone design

- DSP was becoming faster, permitted better voice codecs
- DPS and controller merged in one chip/component to simply PCB design
- Improvements on analog side from IF to zero-IF to low-IF designs
- Smaller silicon processes for power and space savings

Personal Digital Assistants

- In the late 1990ies, PDAs became popular (Palm, Sharp, Compaq, ...)
- A PDA was a mostly pen-operated embedded device with large screen
- PDAs only had RS-232 to sync with desktop PCs but no wireless interfaces
- Some people connect your PDA over RS-232 to the mobile phone
- But: Until 2000, SMS and CSD was the only data transport medium

From classic phone to smart phone

- Companies started to put a phone and a PDA in one case
- Interconnection between still a normal UART with AT commands
- Phone part had keyboard and display removed, AT commands are only interface
- OS on PDA side much more powerful than OS on phones at that time (PalmOS, Windows CE / PocketPC, ...)
- PDA-side CPU called *Application Processor* (AP)
- Phone-side CPU called *Baseband Processor* (BP)

smart phone evolution

- GSM phone (now called "modem") gets GPRS, later EDGE support
- AP gets faster (from m68k/arm7tdmi to ARM920, ARM926, ARM11....)
- Color displays, higher resolutions
- Mobile GPUs for video encoding/decoding, cameras, ...
- Resistive touch screens replaced by capacitive touch
- AP OS more full-blown (Linux, iOS, ...)

Baseband processors: An abuse of feature phone SoCs!

Until almost the end of the 2000's,

- BPs continue to be made primarily for feature phones
- BPs thus still contain keypad scan matrix, display interface, etc.
- BPs external interfaces are primarily developed for connecting the feature phone to a computer, i.e. USB.

Only recently, smart phones have been so popular that BPs are designed with them as a primary user!

AP / BP memories

- AP and BP are separate SoCs
- they each have their own address/memory bus and flash memories
- those memories traditionally are in separate components for AP and BP
  - often an integrated NOR+SRAM (later NAND+SDRAM) for the BP
  - SDRAM + NAND (later mDDR + eMMC) on the the AP
- You can still see the 'two brain syndrome' from the DPA + featurephone legacy

2012 smart phones

- Has AP with two or four cores (Exynos 4412, Tegra 3, ...)
- Has BP with ARM1176 core (better than AP some years ago!)
- Still have the separation of AP and BP processor
- Often still use AT commands to control the BP
- Normally don't use UART physical interface anymore, as it's too slow for HSPA speeds

AP/BP interfaces

Many different variants exist today:

- **USB** e.g. used around 2005/2006 by Motorola EZX
- **MIPI HSI** High-Speed serial interface designed specifically for phones
- **HSIC** A different USB physical layer (from usb.org)
- **DPRAM** Dual-Ported RAM

AP-BP IF: Universal Serial Bus

- full-speed USB significantly better than UART speeds
- AP SoC often contained USB host controller anyway
- BP (made for feature phones) also had USB instead of UART for PC connection

AP-BP IF: MIPI HSI

- HSI: High-Speed Synchronous Serial Interface
- MIPI Alliance is a vendor consortium in the mobile space
- They specify a variety of other interfaces, e.g. for display, battery, camera, ABB/DBB, ...
- Adoption of MIPI HSI not very big (yet?) today

AP-BP IF: HSIC

- High-Speed Inter-Circuit specification from USB forum
- removes USB phy for transmission over long wires
- can transport high-speed USB (480 Mbits)
- regular USB protocol stack on AP and BP
- primarily used by Samsung for Infineon XGold BP

AP-BP IF: Dual-Ported RAM

- A RAM component with two separate Address and Data busses
- Shared-Memory mailbox protocol between AP and BP
- Lots of bus routing on PCB
- Some AP have DPRAM internal and connect one side internally to the AP CPU core on the die
- Very good match for SPoC (Smart Phone on a Chip) like Qualcomm MSM

Smart Phone on a Chip (SPoC)

Around the time the Google G1 came out

- Qualcomm was offering the first integrated SPoC (MSM7200)
- Integrate AP and BP CPU core + their peripherals on one chip/die
- Important for reducing required PCB footprint in devices
- Important for reducing PCB routing requirements
- Enables deeper integration between AP and BP

SPoC AP-BP integration

- So far, AP and BP had their own SoCs, address/memory bus, memories, etc.
- With SPoC, you can simply use the same RAM and flash chips, and somehow divide them between AP and BP
  - part of the physical RAM is mapped into AP, another part into BP
  - part of the flash is accessed by the AP, another part by the BP
  - added benefit: you can map some RAM into both, and get a DPRAM-like shared memory mailbox interface for the AP-BP interface

SPoC industry politics, 1/2

- For years, ST-Ericsson only alternative to QC with integrated AP+BP (U8500)
  - Infineon never had an AP business, only BP
  - Samsung System LSI never had a BP business, only AP
  - Nokia has been sleeping too long, then sold off their BP to Reensas
  - TI had a GSM/GPRS/EDGE BP business until 2008, then closed it down
  - NXP sold off their BP business and merged it with ST, later Ericsson Mobile Platforms (EMP) joined to create ST-Ericsson. They all lack a BP business

SPoC industry politics, 2/2

- Industry politics, continued
  - Broadcom has APs, but never been very successful in the BP market
  - Intel once had an AP business (X-Scale, PXA25x,26x,27x), but sold it to Marvell
  - Marvell had integrated AP + GSM/GPRS/EDGE BP, but no WCDMA
- Do you understand why Intel bought the Infineon BP business?

Industry finds SPoC alternatives

Samsung

If you cannot get AP+BP in one package, you have to be innovative

- Samsung has long successful AP line (s3c24xx, s3c6410, Exynos)
  - They also build mDDR and NAND flash as well as SD card controllers
  - They build MCP (Multi Chip Package) with multiple dies in one package
  - Reduces need for external memory components, simplifies PCB routing

Industry finds SPoC alternatives

Texas Instruments

If you cannot get AP+BP in one package, you have to be innovative

- TI has successful OMAP3/OMAP4 AP business
  - They have no RAM/flash business, thus cannot do MCP
  - They start with PoP (Package on Package)
  - Idea: expose memory interface on top of SoC, then solder memory BGa on top of SoC
  - Saves PCB footprint and simplifies routing, but adds height!

Have it the Mediatek way

The MTK GSM/GPRS/EDGE chipsets

- Users want features, they don't care about separate AP/BP
- So instead of adding an AP to a feature phone, just add all the peripherals and software to the BP
- Result: ARM7TDMI, later ARM920-EJS BP with hardware codec, GPU, lots of memory, JAVA, ...
- Lots of applications like web browser, mail, games to make it look like a real smartphone
- You save a lot in silicon footprint and ARM core licensing
- Shipped up to 90 Million units / quarter !

Mediatek 3G Evolution

- Mediatek buys BP business from ADI (Analog Digital)
- This most likely included Blackfin-based 3G baseband
- Modern MTK chipsets are SPoC, with ARM9/ARM11 on AP side and ARM9 on BP
- Shared memory components akin to Qualcomm solution
- How can MTK become successful once they sell outside China (WCDMA patent licenses to QC?)

The ST-Ericsson low-cost solution

- Use a single CPU core for AP and BP
- Run a hypervisor on it to virtualize the hardware
- Run BP OS in one guest compartment, AP in another
- Save on silicon cost/size and ARM core licensing like MTK
- Used in very few phones

AP/BP chipset market distribution

Out of 70 phone models available on German market today,

- Distribution by vendor
  - 47 are Qualcomm BP based (mostly SPoC)
  - 17 are Infineon BP based (BP-only)
  - 5 are ST-Ericsson based (SPoC / 2 core)
- Distribution by AP/BP interface
  - 54 use shared memory interface
  - 8 use HSIC or USB
  - 4 use MIPI HSI

Careful: This is per models. Some models sell more units than 10 other models together ;)

Thanks

Thanks for your attention. I hope we have time for Q&A.