论山寨手机与 Android 联姻的技术基础

By Sunny Cheng cheng.sunny@gmail.com and Kan Deng kan.deng@gmail.com

山寨手机的兴起，离不开 MTK (联发科)。MTK 为手机制造提供了一揽子解决方案，其中既包括硬件，也包括软件。软件方面最重要的，是操作系统。MTK 方案的软件的稳定性非常高，一方面是因为其硬件系统变化不大，另一方面，得益于 MTK 在系统软件上投入的巨额的资金和大量的人力。MTK 采用的操作系统是 Nucleus RTOS。Nucleus 的优势主要在于占用 CPU 时间短，以及占用 Memory 空间少。随着手机硬件的发展，Nucleus 的优势不再那么重要，而日益突出的问题，是需要功能更强大的手机操作系统。

2007 年 11 月，Google 发布 Android OS，剑指手机操作系统市场，并开源免费。 两年来，Android 获得了相当热烈的市场回应。有没有可能用 Android 取代 Nucleus，实现山寨手机的升级换代？

这个问题不容易回答，因为涉及到的方方面面比较多。

1. MTK 的下一代硬件[1]，既能支持 Android，也能支持 Windows Mobile。为什么 MTK 没有选择人气正旺，而且免费开源的 Android，反而选择联姻 WinMobile 呢[2]？

2. 2009 年 3 月，微软与 MTK 宣布结盟，共同开发针对中国 TD-SCDMA 手机市场的芯片[3]。时至今日，8 个月过去了，为什么没有实际成果？

3. MTK 有没有意愿采用 Android，替代 Nucleus 和 WinMobile？

4. MTK 下一代软硬件系统，能不能重现今日风光？

5. 其它公司有没有意愿利用 Android 的强势，为下一代手机制造提供一揽子解决方案，从而取代 MTK 的市场地位？

6. Google 免费提供 Android 的长远打算是什么？有没有雄心挺进硬件行业，甚至打造自有品牌的手机？

当然，“有没有意愿”这种问题，只有相关企业的高管才知道答案。我们这里只关注技术方面的可行性，以及利弊分析。

Hardware Engineer 是硬件工程师，Software Engineer 是软件工程师，那么桌上放着示波器和逻辑分析仪的 Software Engineer 是什么呢？是 Firmware Engineer 固件工程师，或者 Embedded Engineer 嵌入式工程师。最近有幸与一位有过数年市场经验的固件工程师讨论了以上问题，把讨论的内容整理成文，方便大家共同切磋。

Figure 1. 传说中的 Google 自有品牌手机
Courtesy http://farm3.static.flickr.com/2708/4148369461_db9417013f_o.jpg

Reference,

[1] 联发科 MT6516 智能手机芯片。(http://www.shanzhaiji.cn/news/20090220/7579.html)
[2] 联发科 MT6516 为何不支持 Android。(http://www.free-voip-china.com/tag/mt6516/)
[3] Microsoft and MediaTek to develop smartphone chipsets.
(http://www.cn-c114.net/583/a395734.html)

【1】MTK 亮相的历史背景

如果说1960年代是大型机(Mainframe)的时代，1970年代是小型机(Microcomputer)的时代，那么 1980 年代无疑是个人电脑 (PC)的时代，而 1990 年代则是互联网的时代。2000 年以后呢？或许是移动互联网的时代。

与电脑的发展历程类似，移动互联网的发展轨迹，看来也同样是以硬件的改进为先导，软件的繁荣紧随其后，带动整个行业的井喷式的爆发性增长。

Figure 2. 第一代手机，俗称大哥大。
Courtesy http://farm3.static.flickr.com/2711/4149584622_1338223724_o.jpg

1980 年代，手机开始商用。第一代手机俗称大哥大，特点是无线网络通讯信道中传输的是模拟信号。传输模拟信号有两个缺点，一是耗电，二是同一频段能够同时容纳的用户数量少。因为耗电，所以手机必须携带大块的电池，导致体积庞大，形如板砖。街头流氓打架时，常常捡起地上的板砖砸人，如果随身携带着大哥大， 情急之时也可以把大哥大当板砖用。

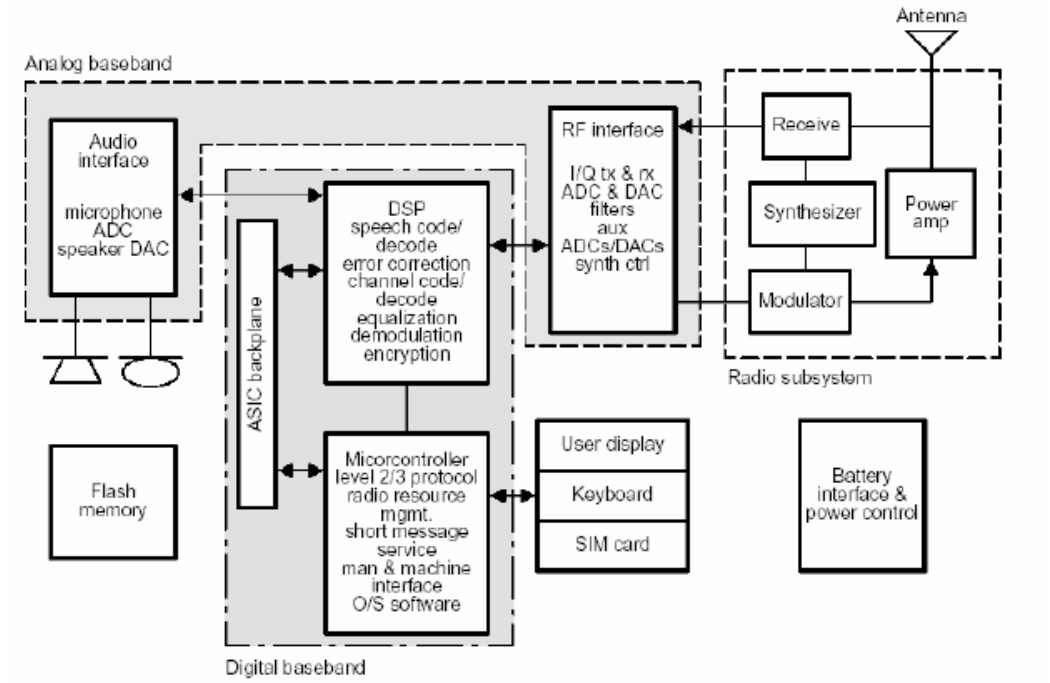


Figure 3. 以 DSP 为核心的第二代手机的硬件架构 [4]。
Courtesy http://farm3.static.flickr.com/2751/4146507443_9601fd7d08_o.png

为什么传输模拟信号，会有耗电以及频段容量低的缺点？对比一下数字信号就清楚了。如果把语音转换成数字，就可以采取数据压缩的办法，减少传输语音时占用的带宽。同时由于数字信号容易处理，所以在传输数字语音信号时，可以使用复杂的传输协议与控制，以便在同一频段，同时容纳更多用户相互通话。而对于模拟信号， 很难使用类似的协议与控制。

第二代手机的核心，是数字信号处理器，DSP(Digital Signal Processor)。第二代手机的硬件架构，如 Figure 3 所示，分为三部分。

1. 射频芯片组 (Radio Subsystem)。它负责调制-发送，以及接收-解调无线信号。无论是发送还是接收，射频芯片组只处理模拟信号。

2. 模拟基带芯片组 (Analog Baseband)。这个芯片组中，主要包括两个功能块，射频接口 (RF Interface)，以及音频接口 (Audio Interface)。

射频接口负责把从射频芯片组接收来的模拟信号，转换成数字信号，转发给数字信号处理器 (DSP)，以及把 DSP 输出的数字信号，转换成模拟信号，转发给射频芯片组以便发送。

音频接口负责把从麦克风接收来的模拟信号，转换成数字信号，然后转发给 DSP 做进一步处理。同时，它也负责把 DSP 输出的数字信号，转换成模拟信号，然后转发给喇叭以便播放。

3. 数字基带芯片组 (Digital Baseband)。这个芯片组主要由两部分构成，数字信号处理器 (DSP)，以及微控制器(Microcontroller)。

DSP 的主要任务是进行语音处理，例如去除噪音和语音矫正等等。此外 DSP 还负责，对语音数据流的压缩解压，不同格式之间的编码解码和转换，还有加密解密等等。 如果单块 DSP 芯片的功能不够，还可以借助于其它专用芯片(ASIC)。

微处理器负责两个任务，1. 处理无线通信协议，2. 运行手机操作系统。

当一位用户拨号呼叫另一位用户时，首先要建立一个通话通道，连接主叫方与被叫方。双方对话的语音数字信号，在这个通话通道里传输。七号信令系统负责建立这个通话通道[5]。为了保证信息安全，以及提高系统效率，采取了分离控制流与数据流的做法，也就是说，七号信令系统是一套独立的系统，游离于承载语音数字 信号的通话通道之外。

七号信令由一系列协议组成，与有线网络协议的 ISO 七层模型大致对应，参见 Figure 4。微处理器负责处理七号信令的第一层到第三层协议，MTP1，MTP2，MTP3。

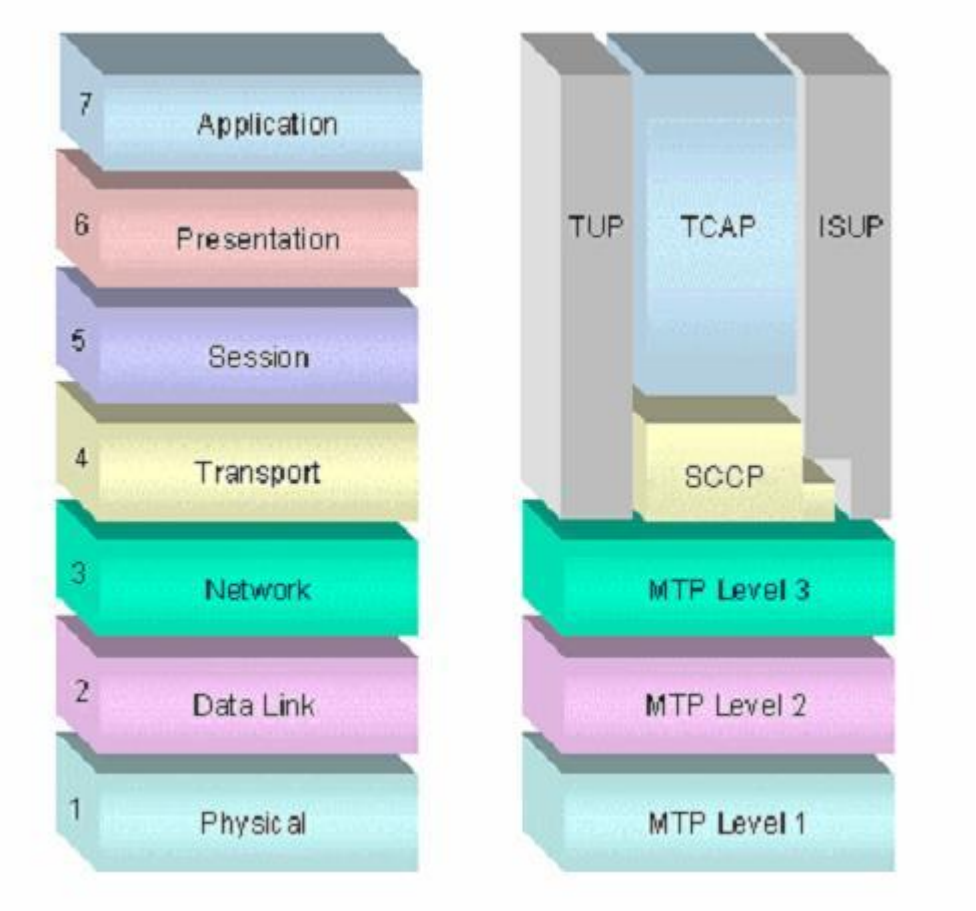


Figure 4. Comparison SS7 Protocol Suite and ISO Protocol Model [6]
Courtesy http://farm3.static.flickr.com/2742/4152165133_959a2cb7a3_o.jpg

手机操作系统，例如 Nucleus RTOS，负责处理如何开机/关机/锁机，屏幕显示，音量控制，响铃与震动等等外围动作。此外，还负责手机各个功能模块的运行调度 (Scheduling)，以

及不同进程间的数据交换(IPC)。虽然 DSP 在手机中的地位非常重要，但是 DSP 仍然接受手机操作系统的控制。

微控制器处理的数据，存放在 Flash 存储器中。

第二代手机的核心任务是实时通讯，表现为通话与短信两种功能。围绕实时通讯这个核心，操作系统具体协调各部分的工作。与用户的交互手段，依赖于十几个按键，以及一小块单色液晶显示屏。1998 年开始销售的 Nokia 5165，是第二代手机的一个经典，参见 Figure 5。

Figure 5. 第二代手机，Nokia 5165，1998 年
Courtesy
http://i1.phonearena.com/showimage.php?m=Phones.Images&f=image&id=7252&v=default

Reference,

[4] Trends in Hardware Architecture for Mobile Devices.
(http://www.inf.fu-berlin.de/inst/pubs/tr-b-04-17.abstract.html)
[5] Signaling System 7, SS7. (http://en.wikipedia.org/wiki/Signaling_System_7)
[6] Comparison SS7 Protocol Suite and ISO Protocol Model.
(http://www.kenneyjacob.com/2007/06/05/ss7-backbone-of-mobile-networks/)

【2】 手机 OS 成为核心

手机凭借通话和短信这两项基本功能，积累了用户，开拓了市场。但是用户的需求是永无止境的，对于手机制造商来说，紧跟用户需求，拓展手机功能，是机会也是挑战。

1988 年第一款数码相机，在日本上市。数码相机的关键是感光芯片。最初的数据相机，使用的是 CCD 芯片。1990 年代初，美国宇航局的科学家 Eric Fossum 发明了 CMOS 感光芯片，体积更小，感光效果更好。如果把 CMOS 感光芯片集成到手机上去，那么手机就可以兼具照相机和摄像机的功能。

但是事情没有那么简单，给手机配上镜头以及 CMOS 感光芯片只是起步，接下去还有其它问题需要解决。1. 微控制器的处理能力需要加强。2. 操作系统需要增添相应的驱动程序，同时改进任务调度的机制。3. 多媒体播放器，在液晶显示屏上（LCD）显示照片，播放视频，同时协调扬声器同步播放视频的声音。4. 不仅可以在手机本地存储并显示照片和视频，还要支持连网，支持用户上传和下载多媒体文件。

1997 年，硅谷工程师 Philippe Kahn 制成了世界第一台具有摄像功能的手机。与相机手机同时出生的，是他的女儿。Philippe 用手机给襁褓中的女儿拍了照片，并转发给 2000 多名亲友，这是人类历史上，第一次用手机拍摄，并通过移动网络散发的照片[7]。

从此，多媒体成为手机不可或缺的功能。此外，手机还添加了日历，记事本，计算器，音乐播放器等等功能。以及 Java VM，以便运行用 J2ME 编写的程序。还有 WAP，用于访问互联网。

第二代手机的使命结束了，取而代之的是第三代手机，也就是所谓功能手机（Feature Phone）。如果说，对于第二代手机而言，DSP 是核心，操作系统是配角。那么自从 Feature Phone 以来，操作系统的功能大大强化了，地位也上升了，由配角熬成了主角。

Feature Phone 的 OS 有多种选择。其中，Symbian 长期占据 Feature Phone OS 市场的半壁江山[8]，曾几何时，Symbian OS 叱诧风云，一言九鼎，俨然是手机操作系统领域的霸主。举个例子，从严格意义上来说，Symbian OS 是操作系统内核（Kernel）。同一套内核可以支持多种 GUI 图形界面，当年曾经出现过 S60，MOAP 和 UIQ 三种 GUIs，其中 UIQ 被索爱 （SonyEricsson）热捧。作为手机制造商，索爱是 Nokia 的竞争对手。坊间传说，Nokia 因为恨屋及乌，决定打压 UIQ。2008 年，Nokia 指使 Symbian Foundation 出面宣布，今后 Symbian OS 只支持 S60 一款 GUI。被冷落的 UIQ 别无选择，只好关门大吉[9]。

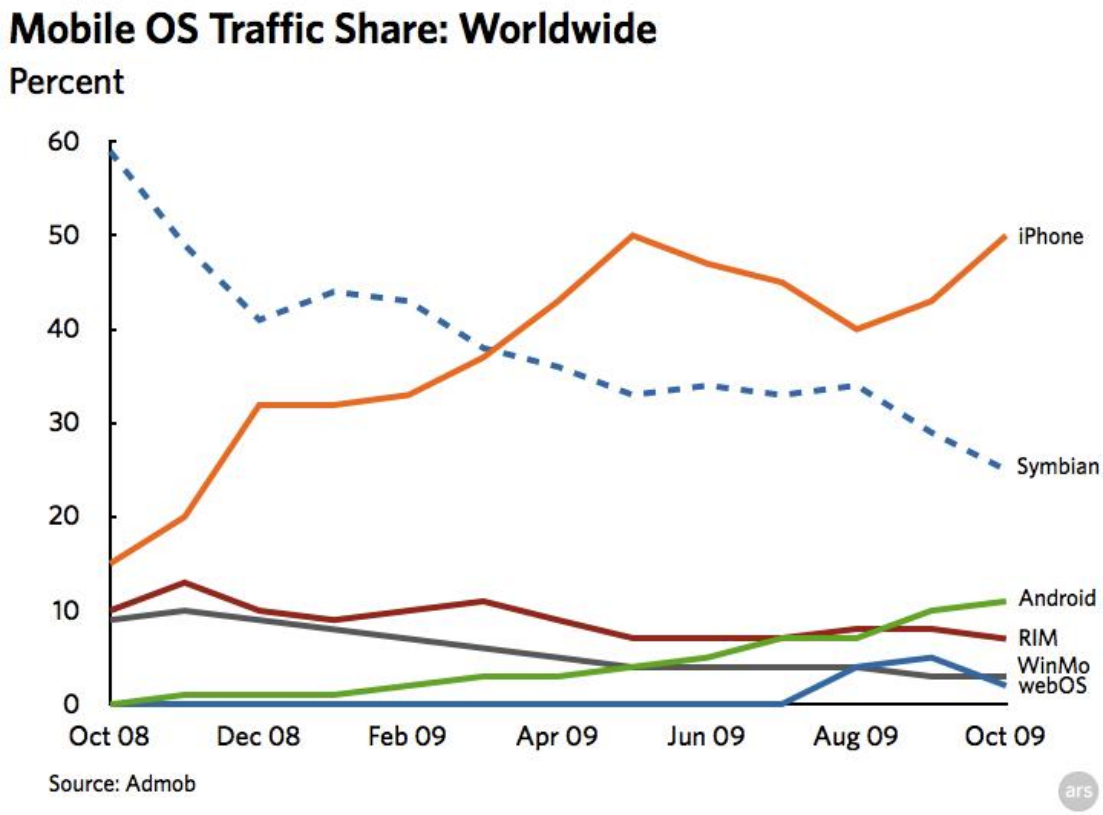


Figure 6. Mobile OS marketshare recent history [10]
Courtesy http://farm3.static.flickr.com/2568/4153933833_bdd657cde7_o.png

但是近年来，手机操作系统市场急剧动荡。带头造反的是 Apple 的 iPhone OS，第二冲击波来自 Google 的 Android，此外还有 Palm 的 WebOS 凑热闹，参见 Figure 6。有评论认为，

1. Symbian 老矣，很难逃脱日薄西山的命运。

2. iPhone 特立独行，走精品路线，成为时尚风向标。

3. Android 稳扎稳打，免费开源，走群众路线，将来最有可能成为手机 OS 的主流，取代 Symbian 的盟主地位。

4. WinMobile 偏安一隅，虽不大富，却也小康。

5. WebOS 喧嚣一时，如昙花一现。

6. RIM 的未来在于投靠强人门下。假如自立山头，则前途暗淡。不仅自毙，而且有可能殃及热销中的黑莓手机（BlackBerry）。

Nucleus OS 在哪里？这是一个被市场遗忘的角落。

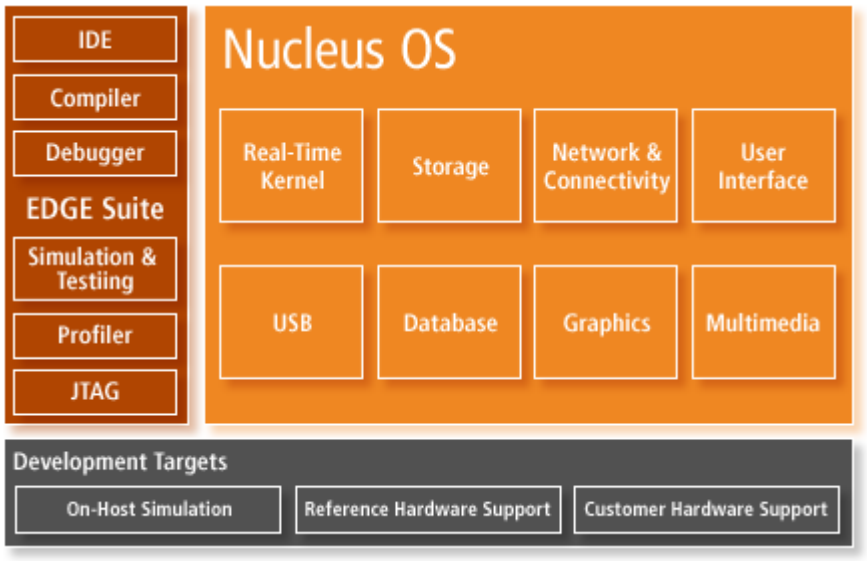


Figure 7. Nucleus OS Functional Modules [11]
Courtesy http://farm3.static.flickr.com/2560/4152533296_eceecd1965_o.gif

是什么原因，使 Nucleus 成为昨日黄花？Figure 7 描述了 Nucleus 内部各个功能块。Nucleus 本身有不可回避的技术限制，例如没有虚拟内存，而且不分 Kernel Space 和 User Space，系统和应用程序运行在同一个空间中。这对于 Feature Phone 来说，问题还不是很大，但是对于 SmartPhones 来说就非常致命了。因为如果应用程序不受限制，那么恶意程序就可以钻空子，获取整个操作系统的控制权，为非作歹。典型的案例就是死机短信，恶意操作致使整个操作系统崩溃。

但是在 2000 年，MTK 借力 Nucleus，从一家默默无名的 IC Design House，发展成为 2009 年一季度世界第 20 名芯片销售大户，参见 Figure 8。更重要的是，MTK 颠覆了传统的手机制造产业链。

MTK 最初靠什么发家？技术上有什么优势？商业模式上有什么优势？且听下回分解。

1Q09 Top 20 Semiconductor Sales Leaders ($M)

1Q09 Rank	2008 Rank	Company	Headquarters	2008 Tot Semi	08/07 % Change	1Q09 Tot Semi
1	1	Intel	U.S.	34,490	-2%	6,573
2	2	Samsung	South Korea	20,272	2%	3,686
3	5	Toshiba	Japan	10,422	-12%	2,008
4	3	TI	U.S.	11,618	-13%	1,982
5	6	ST	Europe	10,325	3%	1,660
6	8	Qualcomm**	U.S.	6,477	15%	1,316
7	9	Sony	Japan	6,420	-11%	1,270
8	7	Renesas	Japan	7,017	-12%	1,233
9	12	AMD	U.S.	5,808	-1%	1,177
10	4	TSMC*	Taiwan	10,556	8%	1,162
11	14	Micron	U.S.	5,688	3%	1,010
12	11	Infineon	Europe	5,903	2%	970
13	10	Hynix	South Korea	6,182	-33%	927
14	13	NEC	Japan	5,732	2%	863
15	18	Broadcom**	U.S.	4,509	20%	853
16	19	Panasonic	Japan	4,321	13%	850
17	17	Fujitsu	Japan	4,536	-1%	820
18	16	Freescale	U.S.	4,959	-11%	798
19	22	Sharp	Japan	3,411	-7%	790
20	25	MediaTek**	Taiwan	2,845	16%	704

*Foundry **Fabless

Source: IC Insights, company reports

Figure 8. Top 20 Semiconductor Sales Leaders, Q1, 2009 [12]
Courtesy http://farm3.static.flickr.com/2752/4154795958_eda5f2f9d0_o.jpg

Reference,

[7] Philippe Kahn created the first camera phone in 1997.
(http://en.wikipedia.org/wiki/Philippe_Kahn)
[8] Mobile OS market share. (http://en.wikipedia.org/wiki/Mobile_operating_system)
[9] UIQ history.
(http://en.wikipedia.org/wiki/UIQ, http://en.wikipedia.org/wiki/Symbian_Foundation)
[10] iPhone and Android in two-horse smartphone OS race.
(http://arstechnica.com/apple/news/2009/11/admob-iphone-and-android-in-two-horse-smartphone-os-race.ars)
[11] Nucleus OS modules.
(http://www.mentorg.co.jp/products/embedded_software/nucleus_rtos/mainColumnParagraphs/2/content_files/file/ill-nucleus.gif)
[12] Chaos reigns in top 20 semiconductor company ranking.
(http://www.evertiq.com/news/14176)

【3】手机是怎样生产出来的？

要说清楚 MTK 在商业模式上有什么优势，以及 Android 对于 MTK 未来的手机开发会有什么影响，首先得了解手机从设计，开发到生产的整个过程。

让我们先来看看手机的生产过程。在生产制造环节，山寨手机和正牌手机的区别其实不大。

1. 装配主板

大多数电子设备的制造过程，实际上就是按照设计图纸把各部分部件组合在一起，手机也不例外。手机的主要部件有：1. 硬件主板，目前大部分的手机是单板结构，2. 天线，3. 键盘，4. 显示屏，5. 外壳。其中主板是关键部件。各个手机制造商的技术能力不同，在手机制造产业链中的定位也不同。有实力的厂家会从 Gerber 文件开始，自己生产 PCB 板。 而不具备 PCB 生产能力的小厂，可以向其它厂家订购已经生产好的 PCB 板。Figure 9 是一款 MTK 出品的 PCB 板。

Figure 9. 一款 MTK 出品的 PCB 板 [13]
Courtesy http://farm3.static.flickr.com/2638/4165315089_04cccc5383_o.jpg

有了 PCB 板以后，就可以着手印刷和贴片。随着技术发展，老式的过孔型的 PCB 板已经几乎绝迹，现代 PCB 板大部分采用表面贴装技术。贴装工序分三步。

1. 把 PCB 板送入印刷机，印刷机把焊锡（Solder Paste)通过模板印刷在需要焊接的部位，参见 Figure 10。

2. 把印刷好焊锡的 PCB 板送入贴片机，贴片机把元器件贴装在 PCB 板上，Figure 11。小的元器件是装在大盘上，大一些的从塑料管中送进贴片机的，Figure 12。

3. 把贴好的板子送入回流焊机，经预热，加热后，元器件就焊装在 PCB 板上了。Figure 13 显示的是焊接好的主板。

Figure 10. 印刷机把焊锡通过模板印刷在 PCB 板需要焊接的部位 [13]
Courtesy http://farm3.static.flickr.com/2642/4166073144_858c9b9df6_o.jpg

Figure 11. 贴片机把元器件贴装在 PCB 板 [13]
Courtesy http://farm3.static.flickr.com/2738/4166074266_048dae75b2_o.jpg

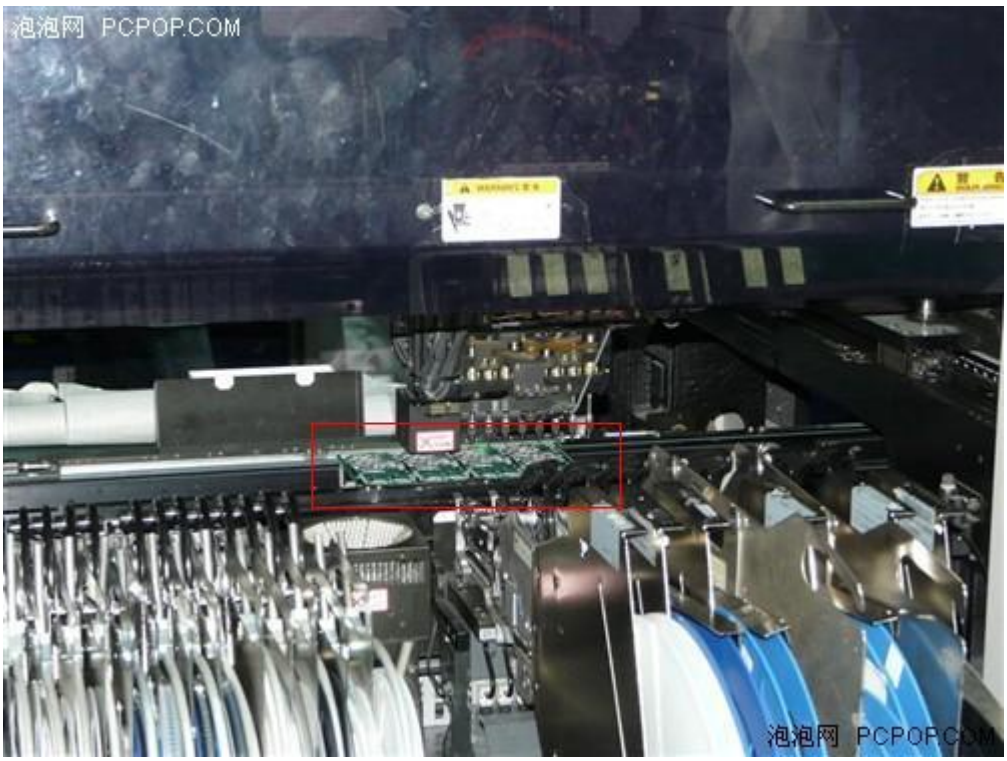


Figure 12. 贴片机近景，小的元器件装在大盘上，大一些的从塑料管中送入贴片机 [13]

Courtesy http://farm3.static.flickr.com/2661/4169062298_565433bd94_o.jpg

Figure 13. 焊接好的手机主板 [13]
Courtesy http://farm3.static.flickr.com/2660/4166077558_91bc66bf8e_o.jpg

制造过程强调质量控制，质量控制体现在多个环节。

1. 生产线上配备多种自动设备，检测各个工序是否工作正常。Figure 14 显示的是手机生产线上的一个产品质量显示器。

2. 焊接好的手机主板被送入测试台，测试台给手机主板加电测试，Figure 15。

3. 如果各项指标合格，就可以进入下一工序，安装系统软件。没通过的就需要手工检验和修复，Figure 16。举个例子，有的 IC 是正方形的，贴的时候有可能被转了 90 度。

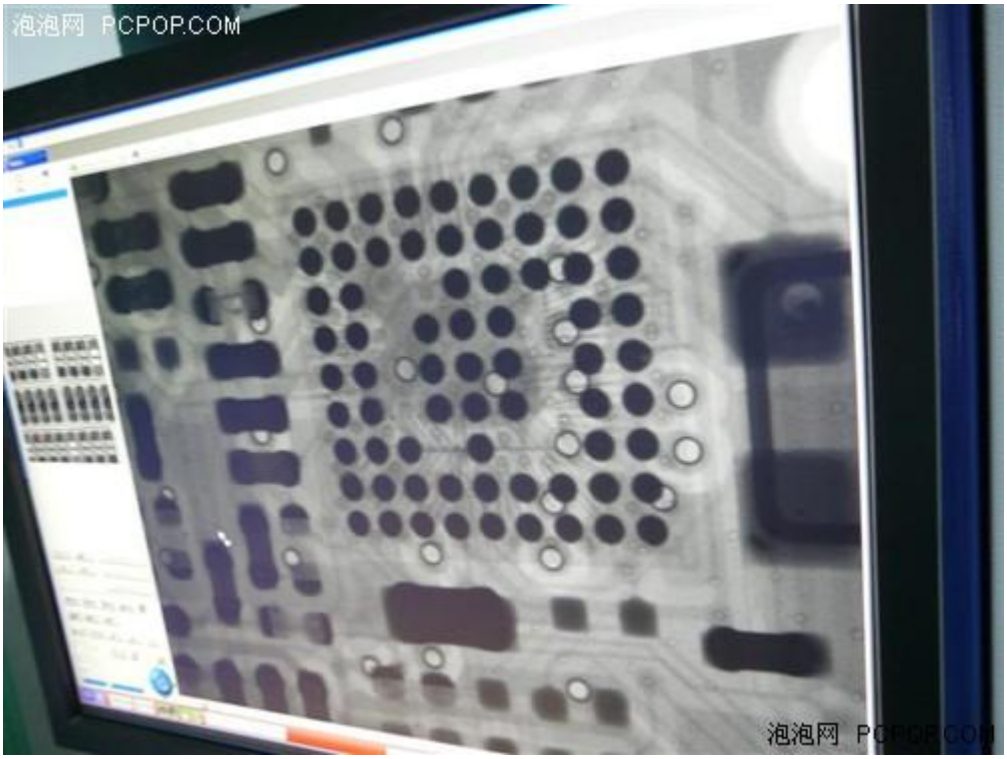


Figure 14. 手机生产线上的一个产品质量显示器 [13]
Courtesy http://farm3.static.flickr.com/2670/4165330751_b326843496_o.jpg

Figure 15. 测试台给手机主板加电测试 [13]

Courtesy http://farm3.static.flickr.com/2562/4165321507_de2b35349f_o.jpg

Figure 16. 手工检验和修复 [13]
Courtesy http://farm3.static.flickr.com/2572/4166083106_e63709dcb5_o.jpg

2. 烧录系统软件

硬件制造结束并检验合格后，下一步是烧录手机系统软件。手机系统软件是以 Flash Image 的形式，存放在工作站里面。把手机主板，通过串口或者 USB 口，与工作站相连。然后启动工作站里的安装程序，把系统软件烧到手机主板上的闪存 里，Figure 17。一台工作站可以同时烧录几十台手机裸板。

Figure 17. 手机系统软件安装工作台 [15]
Courtesy http://farm3.static.flickr.com/2543/4168191161_f66d9740ce_o.jpg

3. 装配外围设备

有一些部件，是无法使用回流焊机这样的自动设备，需要手工处理。Figure 18 显示的是在主板上手工焊接手机话筒。有些零部件不需要焊接，手工装配，或者拧螺丝即可。Figure 19，装配无须焊接和螺丝的手机部件。Figure 20，装外壳。Figure 21，手工贴手机编码串号。

Figure 18. 手工焊接手机话筒 [14]
Courtesy http://farm3.static.flickr.com/2640/4168962000_7b8b2cf9a0_o.jpg

Figure 19. 手工装配无须焊接和螺丝的手机部件 [14]
Courtesy http://farm3.static.flickr.com/2544/4168985040_f7f4ddb504_o.jpg

Figure 20. 手工装配手机外壳 [14]

Courtesy http://farm3.static.flickr.com/2517/4168217589_ac6c4594de_o.jpg

Figure 21. 手工贴手机编码串号 [14]
Courtesy http://farm3.static.flickr.com/2546/4168228041_ab02af61db_o.jpg

4. 校准和检测

手机组装结束以后，还需要检测辐射量，发射功率，待机时间等等，另外还有一些部件校准，例如天线。Figure 22 估计是在校准天线。Figure 23 在测试声音。大厂会用更专业的检测仪器，Figure 24.

Figure 22. 可能是在校准天线 [14]
Courtesy http://farm3.static.flickr.com/2606/4168243487_9b4b9841db_o.jpg

Figure 23. 测试声音 [14]
Courtesy http://farm3.static.flickr.com/2785/4169007364_43fdd90aee_o.jpg

Field Performance Evaluation

Laboratory Assessment

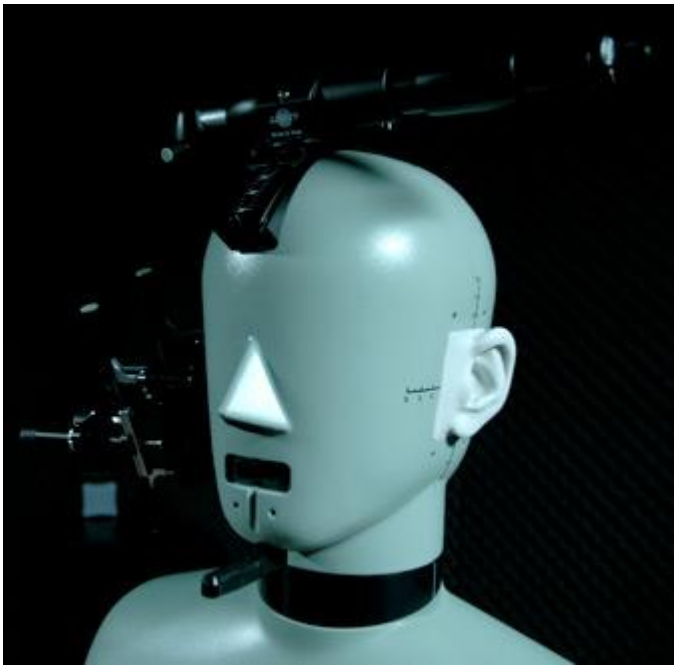


Figure 24 更专业的检测仪器 [16]
Courtesy http://farm3.static.flickr.com/2623/4170586975_4bbbe14b62_o.jpg, http://farm3.static.flickr.com/2577/4171352084_c49427bdbb_o.jpg, http://farm3.static.flickr.com/2560/4171357448_f740bf3a91_o.jpg

5. 打包出厂

前叙工序都完成以后，就可以打包出货了，Figure 25。

Figure 25. 打包准备出厂的山寨机 [14]
Courtesy http://farm3.static.flickr.com/2702/4168249409_348a63a654_o.jpg

由此，我们可以明白手机的生产过程和其它所有电子设备的生产几乎相同。能不能生产手机，一方面离不开必要的资金，去购置生产设备和培训员工。另一方面，需要得到软硬件的设计方案。而后者可能更重要。软硬件的设计包括以下内容。

1. 主板设计，或者 Gerber 文件，或者 PCB 板。

2. 系统软件。

3. 需要组装的全部元器件的清单（BOM List）。

4. 配套的外壳。

1,2 属于设计，3，4 属于采购

一旦得到了软硬件的设计方案，以及 BOM List，就可以从市场上采购，备料，然后就可以开始制造了。问题是，谁提供软硬件的设计方案以及 BOM List 呢？

Reference,

[13] 山寨手机制造大揭秘。
（http://news.xinhuanet.com/it/2009-02/02/content_10749450.htm）
[14] 山寨新闻调查。
（http://laiba.tianya.cn/laiba/CommMsgs?cmm=34721&
tid=26454409902158165 70&ref=commmsgs-paging&na=3&nst=501&
amp;pno=11&cpno=9& nid=34721-264544099021581657 0-26559613751684150 98）
[15] 友利通手机高层领导访谈记实。（http://www.unitone.com.cn/newsshow.asp?id=76）
[16] Metrico for mobile device performance assessment。
（http://www.metricowireless.com/services/index.php）

【4】 手机产业链与 Design House

前文说到，生产手机以前，制造厂家需要预先得到软硬件的产品级设计方案，然后按照设计方案亦步亦趋地做，就可以制造出手机了。软硬件的产品级设计包括以下内容，

1. 主板设计，或者 Gerber 文件，或者 PCB 板。
2. 产品级的系统软件。
3. 需要组装的全部元器件的清单（BOM List）。
4. 配套的外壳。

谁负责这些设计呢？答案：大厂有自己的设计部门，例如 Motorola，Nokia 等等。小厂可以外购设计，不仅芯片厂家能够提供设计服务，而且还可以求助专业的设计公司（Design House）。Design House 根据芯片厂家提供的手机参考方案，完成手机的产品级设计然后卖给手机生产厂家。

照理说，合乎常理的顺序是手机经销公司确定手机功能，然后联系制造厂商定货，制造厂商把设计任务交给 Design House，Design House 确定需要什么样的芯片后，向芯片厂商定货。即，经销商 -> 制造厂商 -> Design House -> 芯片厂商。

但是早期的手机制造产品链不是这个顺序，而是正好反过来。芯片厂商制造芯片，提供手机参考设计，然后向 Design House 兜售这些芯片和参考设计。Design House 把参考设计完善成产品级的设计方案后，推销给制造厂商。制造厂商生产出手机后，通过营销公司向市场推销。即，芯片厂商 -> Design House -> 制造厂商 -> 经销商。

为什么会造成这种首末倒置的现象？据传，有人问发明汽车的亨利福特，为什么不重视市场调查，福特的回答是这样的，“如果我问大家想要什么？他们会说，他们想要一匹跑得更快的马。（If I'd asked people what they wanted, they would have asked for a better horse.）[17]”。无独有偶，引领新潮的 Apple 公司的 CEO，Steve Jobs，在谈到 Apple 公司的创新理念时，他说，“Apple 公司的设计宗旨很简单，就是做一个 Apple 员工自己喜欢的产品”。在技术迅速发展的领域，研究引导制造，制造引导市场。

专业设计公司，Design House，不是一个全新的概念。中国手机的 Design House，从曾经昙花一现，到如今惨淡经营，大起大落只有不到短短 10 年的时间。

中电集团的 CECW (CEC Wireless)，从 99 年开始与荷兰 Philips 合作，到 2001 年卖下 Philips R&D 设立中电赛龙，成为中国第一家手机 Design House[18]。从那以后尤其是 2002 年，国内 Design House 一度雨后春笋般成立的，2003 年以后引起广泛注意。除中电赛龙外，国内比较有名的 Design House 有，经纬科技，龙旗，德信。

微软曾经大力扶持德信，动机或许是企图以此改变微软对台湾的 HTC 的过渡依赖，也可能是打算控制住 Design House，而 Design House 是手机制造产业链的龙头，控制住龙头就

影响了整个产业链。但是不幸的是，德信并没有如愿成长起来。倒是 HTC，踏踏实实，一步一个脚印，迅速做大。例如从 HTC TouchFlo 开始，HTC 向 Shell 方面发力。当时大家都觉得奇怪，WinMobile 的 Shell 已经很不错，作为微软的协作厂商，HTC 为什么要搞重复建设呢？当 HTC Hero 亮丽出场以后，一切都得到了解释。人无远虑，必有近忧，如果德信当年预见到软件的力量，像 HTC 一样，花大力气积累技术实力，或许时至今日，就不会把自己的陨落归结于产业链升级等等这些外因了。

2003 年度，国内 Design House 的利润率曾经高达 70%。但是好景不长，一年以后，2004 年平均利润率下降至 35%左右。各个 Design House 为了扭转败局，改变了以往的商业模式，转而采用对制造厂商更为优惠的方式。以往 Design House 的商业模式是，一手交钱一手交设计方案，收取开发费。现在的模式是，根据销量提成的模式，与制造厂商分摊手机销量不畅的风险。但是，形势进一步恶化，到了 2005 年，由于更多的公司掌握了手机设计技术，Design House 的平均利润率，进一步下降到 23%[19]。Figure 26 列举了 2006 年国内主要手机厂商及 IC 供应商。

中国主要手机厂商及其 IC 供应商

手机公司	公司名称	主要 IC 供应商
手机厂商	Lenovo	TI、MTK、Spreadtrum、Broadcom
	Bird	TI(Sagem)、MTK、Infineon
	Amoi	Agere、Spreadtrum
	TCL	TI(Alcatel)、MTK
	Konka	MTK
	Hisence	Spreadtrum
手机设计公司	Longcheer(龙旗)	MTK、ADI、TI（Smartphone）、Qualcomm
	SIM Tech（晨讯）	ADI、MTK、Ta tung-ADI(TD-SCDMA)
	Tianyu（天宇）	MTK
	Techfaith（德信）	NXP、Freescale、T3G(TD-SCDMA)
	CECW（中电）	NXP、Spreadtrum
	Wingtech(闻泰)	Spreadtrum
	其它	MTK、Spreadtrum 、ADI

Source：拓扑产业研究所，2006/12

Figure 26. 2006 年中国主要手机厂商及 IC 供应商 [20]
Courtesy http://farm3.static.flickr.com/2621/4183861726_79e05c560e_o.jpg

就在 Design House 冬天即将来临的时刻，2006 年，MTK 方案进入市场，并且迅速挤兑了其它 Design House 的市场份额，使得国内 Design House 的平均利润率，2006 年跌至 15%，2007 年是 5.1%，而 2008 年可能只剩 3%[19]。

令人疑惑也令人感兴趣的是，眼看着 Design House 的严冬即将来临，MTK 却似乎极具抗寒能力，而且在其它企业面临萎缩的形势下，MTK 却异军突起，2006 年一举占据了国内手机芯片市场的 40%，见 Figure 27。他们的独门秘笈是什么？

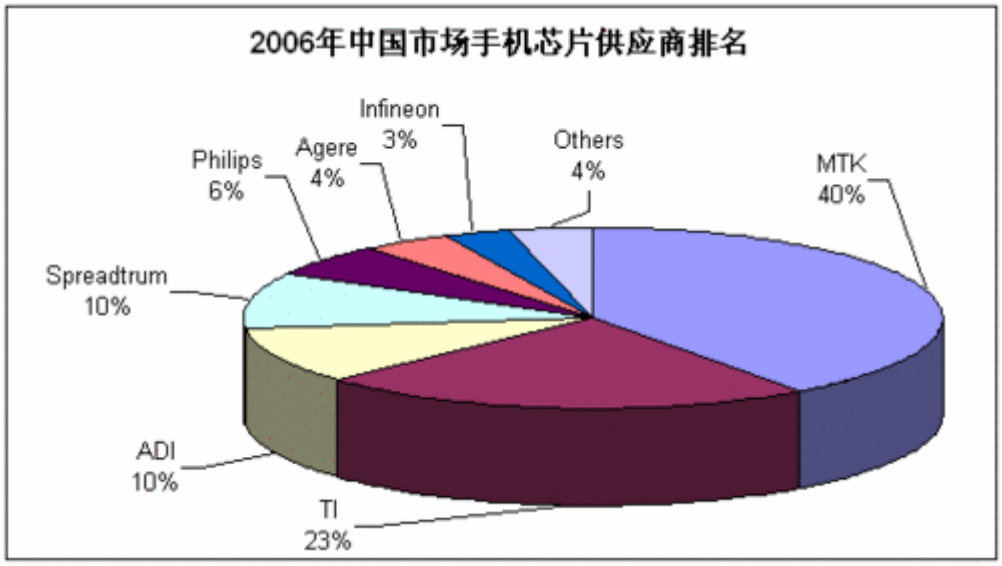


Figure 27. 2006 年 MTK 芯片方案占中国市场 40%份额[20]。
Courtesy http://farm5.static.flickr.com/4045/4183858092_dda7e761ef_o.gif

MTK 的董事长蔡明介，早年是台湾第二大半导体企业，台联电的打工仔。1995 年，台联电调整业务方向，要把蔡明介所在的 IC 设计部门剥离出去，分炉吃饭。蔡明介就这么被逼上梁山，开始了创业的历程。经过一番波折以后，联发科（MTK）于 1997 年成立。塞翁失马，焉知非福，不到两年的时间，MTK 就赚到了第一桶金。

联发科起家靠的是 CD-ROM 芯片。CD-ROM 的读盘速度以 150KB/秒为基数，当时大多数 CD-ROM 的数据是 4 倍和 8 倍，即 4x150KB/s 和 8x150KB/s。MTK 迅速推出 20 倍机型，顺利确定了市场地位。

从 1999 年底开始，蔡明介频频访问美国加州，他注意到 Intel 的增长率放缓了，只有 5%，而高通的增长率却高达 26%。他意识到，为手机设计 IC，前景看好。主意拿定以后，立刻采取行动，他从 Rockwell 挖来了手机基带芯片专家徐至强。徐上岗以后，2001 年，MTK 正式开始无线通信芯片的研发。 2003 年底，第一款 MTK 基带芯片研发成功。

产品研制出来以后，接下去就是营销。MTK 的营销方式称为“Turnkey”，即把手机的关键组成部分，芯片，操作系统，以及一些应用软件，这三者捆绑起来，给手机制造厂商提供“一站式解决方案”。有人戏说，有了 MTK 以后，只要三个人就可以成立手机公司，一个人接洽 MTK，第二个人找代工厂，第三个人做营销。这个说法比较夸张，但是的确也说明了，MTK 大大降低了手机制造的难度。

另外，山寨手机之所以繁荣，除了 MTK 以外，还离不开配套元器件生产厂商，例如比亚迪（BYD）。BYD 提供外壳，柔性线路板，液晶屏，摄像头，马达，键盘等等几乎手机所有配件。除了做手机配件以外，比亚迪现在还制造汽车。

MTK 的“一站式解决方案（Turnkey）”，很多人耳熟能详。客观上讲，把芯片，OS 和基本 Apps，三者捆绑起来，这个主意并不是具有突破性的技术创新。为什么其它公司没有做到，

偏偏让一个小公司，一个原本在手机芯片领域名不见经传的小公司，大红大紫呢？MTK 在技术上做了哪些贡献呢？具体分析，留给下一节。

Figure 28. MTK 董事长蔡明介 [21].
Courtesy http://farm3.static.flickr.com/2653/4184006050_f485c242fc_o.jpg

Reference,

[17] Henry Ford's Quote. (http://en.wikiquote.org/wiki/Talk:Henry_Ford)
[18] Philips transferred its mobile handset activities to China Electronics Co (CEC). (http://www.online-ma.com/cma/doc.asp?id=23)
[19] China Mobile Phone Design House Report 2007. (http://www.researchandmarkets.com/reports/554493)
[20] MTK 方案及代表手机大揭秘。(http://blog.163.com/xiaotu_sh2008/blog/static/68312596200811169584961 7/)
[21] 联发科董事长蔡明介。(http://www.esmchina.com/ART_8800096032_1100_0_0_4200_99d3a820.HTM)
[22] MTK 发家史 (http://telecom.weaseek.com/2008/0624/45326621_2.shtml)

【5】MTK 颠覆手机产业链

MTK 一站式解决方案（Turn-Key）模式出现以前，手机设计开发流程大约可以分成以下 6 步。

第 1 步，Design House 从芯片厂商那里拿到参考设计。

芯片厂商根据自己的市场部门对手机市场的预测，决定未来几年手机需要哪些功能，然后围绕自己的 CPU 内核，确定手机的参考设计，宗旨是推销自己的芯片。例如 2003 年，MTK 最早的 MT6205 基带芯片，内核为 ARM7，只有 GSM 等等基本功能。可能是因为当时 MTK 认为，GPRS，WAP，MP3 等等功能，市场上可能没有需求，所以决定 MT6205 基带芯片轻装从简，把这些累赘的功能统统裁剪掉。

等到参考设计的软硬件开发都接近完工了， 芯片厂商的营销人员就挨家挨户地拜访 Design Houses，展示新款的参考设计，游说新款方案具有广阔的市场前景。如果 Design House 同意合作，那么 Design House 会依据新款的参考设计，设计新款手机的整套方案。然后 Design House 把新款手机的整套方案，推销给手机制造厂商。制造商一旦决定投产，就会向芯片厂商批量订购芯片，芯片厂商因此获利。

第 2 步，确定配件元器件。

芯片厂商提供给 Design House 的是参考设计，而 Design House 提供给制造厂商的是产品级设计。前文说过，所谓产品级设计，包括以下部分，

1. 主板设计，或者 Gerber 文件，或者 PCB 板。
2. 系统软件。
3. 需要组装的全部元器件的清单（BOM List）。
4. 配套的外壳。

芯片厂商提供参考设计，宗旨是推销芯片，尤其是基带芯片。对于其它外围元器件，则留有余地，让 Design House 自己去选择。Design House 选择外围元器件的标准，除了质量以外，还需要考虑成本，以及供货商是否能按时供货等等因素。Design House 确定了这些元器件以后，就可以着手设计主板的布局和连线，决定配件元器件的清单（BOM List），系统软件，和外壳等等。

芯片厂商提供的参考设计，往往以开发板的形式出现。所谓开发板，也被称为大板，因为尺寸远比手机大得多，有的大板甚至可以媲美报纸的面积。Figure 29 显示的是 Samsung 的 S3C44BOX 芯片开发板[24]。这个开发板的参考设计，包括使用 HY57V641620 8M SDRAM，HY29LV160 2M Flash。假如 Design House 认为，8M 的内存小了，2M 的闪存也小了，需要换成更大空间的 RAM 和 Flash。LCD 也可以换成比亚迪（BYD）的产品，性能更好，价格却更便宜[25]。在这个开发板上，可以方便地改变连线，测试选用不同的配件元器件的性能和能耗等等。

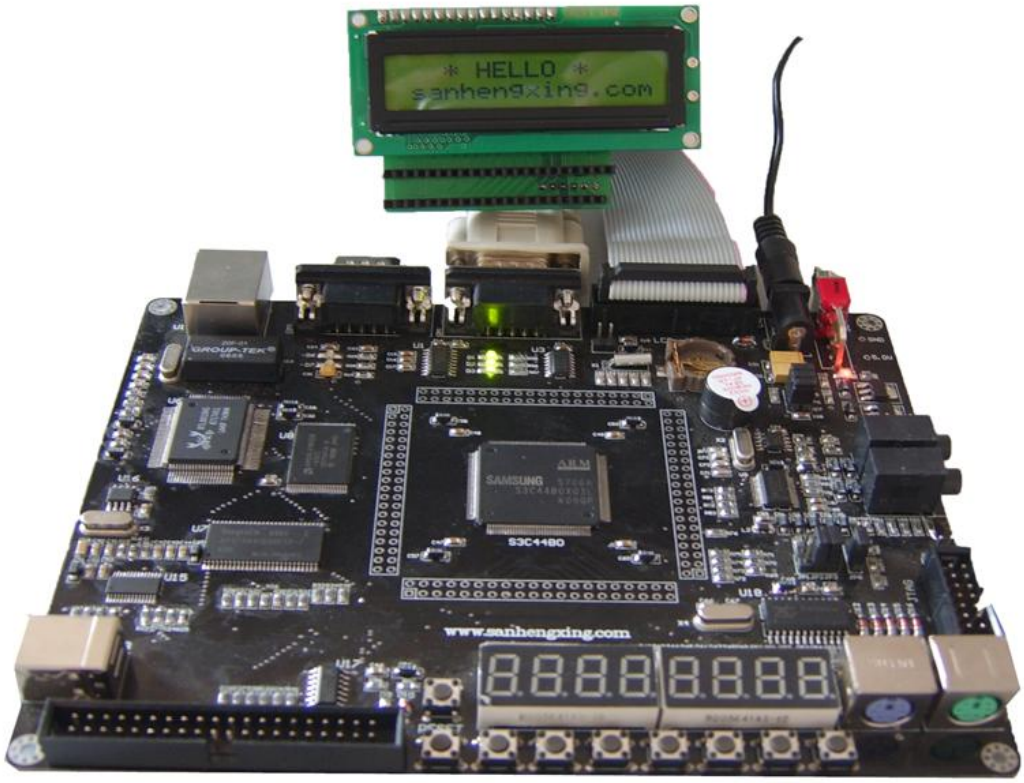


Figure 29. Samsung S3C44BOX 开发板，内核是 ARM7TDMI，一些 MTK 基带芯片也采用同级别的 ARM7EJ-S 内核[24]。
Courtesy http://farm3.static.flickr.com/2573/4194503829_e8cc18b36a_o.jpg

第 3 步，开发调试驱动程序。

在确定配件元器件的时候，要同时开发及调试相应的驱动程序。

第 4 步，产品级主板设计。

确定了微处理芯片以及配件元器件以后，Design House 着手把大板改成小板，也就是设计产品级主板。产品级主板设计主要是让主板更紧凑，这包括布局和连线，同时加上紧固件以及绝缘和散热材料，使手机更加坚固耐用。

Figure 30. iPhone 初版双主板 [26]
Courtesy http://farm3.static.flickr.com/2752/4197014647_c1e51e976e_o.jpg

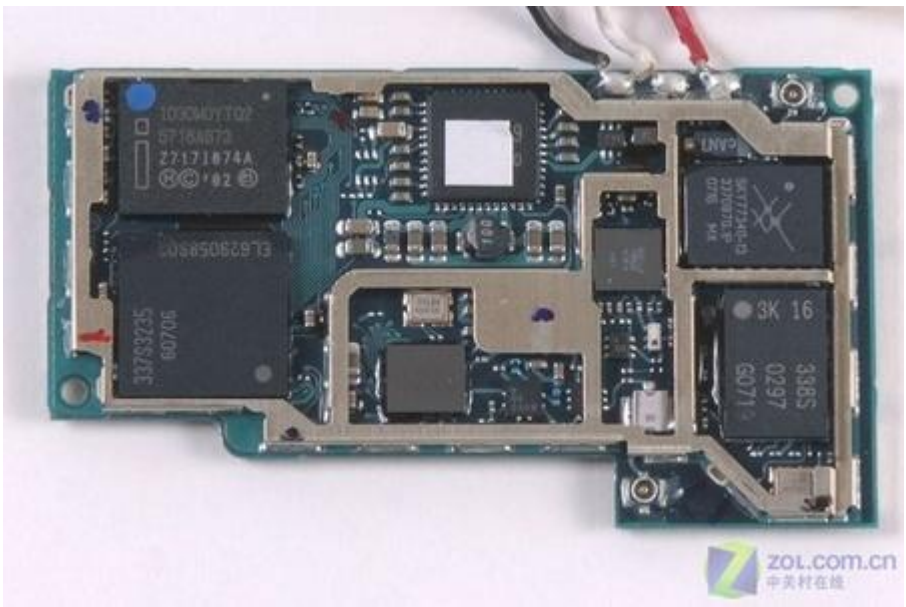


Figure 31. iPhone 初版无线主板 [26]
Courtesy http://farm3.static.flickr.com/2659/4197014655_e506f6e60f_o.jpg

Figure 30 显示的是 iPhone 初版的主板。iPhone 有两块主板，左边是 AP（Application Processor）主板，操作系统，用户界面以及应用程序都运行在 AP 主板上。图中黄色部分是覆盖在芯片上的绝缘膜，四周的铝合金边框使手机更坚固。右边是 BP（Baseband Processor）主板，负责通讯功能。Figure 31 显示的是 BP 主板的背面，从图中也可以看到很多用于紧固的铝合金边框。这两张图片[26]显示的是初版 iPhone 的主板，3G 版的 iPhone 主板，可以参考[27]。

严格说来，在这篇介绍 FeaturePhone 的章节里，用 iPhone 做例子，是不准确的。因为 iPhone 是 SmartPhone，而不是 FeaturePhone。但是无论是 FeaturePhone，还是 SmartPhone，从大板到小板的设计过程，却是相似的。

第 5 步，进一步调试软硬件，使之达到产品级。

所谓产品级的最高标准，是稳定，是不出 bugs。当然在现实生活中，完全杜绝 bugs 是不可能的。但是产品有优劣之分，bugs 数量的多寡，是衡量产品质量的一个重要指标。

第 6 步，Design House 设计一些参考外壳，参见 Figure 32，然后把从里到外的整套设计演示给制造厂商看。

Figure 32. Ginwave (经纬) Design House 的设计样品 [28]
Courtesy http://farm3.static.flickr.com/2503/4197117113_e64c36dfa8_b.jpg

总结一下前面所述，传统的手机设计开发分成 6 步，这六步均由 Design House 负责。

1. 从芯片厂商那里拿到参考设计。
2. 确定配件元器件。
3. 开发调试驱动程序。
4. 设计产品级主板。
5. 进一步调试软硬件，使之达到产品级。
6. 设计一些参考外壳，然后把从里到外的整套设计演示给制造厂商看。

MTK 一站式解决方案（Turn-Key）模式出现以前，手机 Design House 与制造厂商的合作模式，主要是 Open BOM 模式。在这个合作模式下，Design House 提供主板设计的图纸，以及需要采购的配件元器件清单（BOM List）。手机制造厂商拿到主板设计图纸以后，让芯片厂商按图纸制造主板。同时，手机制造厂商根据 BOM List，采购其它所需配件元器件。 主板和配件元器件到齐以后，手机制造厂商组织生产以及质量测试。然后把生产出来的手机整机交付营销商销售。

MTK 的一站式解决方案（Turn-Key），实质上是把芯片厂商与 Design House 两家的工作，由 MTK 一家包揽了。MTK 提供给手机制造厂商的不是设计图纸，而是提供已经组装了主要元器件的主板实物（PCBA），以及供参考的 BOM List。手机制造厂商，只需要根据 BOM List，选择采购与主板兼容的 LCD，麦克风，扬声器，以及外壳。然后把这些外设以及主板组装起来，贴牌打包，即可上市销售。

采用 Turn-Key 模式，手机制造厂商需要采购 LCD 等等外设，然后组装到主板上。如果手机制造厂商，连这两个步骤也嫌麻烦，MTK 甚至可以提供完整的裸机。这种模式，称为整机解决方案（Whole-Set）。采用 Whole-Set 模式，手机制造厂商只需采购并组装外壳，就可以贴牌打包上市销售了。

Figure 33. MTK 提供的主板，组装了外设以后的裸机，以及装上外壳后的手机 [29]。
Courtesy http://farm5.static.flickr.com/4002/4195300972_a1dd764eb8_o.jpg

Figure 34. 裸机主板的正面 [30].
Courtesy http://farm3.static.flickr.com/2625/4194503831_d5fbf67d28_o.png

总之，MTK 模式的出现，颠覆了以往的 Open BOM 模式，取而代之以 Turn-Key 模式，甚至 Whole-Set 模式。在 Turn-Key 模式下，MTK 只提供主板，参见 Figure 33 中，左边那张照片，以及与主板兼容的可供选择的 BOM List。在 Whole-Set 模式下，MTK 不仅提供主板，而且连外设也组装好了，手机制造厂商只需要组装外壳，参见 Figure 33 中，中间那张照片。中间那张已经组装好了外设的主板的反面，参见 Figure 34 [30]。图中可以清晰地看见 MTK 的芯片，MT6225A。

MTK 模式的出现，打破以往手机制造大厂，垄断手机市场的局面，催生了众多小资本小规模的手机制造厂商。对于消费者来说，MTK Feature Phone 的卖点是，价格低廉，外壳新潮，但是缺点是功能雷同。

MTK 模式出现以后，其它 Design House 并不是无事可做，他们仍然可以在 MTK 基础上，做一些增值软件开发等等工作，但是这些修修补补的工作，难以重现往日 Design House 日进斗金的辉煌了。

对比 Figure 34 中 MTK FeaturePhone 的主板，与 Figure 30 中 iPhone SmartPhone 的主板，一个明显的区别是，前者只有一块主板，而后者分为 AP 和 BP 两块主板。MTK 在 FeaturePhone 时代的成功，是否能够在 SmartPhone 时代继续发扬光大？要回答这个问题，首先要深入了解 FeaturePhone 与 SmartPhone 在硬件及软件方面的区别。

Reference，

[23] MTK 平台发展及各款芯片的功能。
(http://bbs.cniso.org/bbs/thread-64473-1-1.html)
[24] 增强型 Samsung S3C44BOX/ARM7TDMI 开发板。
(http://www.cediy.com/webHtml/Product/tooles/ARM /ARM7/16420090317111000.html)

[25] 比亚迪 LCD 产品介绍。(http://www.bydit.com/docc/products/lcd_p.asp)
[26] 拆解初版 iPhone。(http://hkmsyp.com/forum/thread-10198-1-1.html)
[27] 拆解 3G 版 iPhone。(http://www.beareyes.com.cn/2/lib/200807/14/20080714332.htm)
[28] 手机 Design House 与制造厂商的合作模式。
(http://www.ginwave.com/docc/product/product.asp)
[29] MTK 平台手机。
(http://wujianspace.spaces.live.com/?_c11_BlogPart_BlogPart=blogview&_c=BlogPart&partqs=cat%3D%25e8%25ae%25a1%25e7%25ae%2597%25e6%259c%25ba%25e4%25b8%258e%2520Internet)
[30] 山寨手机存活的理由。
(http://tech.sina.com.cn/mobile/n/2008-06-12 /10122253121.shtml)

【6】MTK 手机的基带芯片

MTK 的硬件技术的核心，在于它的基带芯片。为了降低成本，同时缩减手机主板的面积，基带芯片中除了 CPU 以外，还集成了很多外设控制器。FeaturePhone 的功能，基本上取决于基带芯片所支持的外设功能。

最早的 MT6205 方案，只有 GSM 的基本语音功能，不支持 GPRS 数据通信、没有 WAP、MP3 等功能。

随后 MT6218 在 MT6205 基础上，增加了 GPRS 数据通信、WAP 浏览、MP3 功能。

接着 MT6219 在 MT6218 基础上，又增加了内置 1.3M 照相/摄像功能，同时还增加了 MP4 功能。

MTK 再接再厉，在 MT6219 基础上进一步优化，开发了 MT622x 系列产品。例如，MT6226 是一款性价比相当高的产品，内置 VGA 照相/摄相处 理，支持 GPRS、WAP、MP3、MP4 等。同时，还开发了多款衍生品，例如，MT6226M 支持 1.3M 相机的。MT6227 支持 2M 相机。而 MT6228 不 仅增加了电视输出功能，同时还支持 3.0M 相机，等等。

从已经淡出市场的 MT6205，MT6217，MT6218，MT6219，到现在仍然在市场销售的 MT6223，MT6225，MT6226，MT6227，MT6228，MTK 生产的所有 Feature Phone 的基带芯片，均采用 ARM7 的内核。

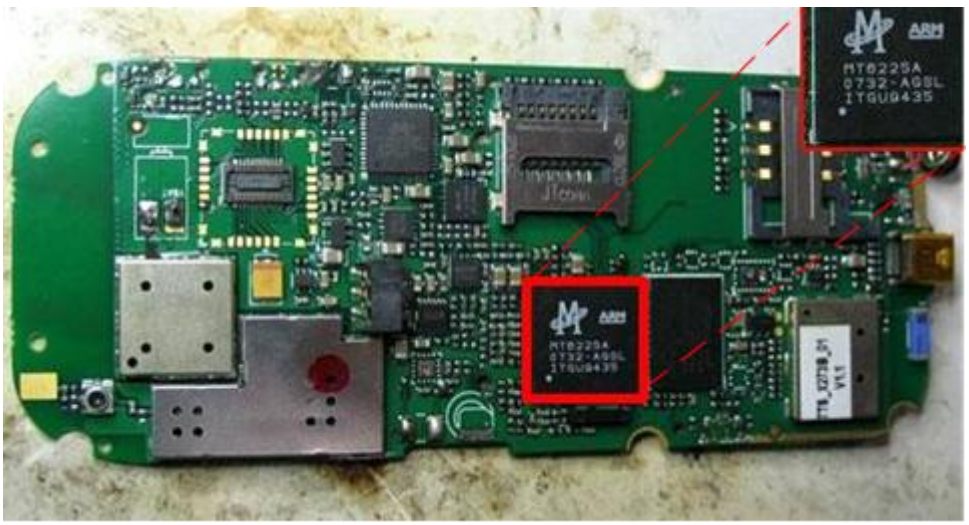


Figure 34. 以 MT6225 基带芯片为核心的 MTK 主板 [30]
Courtesy http://farm3.static.flickr.com/2625/4194503831_d5fbf67d28_o.png

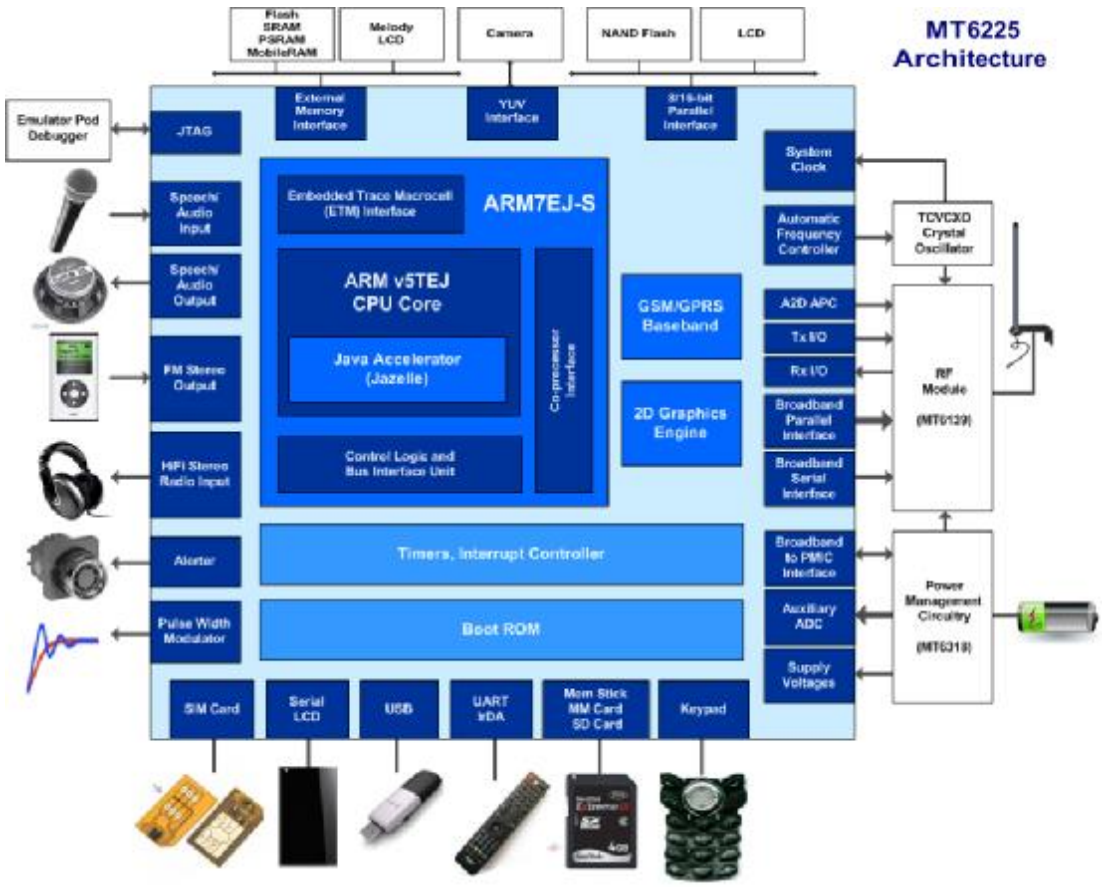


Figure 35. MT6225 Architecture [31,32,33,34]
Courtesy http://farm3.static.flickr.com/2735/4210933610_15de4f53c2_o.png

在 Figure 34 中，整个 MTK 手机主板的核心，是红线标出的 MT6225 基带芯片。虽然 MT6225 芯片的尺寸很小，但是它包含的功能却不少，参见 Figure 35。

以 MT6225 基带芯片为核心，加上电源管理芯片（PMIC）例如 MT6318，还有射频芯片例如 MT6139，另外再加上 Flash 存储芯片，就构成了 MTK 手机主板的基石。把这些芯片的引脚，连接上天线，LCD 显示屏，SIM 卡槽，扬声器麦克风等等外围设备，就实现了一个完整的 FeaturePhone 的基本功能。

MT6225 芯片的核心，是 ARM7EJ-S 微处理器（Micro Controller Unit，MCU）。ARM7EJ-S 微处理器的基本任务，是执行最基本的计算机指令（Instruction Set），例如 move，add，branch，shift，and，push/pop 等等[34]，学过汇编语言的同学应该不陌生。

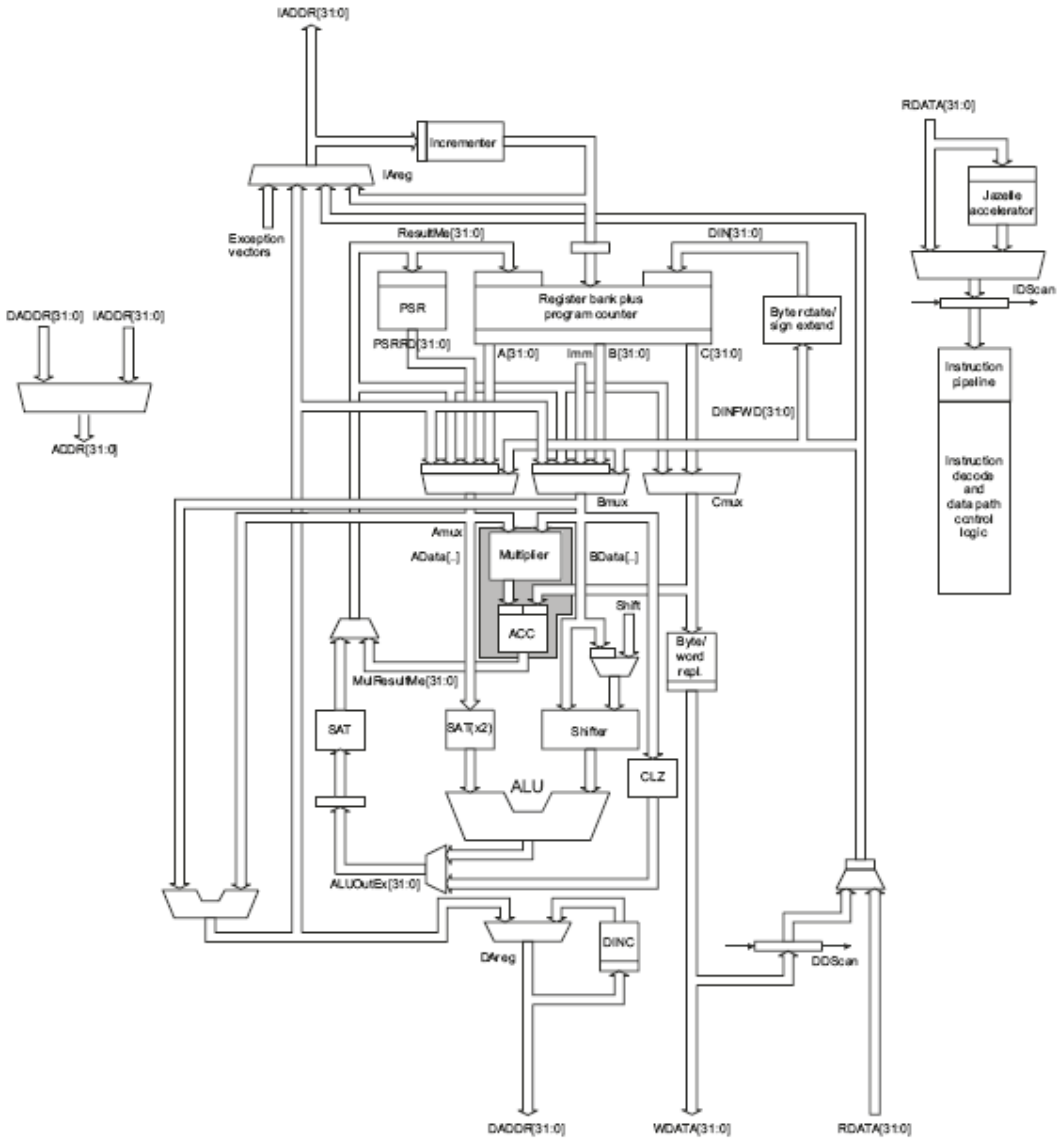


Figure 36. ARMv5TEJ CPU Core Block Diagram[34]
Courtesy http://farm3.static.flickr.com/2600/4216312750_de8d884003_o.png

在 ARM7EJ-S 微处理器内部，又可以细分为多个模块。其中，负责执行机器指令的模块，是 ARMv5TEJ CPU 内核。

指令执行的物理实现方式，决定了 CPU 内核的结构。CPU 内核结构的设计，包括如何设置 memory 和 register，如何读入数据以及移出数据，如何处理 address，interrupt，exception，等等。ARMv5TEJ CPU 内核的物理结构，如 Figure 36 所示。图中显示了 CPU 内部各个物理模块，以及各个模块之间相互勾连的组织方式。其中包括数据处理模块，如 load/move，算术运算模块，如 add/multiply，以及数位操作模块，如 shift/rotate，等等。

ARMv5TEJ 这个 CPU 内核型号中，v5 代表第 5 号版本的 ARM 指令集，以及相应的 CPU 内核物理结构。ARMv5TEJ CPU 内核被运用在多款微处理器中，包括 ARM7EJ-S 和

ARM926EJ-S。StrongARM 系列微处理器的 CPU 内核是 v4，ARM11 系列的 CPU 大多是 v6，而 ARM Cortex 的 CPU 则是 v7[36,37,38]。

虽然 ARM 有不同版本的指令集，但是这些指令的物理意义大同小异，不同之处在于指令数量的多寡，以及指令的语法规则的调整。不管是哪一个版本，ARM 的指令集都属于精简指令集 RISC 系列。RISC（Reduced Instruction Set Computer）的设计宗旨，是把逻辑复杂的指令，分解为一连串简单的基本指令，而 RISC 指令集只包含这些基本指令。RISC 的好处是，逻辑电路简单，体积小，同时可以通过提高频率的办法，提高 CPU 运行速度。但是代价是增加了 CPU 与 Memory 之间数据交换的负担。

所谓精简指令集中的“精简（Reduced）”，是相对于早年不精简的指令集而言。不精简的指令集，或者专业一点讲，复杂指令集 CISC（Complex Instruction Set Computer）并没有过时，并没有成为被淘汰的技术，例如 Intel 的 x86 CPU 系列，不仅当今仍然是电脑 CPU 的霸主，而且 Intel 正在积极努力，把 x86 CPU 芯片，推向手机芯片市场。

老牌 CISC 学派不同意 RISC 的思路，他们认为，单纯提高 CPU 的频率，并不能提高整个系统的运行效率，理由是 Memory 的 IO 速度比 CPU 慢，拖了整个系统的后腿。所以，为了提高系统的运行效率，应该设法降低 CPU 与 Memory 之间的数据交换。过份精简指令的数量，导致的后果是增加了 CPU 与 Memory 之间的数据交换，从系统整体性能上看，得不偿失[39]。

来自 CISC 阵营的批评很有道理。于是，ARM 的设计者们在两个方面改进了 ARM 微处理器的设计，1. 扩展指令集，2. 添加 memory 管理的模块。

1. 扩展指令集。

前文说到，ARMv5TEJ 是一款 CPU 内核的型号名称，其中 v5 代表第 5 版本的 CPU 内核，T 代表 Thumb 指令集，J 代表 Java bytecode 指令集。

ARM 原有的指令都是 32-bit，而 Thumb 指令只有 16-bit。Thumb 指令集基本上是原有 ARM 指令集的一个子集，通过压缩参数数量的办法， 降低指令长度。降低指令长度的目的，是变相降低 CPU 与 Memory 之间的 IO，从而提高运行效率。但是压缩参数数量，等同于弱化了微处理器的灵活性，降低了它的功能。为了解决这个问题，ARM 采取了同时支持原有 ARM 指令集以及 Thumb 指令集的办法。通过识别指令的类别，对这两个指令集，分别处理。

除了支持 Thumb 指令集以外，ARMv5TEJ 微处理器还同时支持 8-bit 的 Java bytecode。负责执行 Java bytecode 指令的，是 Jazelle 模块。

至于 ARMv5TEJ 中那个“E”，意思是该微处理器还支持专为数字信号处理（DSP）设计的特殊指令集。

2. 添加 memory 管理的模块。

前文还说到，ARMv5TEJ CPU 内核被运用在多款微处理器中，包括 ARM7EJ-S 和

ARM926EJ-S。这两款微处理器的型号中都带有“-S”后缀，代表可合成 （Synthesis），意味着购买此微处理器技术的客户，可以自行对微处理器结构做进一步修改，例如改变频率，扩展指令集等等。例如，前面 Figure 35 描述了 MT6225 芯片的内部结构，其中包括嵌入的 ARM7EJ-S 微处理器部分。

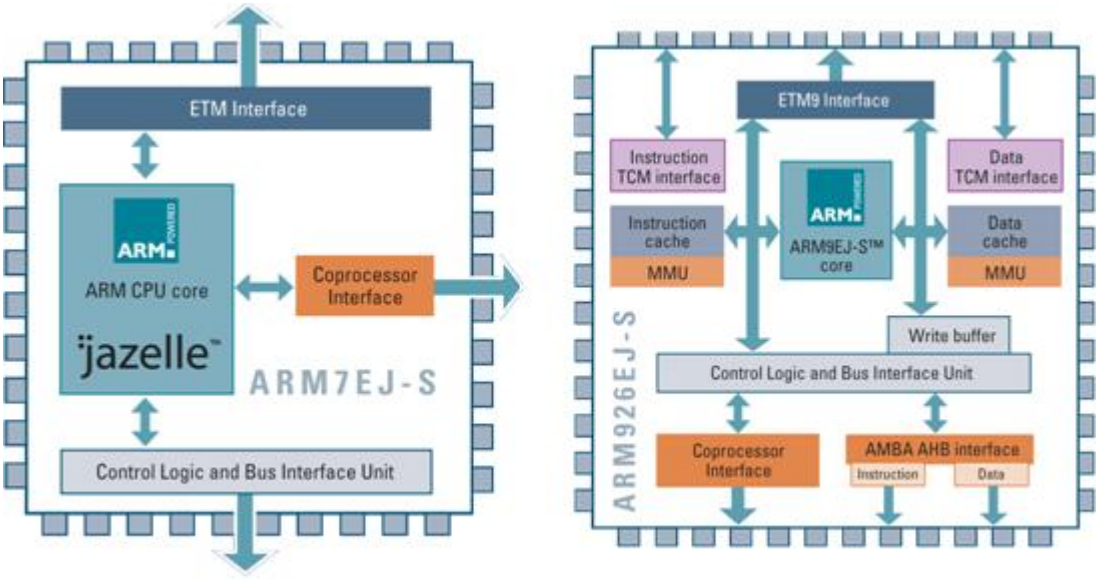


Figure 37. Comparison of ARM7EJ-S and ARM926EJ-S Architectures [36]. Courtesy http://farm3.static.flickr.com/2547/4215334659_3c87870224_o.png

Figure 37 对比了 ARM7EJ-S 与 ARM926EJ-S 两款微处理器的逻辑结构。ARM7EJ-S 微处理器的逻辑结构，如 Figure 37 中左侧所示。这款微处理器的结构很简单，以 ARMv5TEJ 为 CPU 内核，辅以数据总线接口，用来接收来自外部的控制指令，以及交换数据。另外，还设有与其它芯片协同工作的接口，以及 Embedded Trace Macrocell（ETM）接口，用来跟踪和调试 CPU 内部工作状态。

Figure 37 中右侧图，显示的是 ARM926EJ-S 微处理器的逻辑结构。对比 ARM7EJ-S 与 ARM926EJ-S，后者复杂很多。但是概括一 下，ARM926EJ-S 结构的调整，着力于两个方面，1. ARM7 遵循的是冯诺依曼结构，而 ARM9 转变成了 Harvard 结构，也就是把指令与数据分开处理[45]。2. 增添了核内缓存（Cache），以及与紧致内存（Tightly Coupled Memory，TCM）的接口[46,47]，此外，还增添了 MMU(Memory Management Unit)，强化对内存的管理。

由于 ARM7 系列微处理器内部没有 MMU，所以 ARM7 系列无法实现虚拟内存。没有虚拟内存的后果是，各个进程和内核之间可以互相访问对方使用的地址空间，这个漏洞的隐患很大，有可能让恶意程序钻空子，获取整个操作系统的控制权，然后为所欲为。典型的案例就是死机短信[49]，这条短信利用了短信处理程序中的 bug，造成黑屏和抖动，让手机系统失常。

从 ARM 的网站上可以查到，MTK 直接从 ARM 购买的生产许可证，仅限于 ARM7 系列，包括 ARM7TDMI，ARM7TDMI-S，ARM7EJ-S[40]。这个局面，一直延续到 2007 年 9 月 10 日才发生改变，当时 MTK 收购了 ADI 旗下 SoftFone 手机芯片系列。MTK 此举的目的，

主要是着眼于 ADI 在 3G 上的专利，但是 MTK 同时间接获得了 ARM9 和 ARM9E 系列的生产许可证，可谓一箭双雕。

从此 MTK 基带芯片产品，有两个系列，嫡系的 MT 系列与兼并来的 SoftFone 系列[42]。在 MT 系列中，编号小于 MT6235 的各款芯片，内核均为 ARM7 系列。而 SoftFone 系列各款芯片中，有的以 ARM7 系列为内核，也有的以 ARM9 系列为内核，ARM9 系列中使用最多的，是 ARM926EJ-S 这一款微处理器[43]。

回顾历史，MTK 通过不断地优化升级自己的芯片，从而确定并扩大自己的市场地位。延续这一做法，是否能够保持 MTK 的发展势头呢？不一定。 MTK 的传统领地在于 FeaturePhone，但是 FeaturePhone 正在被 SmartPhone 淘汰。MTK 如何跟上 SmartPhone 浪潮呢？且听下回分解。

Reference，

[30] 山寨手机存活的理由。(http://tech.sina.com.cn/mobile/n/2008-06-12 /10122253121.shtml)
[31] MT6225 芯片简介。(http://www.study-kit.com/list.asp?ProdId=0203)
[32] MTK6225 内部结构简述。 (http://weboch.cn.alibaba.com/athena/offerdetail/sale /weboch-50910-483309568.html)
[33] AM7EJ-S Introduction. (http://www.arm.com/products/CPUs/ARM7EJSCore.html)
[34] ARM7EJ-S Technical Reference Manual. (http://infocenter.arm.com/help/topic/com.arm.doc.ddi0214b/index.html)
[35] ARM926EJ-S Technical Reference Manual. (http://infocenter.arm.com/help/topic/com.arm.doc.ddi0222b/index.html)
[36] ARM Processor Survey. (http://en.wikipedia.org/wiki/ARM_architecture)
[37] ARM Processor Selector. (http://www.arm.com/products/CPUs/core_selector.html)
[38] ARM Core Overview. (http://digital.knu.ac.kr/lecture/%EC%82%BC%EC%84%B1%ED%85%8C%ED%81%AC %EB%85%B8MBA/2_arm_core.pdf)
[39] RISC vs CISC. (http://www.pic24micro.com/cisc_vs_risc.html)
[40] ARM Processor Licensees. (http://www.arm.com/products/licensing/licencees.html)
[41] MTK 收购 ADI 手机芯片产品线。 (http://www.esmchina.com /ART_8800078804_1400_2101_3101_4300_b1c7f2ad.HTM)
[42] MTK Product Lines. (http://www.mediatek.com/en/product/list.php?cata1=1)
[43] MTK SoftFone Product Line. (http://www.mediatek.com/en/product/list.php?cata3=2)
[44] MTK 常用术语缩写。 (http://www.mtkmtk.com/html/download/mtkmmi/2009/0717 /4109.html)
[45] Difference of ARM9 from ARM7. (http://en.wikipedia.org/wiki/ARM9)
[46] 对 ARM 紧致内存的理解。(http://hi.bccn.net/space-21499-do-blog-id-15164.html)
[47] ARM Technical Reference, Tightly Coupled Memory (TCM). (http://infocenter.arm.com/help/topic/com.arm.doc.ddi0338g/Chdhbjjb.html)
[48] Introduction to MMU. (http://en.wikipedia.org/wiki/Memory_management_unit)

[49] 让你手机死机黑屏的短信。(http://www.177hy.com/bbs/viewthread.php?tid=69038)

【7】 MTK 手机软件系统

MTK feature phone 的基本功能是通话和短信，要了解 MTK 手机软件系统，首先需要简要回顾几个移动网络通讯的基本概念。

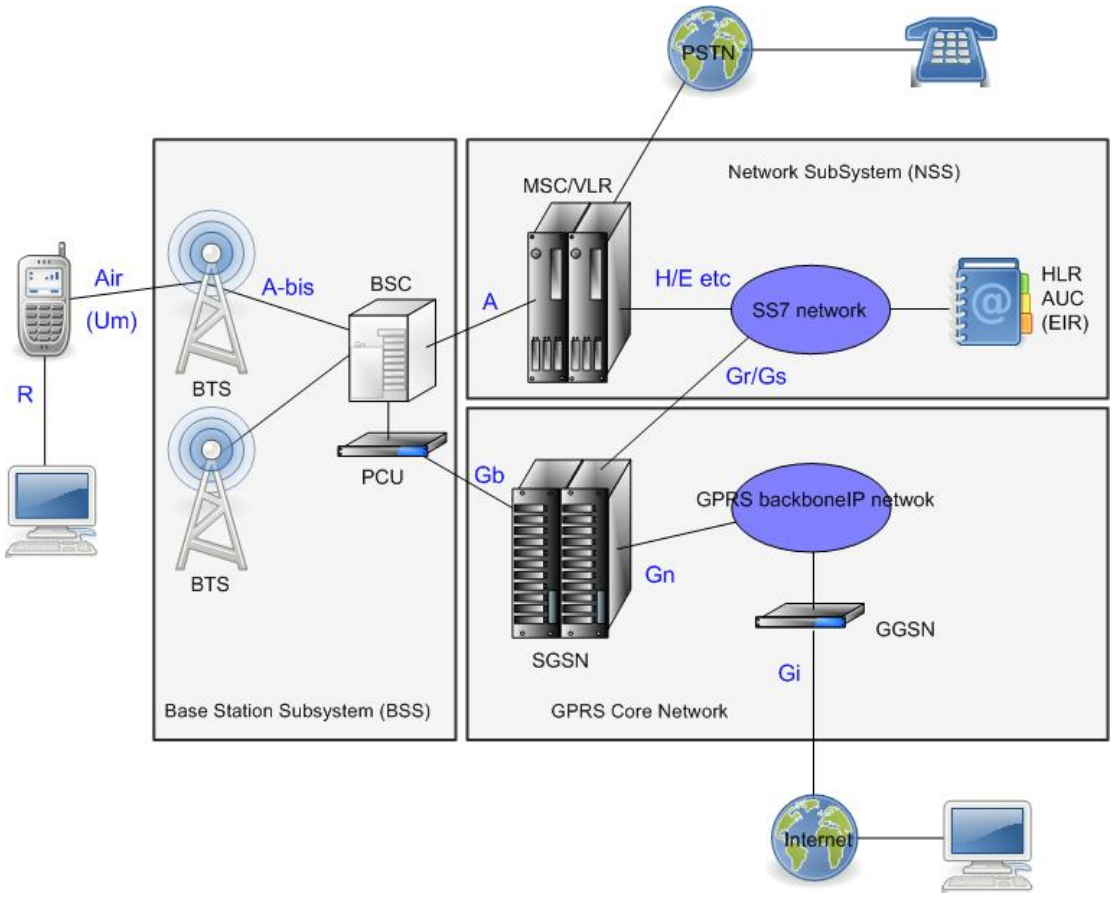


Figure 38. GSM-GPRS Architecture
Courtesy http://farm3.static.flickr.com/2694/4239683146_55f0dd7e11_o.png

以 GSM 系统为例，手机以无线方式建立起与基站（BTS）的联系，两者之间通讯接口是 Um。基站与基站控制器（BSC）之间的通讯接口是 Abis，基站控制器与移动交换中心（MSC）之间的通讯接口是 A，参见 Figure 38。

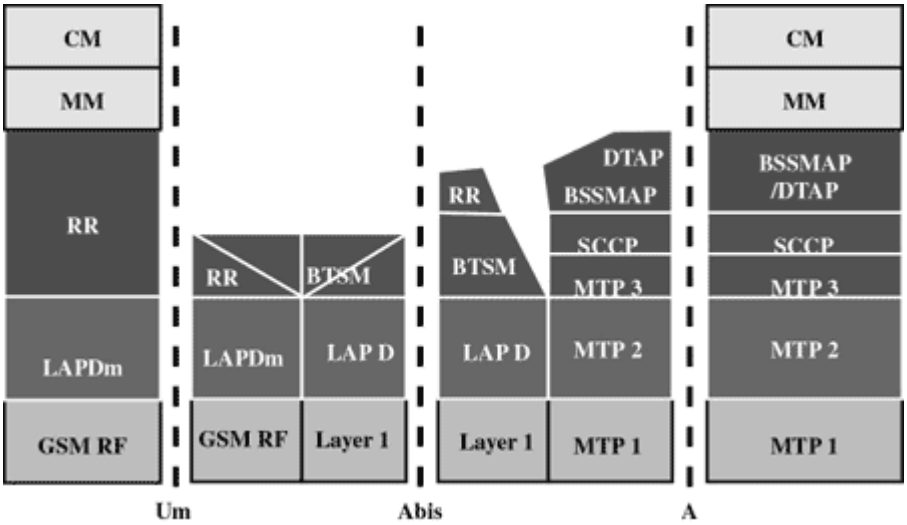


Figure 39. GSM Protocol Layer [1]
Courtesy http://farm3.static.flickr.com/2743/4284005175_06873d175f_o.gif

所谓接口（Interface），是一组协议的代名词，而这些协议可以分成若干层，层层叠叠，所以接口又被称为协议栈（Protocol Stack）。Figure 39 中最左边一列，显示的是手机需要处理的协议栈。从第二列到第四列，分别显示的是基站（BTS），基站控制器（BSC），和移动交换中心（MSC）分别需要处理的协议栈。相邻两列之间的虚线表示通讯接口，接口两侧的协议栈对称，以保证通讯中传递的信息能够被对方识别。

MTK 手机软件系统，需要处理的是最左边的协议栈 [2]。

1. 该协议栈的底层是物理层（Physical Layer），负责无线射频（GSM RF）和信道管理（Channel Access Method），用来传输原始的比特数据流，例如 GSM 系统中的 TDMA。

2. 第二层是数据链路层（Data Link Layer），LAPDm 是该层使用的协议，负责把数据流分成若干帧，并处理流控制。

3. 第三层是网络层（Network Layer），负责建立手机通讯发起方与接收方之间的连接。手机的连接离不开基站，基站控制器以及移动交换中心。而且当手机的位置不固定时，譬如在运动中的汽车上打电话，经过的基站，甚至基站控制器都不固定。所以，网络层又细分为三个子层，分别是 RR 层，MM 层，以及 CM 层。

3.1. RR 层负责无线资源管理（Radio Resource Management），负责建立手机与基站之间的联系，尤其是当多个手机同时与同一个基站联系时，如何避免多个信道之间的相互干扰。

3.2. MM 层负责移动的管理（Mobile Management）。运动中的手机由一个基站切换到另一个基站，甚至由一个基站控制中心切换到另一个基站控制中心，切换过程中如何保持通话的连续性，诸如此类的工作由 MM 层负责。

3.3. CM 层，又被称为 CC 层，负责连接和呼叫的管理（Connection Management, or Call

Control）。在手机通话发起方拨号是，CM 层负责查询接收方当前所在位置，以及是否在通话中，是否需要转入语音留言箱等等。

简要回顾一下 GSM 的协议栈，有助于理解 MTK 的软件系统。GSM 协议层只规定了 L1 到 L3 三层协议，即物理层，数据链路层和网络层，并没有规定 L4 以上的协议内容。MTK 把 L4 视作应用层，L4 的协议用来让应用程序调用网络层 L3 中的 CM/CC 子层功能模块。

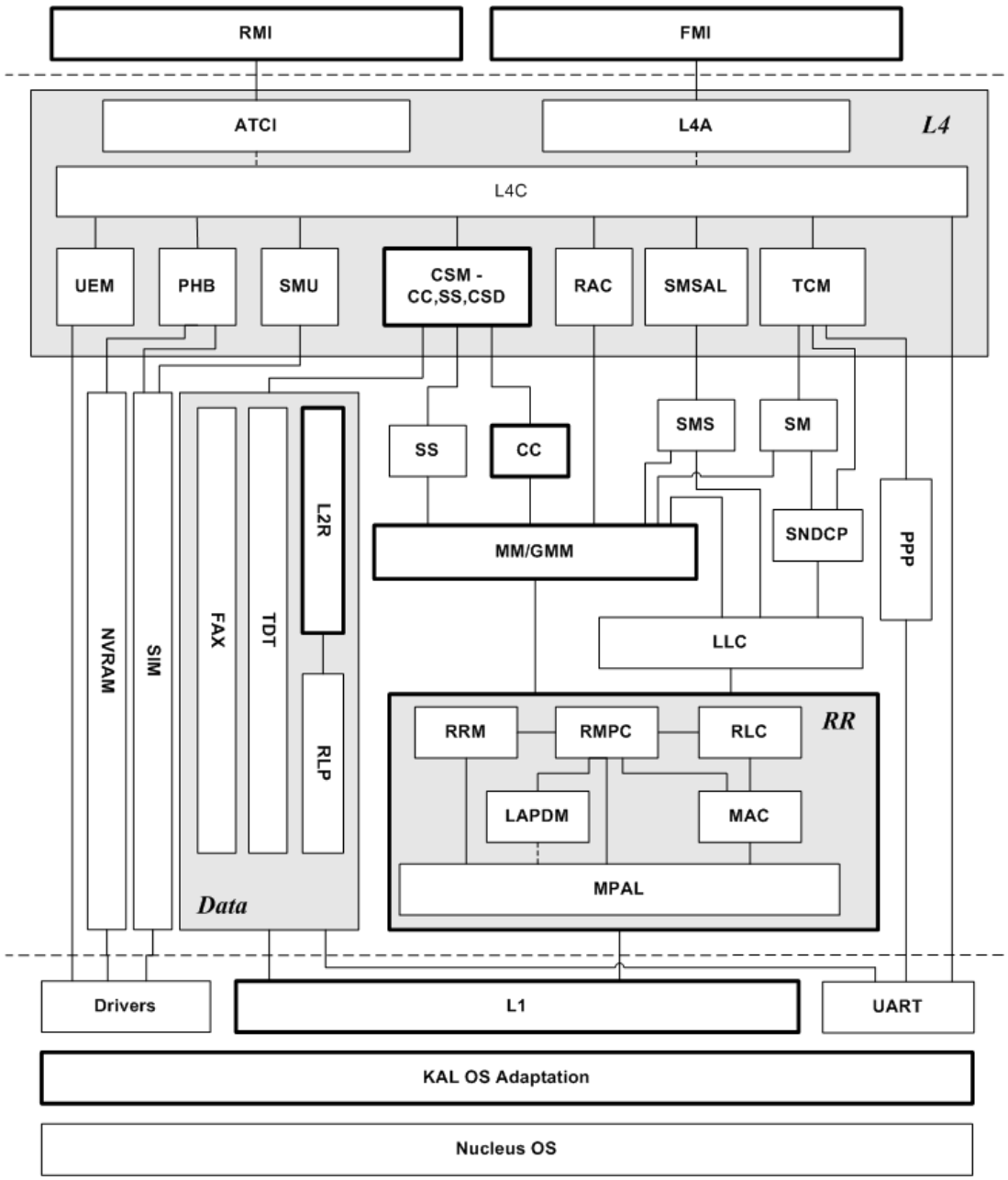


Figure 40. MTK software function modules [3].
Courtesy http://farm5.static.flickr.com/4062/4294578472_bfcf09c6f5_o.png

Figure 40 显示了 MTK 软件平台中包含的基本模块，来自 MTK 工程师的演讲稿[3]。其中各

个模块的名称缩写的含义，可参阅附录（Appendix）。虽然该资料来源可靠，但是 Figure 40 图中存在一些令人疑惑的细节，

1. 物理层（L1），负责无线射频和信道管理。Figure 40 中 L1 模块，如粗边框图所示。它的左边是驱动器（Drivers）模块，右边是 UART 串口。这种绘制方式不太准确，其实 L1 和 UART 都可以看成是硬件加驱动器的一种。

MCU（微处理单元）支持多种外设，例如扬声器/USB/远红外串口等等，参阅前文 Figure 35。每一个外设，不仅需要硬件，也需要驱动软件。MTK 软件平台中包含的驱动软件非常丰富，足以支持所有 MCU 外设。

2. 数据链路层（L2）的模块，包含在 Data 部分，例如 L2R。

按照图中所示，应用层（L4）可以通过 CSM 模块，直接调用 L2 模块。这与先前介绍的 GSM 协议栈是冲突的，按照协议栈的规定，L4 只能与 L3 中 CM/CC 子层联系。但是 MTK 的做法，允许 L4 越级与 L2 直接联系。也就是说，[3]隐含的意思是，GSM 协议栈只是一个建议，在具体实现中不需要严格遵守。

3. 网络层 L3 包含的功能模块很多，可以归纳为 RR, MM/GMM，以及 CC 三个部分，如图中粗边的框图所示。

按照前文所述，GSM 协议栈建议，L3 层中 RR 子层应该只与 L2 模块联系，而不应该直接调用 L1 模块。按图中所示，MTK 没有严格遵守这个规定。更有意思的是，图中把 L2 与 L3 描绘成并列的关系，而且它们之间没有直接联系，这一点也比较费解。

4. 应用层 L4 中的 CSM 模块，既负责与 L3 层的 CM/CC 模块联系，也负责与 L2 层的 L2R 模块联系，这一点似乎不合常规。

L4 是连接应用程序与 GSM 协议栈模块的接口。在 FeaturePhone 的语汇中，应用程序常常被当成是 MMI（Man-Machine-Interface）的同义词，其实细究一下，更准确的说法是，应用程序是 MMI 的一部分[4]。根据[3]的文字叙述，尤其是 pp19 关于 L4A 和 L4C 的介绍，以及 pp38 关于 Keypad 事件触发机制的介绍，似乎 MTK 的应用程序，对于其它功能模块的调用，有四种机制，如 Figure 41 所示。

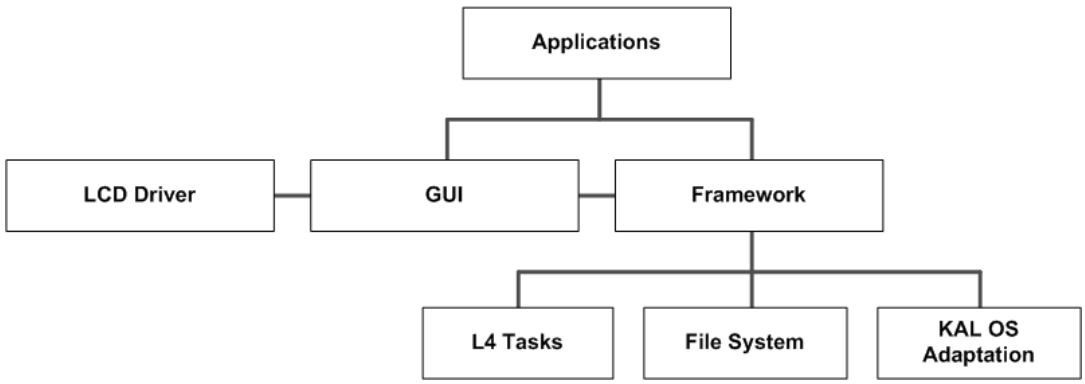


Figure 41. MMI Architecture
Courtesy http://farm5.static.flickr.com/4049/4293838733_7f23594f7d_o.png

4.1. 通过 GUI 模块控制 LCD 显示屏。

4.2. 通过 L4 模块，以任务的方式，实现通信及其它附加功能，例如 SIM 卡控制，语音通信，数据通讯，通话历史记录，电话本，照相机等等功能。

4.3. 通过 Framework 中的 API，直接对文件系统进行操作，而无需通过 OS。

4.4. OS 的功能限于多任务的调度，以及内存的管理。

这四种调用机制中，尤其是第三和第四这两种，与 PC 以及 smartphone 的差别非常大。这阻碍了 MTK 软件平台未来顺畅地发展，这个问题留给后续文章，做进一步讨论。

Figure 40 中没有详述 MTK 应用模块调用底层模块的四种机制，而只是简练笼统地描述成 FMI（Feature Rich MMI）。不妨把 Figure 41，视为 Figure 40 中，FMI 模块的局部放大。

虽然 Figure 40 存在一些令人疑惑的细节，但是基于它对于 MTK 各个功能模块的描述，同时参考同一份资料的另一张图[3]，我们不难勾勒出 MTK 软件系统的结构，参见 Figure 42。这张图略去了 Figure 40 中一些细节，例如 RMI（Remote MMI）。RMI 不仅可以支持 PC 操控手机，而且也为 SmartPhone 中，AP（Application Processor）与 BP（Baseband Processor）的分离打下了基础。这些内容留给后续章节。

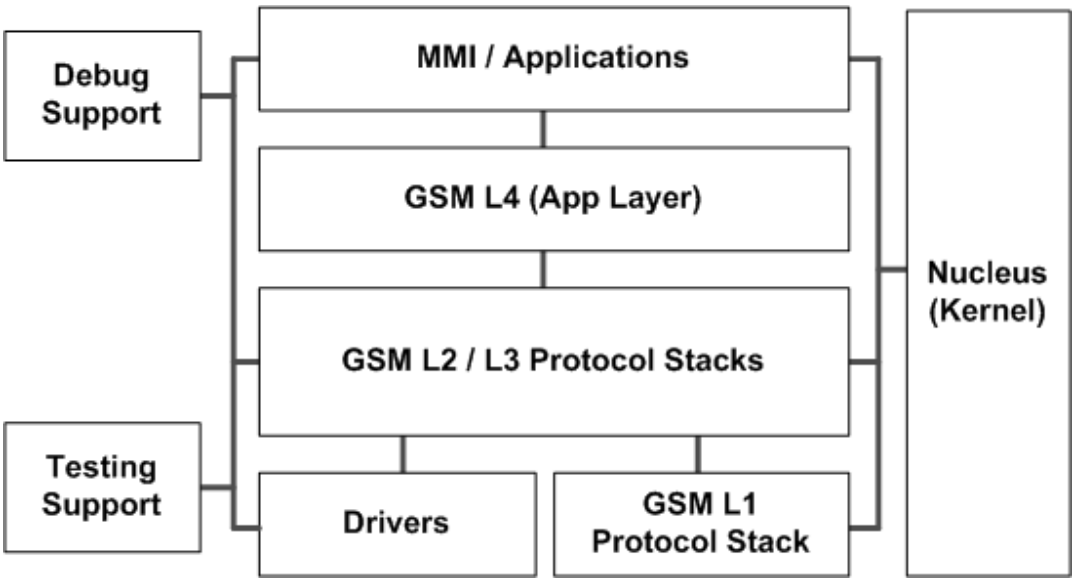


Figure 42. MTK Software Platform Overview [3].
Courtesy http://farm3.static.flickr.com/2743/4283671101_5a60957fb5_o.png

比较 Figure 40 与 Figure 42，Figure 40 中 OS 的位置，应该理解成原理介绍大于实际结构。而 Figure 42 中描绘的，是系统架构，更符合实际情况。即，OS 负责为整个系统，包括各

个协议栈模块，以及应用程序，提供多任务的调度，以及内存的管理。

MTK 使用的 OS 是 Nucleus。Nucleus 原为 Accelerated Technology 公司的产品，开发于 1990 年代。2002 年，被 Mentor Graphics 公司收购。目前 Nucleus 源代码完全开放，无产品版税（Royalty Free），开发和调试工具齐全。Nucleus 系统是模块化结构，可以随意裁剪，支持几乎所有嵌入式微处理器（MCU），可移植性强，无需 BSP（Board Support Package，版级支持包）开发[5]。

Nucleus 除操作系统内核（Kernel）外，还提供 TCP/IP 协议包（Nucleus Net），图形软件包（Nucleus Grafix）等等辅助工具，被广泛应用与各式嵌入式系统中，包括手机，网络设备，车载电子设备，通讯设备，医疗仪器等等。

MTK 选用 Nucleus 的原因，估计有三条，1. Nucleus 质量可靠，2. 开发容易，3. 成本低。而且 MTK 只用了 Nucleus 的内核部分，这样的做法降低了 MTK 软件系统对于 Nucleus 的依赖性。所谓 Nucleus 内核，主要是多任务 并发的处理机制，以及内存的管理，包括以下几个部分。

1. 任务的调度，包括优先级（Priority），时间片（Time Slice），和抢占性（Preemptive）控制机制。

2. 任务间的通信，包括信箱（Mailbox），队列（Queue），和管道（Pipe）通讯机制。

3. 任务间的同步，包括旗语（Semaphore），事件（Event），和信号（Signal）同步机制。

4. 内存的管理，包括分区与动态两种方式，即定长的与不定长的内存分配与释放。

Nucleus 内核，与 Linux 等等其它内核并无重大区别。MTK 在 Nucleus 与其它系统模块之间，设置了一个适配层（KAL OS Adaptation）。这个适配层的意义，在于把 OS 内核的具体实现封装起来，方便系统调用（System Call）。另外，MTK 并没有用到 Nucleus 对外设管理的支持，以及 Nucleus 应用程序图形界面库等等。

关于 MTK 系统的硬件与软件，就介绍到这里。理解了 MTK 的系统，或者更确切地说，针对 FeaturePhone 的软硬件系统，我们就不难理解 SmartPhone 的出现，是 FeaturePhone 的进化产物。而 Figure 40 中提到的 RMI （Remote MMI），可以视为进入 SmartPhone 新世界的入口，且听下回分解。

Appendix,

MTK 软件系统中，各个功能模块名称缩写的全称和简介，参阅 Figure 40。

1. RMI: Remote MMI，例如 PC 可以通过 UART 口与协议栈进行通讯。
2. FMI: Feature rich MMI
3. L4: MMI 通过 L4 与 gsm/gprs 协议栈进行通讯，包括以下子模块,

3.1. ATCI: AT Command Interpreter, 解释来自 PC 端的命令并命令 L4 做相应的动作
3.2. L4A: L4 adaptation Layer, MMI 与 L4A 通过消息通信
3.3. L4C: L4 Control entity, 处理所有的应用程序请求和响应
3.4. UEM: User equipments adaptation, 驱动相关的适配层
3.5. PHB: Phone book management, 电话簿相关的处理，如分类等
3.6. SMU: SIM management Unit, 安全性管理以及 STK
3.7. CSM: Circuit switching protocol stack management 电路交换协议栈管理
3.8. RAC: Registration access control
3.9. SMSAL: Short message service application layer
3.10. TCM: Terminal context management
4. NVRAM: Nor-volatile RAM, 是 MMI 到 Flash 的一个适配层，保存一些默认设置
5. SIM: Subscriber identity module. Handle SIM behavior as ETSI 11.11 description
6. DATA: 电路交换数据服务，包括以下子模块
6.1. FAX: Group 3 Facsimile
6.2. TDT: Transparent circuit switching data
6.3. L2R: Layer 2 relay protocol for non-transparent circuit switching data
6.4. RLP: Radio link protocol for non-transparent circuit switching data
7. CC: Circuit-switched call control 电路交换呼叫控制
8. SS: Supplementary service 附加服务
9. SMS: Short message service 短消息服务
10. SM: Session management 会话管理
11. MM/GMM: Mobility management 移动性能管理
12. SNDCP: Sub-network dependent convergence protocol
13. LLC: Logical link control 逻辑连接控制
14. RR: Radio resource management, 包括以下子模块
14.1. RRM: Handles cell selection and PLMN selection
14.2. RMPC: Handles the procedures in Idle/Dedicated state including the surrounding cell scheme and measurement reporting
14.3. LAPDM: Handles the procedure defined in GSM layer 2
14.4. RLC: Radio link control protocol
14.5. MAC: Medium access control protocol
14.6. MPAL: Adaptation layer for RR and L1A
15. PPP Point to Point protocol layer, 客户端点对点协议

Reference,

[1] GSM Protocol Stack. (http://www.tutorialspoint.com/gsm/gsm_protocol_stack.htm)
[2] GSM Um Interface. (http://en.wikipedia.org/wiki/Um_Interface)
[3] MTK Software Platform. (http://www.docin.com/p-6004509.html)
[4] 浅谈 GSM 手机的 MMI 软件开发. (http://www.ergocn.com/wenzhai35.htm)
[5] Introduction to Nucleus OS. (http://www.docin.com/p-7535534.html)

【8】 自己动手做 XP 手机，DIY 实战指南

2010 年 1 月 20 日，ViewSonic 在北京发布了一款真正意义的电脑手机 VCP08。根据商家的宣传，VCP08 之所以能够被称为真正的电脑手机， 是因为“该机做到了把真正的 WindowsXP 操作系统嵌入进手机当中”[1]。

Figure 8.1 ViewSonic VCP08's shape and size.
Courtesy http://farm5.static.flickr.com/4045/4309204242_024371d466_o.png

ViewSonic VCP08 电脑手机的平面尺寸比普通手机略大，但是厚度则远超普通手机，参见 Figure 8.1。超凡的厚度，并不仅仅是因为 VCP08 手机采用翻盖设计，事实上，VCP08 电脑手机，是 XP 上网本与 MTK 手机，两个独立运行的系统的简单合并。

Figure 8.2 ViewSonic VCP08 is a combination of a XP Netbook, plus MTK feature phone.
Courtesy http://farm5.static.flickr.com/4012/4309206228_4f04c3be75_o.png

VCP08 的外屏延用 MTK 手机系统，是一个自主运行的封闭系统。而内屏则采用 Window XP 系统，配置 Intel Atom Z500 双核 CPU，CPU 速度是 800MHz，内存空间 512MB，硬盘空

间 8GB，内屏屏幕为 4.3 英寸，分辨率高达 800x480 像素，是不折不扣的上网本[2]。不过，VCP08 的电池，只能支持 2 个小时的电脑操作[1]。

一言以蔽之，VCP08 相当于在 XP 电脑上绑一个 MTK Feature Phone。

Figure 8.3 Faked picture, a laptop bundled a MTK phone.
Courtesy http://farm3.static.flickr.com/2735/4308553311_a01df766d6_o.png

有没有可能自己做个电脑手机，也就是能够打移动电话的电脑呢？Figure 8.3 是一个假想图。下面，我们自己动手，做一个电脑手机。

第一步，先准备 4 样硬件。

1. 一台 PC，运行 Windows XP 操作系统。
2. 一张 SIM 卡。

Figure 8.4 SIM Card
Courtesy http://image.tianjimedia.com/imagelist/2009/159/tve53lu1g25x.jpg

3. 带麦克风的耳机。

4. 一台 GSM/GPRS 调制解调器（GSM/GPRS，Modem），例如 MultiTech 的 MTCBA-G-F4 产品系列，串口的 MTCBA-G-F4 或者 USB 的 MTCBA-G-U-F4 都可以，价格分别是 150 美元和 230 美元[3]。 如果嫌 MultiTech 的 Modem 价格偏高，也可以选用国内生产的 GSM/GPRS Modem，安装和调试步骤可能略有不同，请参阅相关产品说明书。

Figure 8.5 GSM/GPRS Modem, MultiModem MTCBA-G-F4 [4]
Courtesy http://farm3.static.flickr.com/2756/4322381820_658a767031_o.jpg

第二步，连线安装。

1. 把 SIM 卡插入 Modem

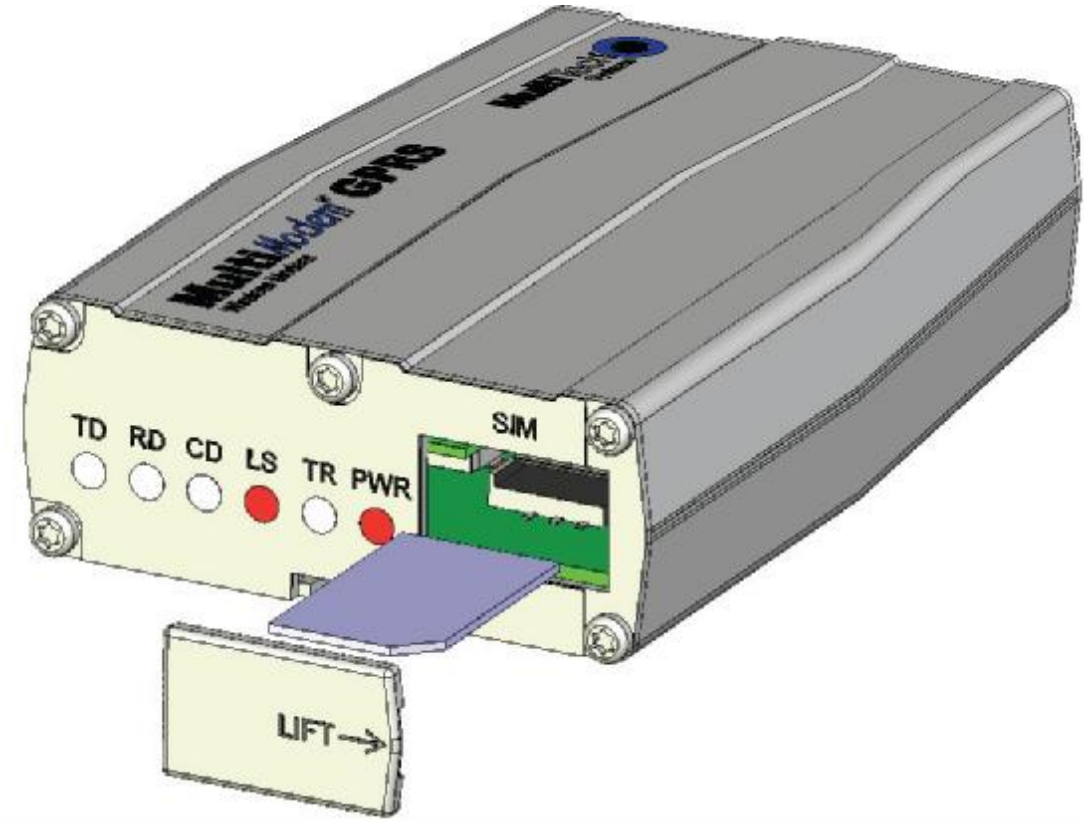


Figure 8.6 Insert the SIM card into the modem [4]
Courtesy http://farm5.static.flickr.com/4029/4321689651_9e75eb95fb_o.png

2. 接上天线和电源，然后接入 PC 机串口或者 USB 口。如果需要语音电话，可以要求厂家提供一条特殊的电缆，一端接 Modem，另一端有两个接头，一个接 PC 机串口或者 USB 口，另一个接带麦克风的耳机，用来接收和传送语音。

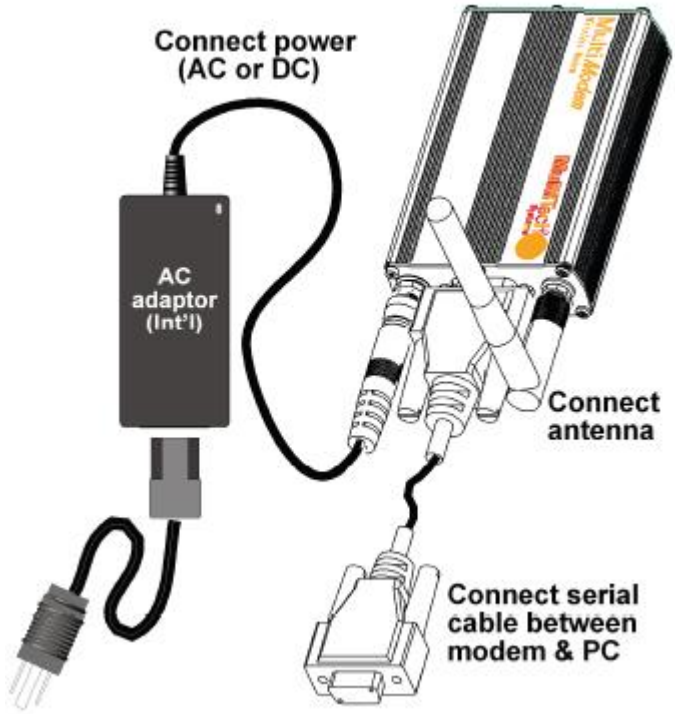


Figure 8.7 Connect to power, antenna, and then the PC via RS232 or USB. [4] Courtesy http://farm5.static.flickr.com/4036/4321691631_daaf69f667_o.png

3. 在 XP 操作系统中，点击 Start（开始）-> Set（设置）-> Control Panel（控制面板）-> Add Hardware （添加硬件）。

如果选用的 Modem 是 MultiModem MTCBA-G-F4，随产品附带的 CD 中，含有相应的驱动程序。

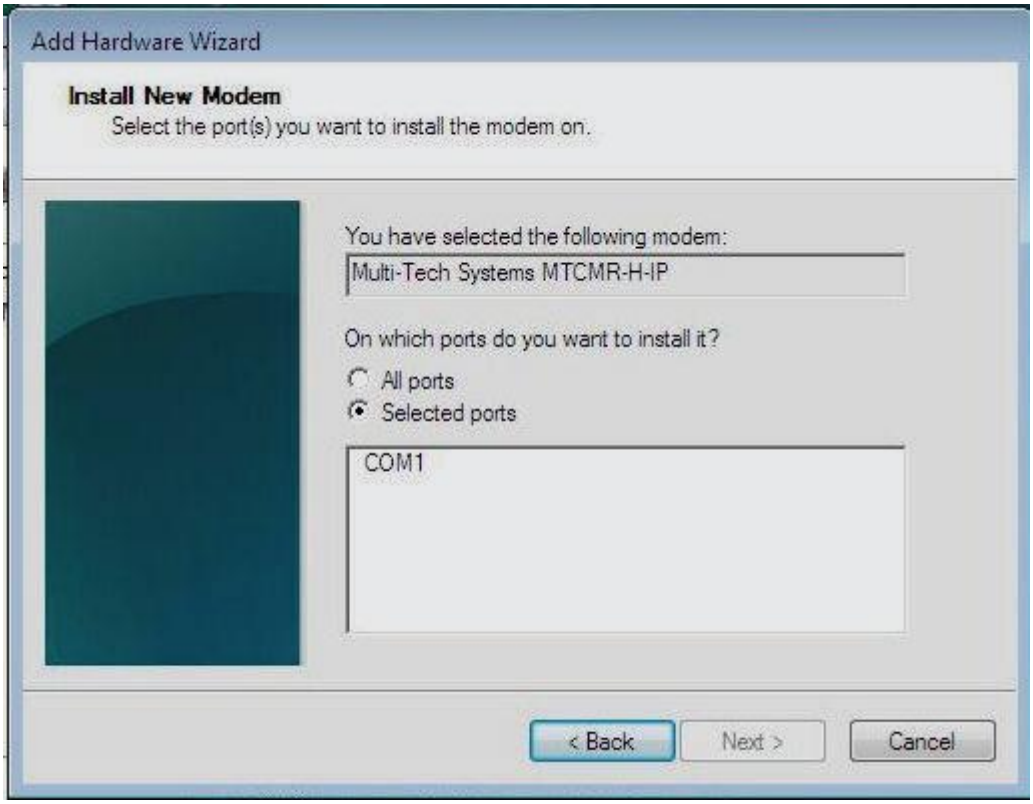


Figure 8.8 Add modem driver.
Courtesy http://farm3.static.flickr.com/2706/4321693937_b38dbaff05_o.png

第三步，调试及使用。

如果一切顺利，DIY 版电脑手机就可以使用了。

1. 监测信号强度。

打开超级终端，即，点击 Start（开始）-> All Programs（程序）-> Accessories（附件）-> Communications（通讯）-> HyperTerminal（超级终端）。如果 PC 操作系统中，没有自带 HyperTeminal 软件，不妨下载替代品，例如 Teraterm，
http://hp.vector.co.jp/authors/VA002416/teraterm.html

在超级终端（HyperTerminal）中，键入 AT+CSQ

2. 检查 GSM 登录及漫游。

在超级终端（HyperTerminal）中，键入 AT+CREG？
回应：0，0 表示还没登录，无法操作
回应：0，1 表示已登录本地网
回应：0，5 表示已登录一个漫游网

3. 打语音电话。

在超级终端（HyperTerminal）中，键入 ATD1234567;
回应：OK
请注意不要忘记键入分号，分号代表语音呼叫。
1234567 是随意举例的一个电话号码，如果你拨打的电话号码是 7654321，那么这个命令就是 ATD7654321;

4. 挂机。

在超级终端（HyperTerminal）中，键入 ATH
回应：OK

5. 发短信。

在超级终端（HyperTerminal）中，键入 AT+CMGS="1234567"发送短信到号码为"1234567"的移动电话。
等待 ">" 出现。
然后键入短信正文，按 Ctrl-Z 结束。

回应：
+CMGS: 52
OK

6. 收短信，这个稍微复杂一些。

在超级终端（HyperTerminal）中，键入 AT+CMGF=1 以此设置成文本格式。
回应："OK"。

键入 AT+CSMS=1，以此设置 SMS 服务为 GSM 07.05 Phase 2+兼容。
回应：
+CSMS: 1,1,1。各个参数的含义参阅[4]。

键入 AT+CNMI=2,2,0,0,0 以此设置短信接收模式为直接转发到我们的 DIY 版电脑手机。
回应：
OK
+CMT: "+17632273726",,"06/03/17,09:06:11+00" （发送端电话号码及时间）
TEST SMS 3 (收到的短信内容）

键入 AT+CNMA，通知网络短信已经收到。
屏幕回应：
OK

7. 连接 Internet 网络。

通过呼叫 PPP，建立 Internet 连接。详细过程比较复杂，参阅[4]。

总结一下，制作一部 DIY 版电脑手机不复杂。如前文所述，电脑手机的关键部件是 Modem。不仅可用 MultiTech 生产的 Modem，其实任何一个 GSM/GPRS Modem 都能用。甚至，也可以用一部 MTK 的 Feature Phone 来替代 Modem，只不过安装和调试略微麻烦一点而已。

我们制作 DIY 版电脑手机，并不纯粹为了自娱自乐，满足好奇心。通过这个例子，有助于认清一下几个问题。

1. 移动通信的任务，其实完全可以用一部 Modem 来完成。

2. 所谓电脑手机，实质上无非是把普通 PC 以及操作系统，与 Modem 相连。PC 操作系统，可以通过 AT 指令，对 Modem 进行相应控制，包括拨号，通话，收发短信等等。

3. DIY 版电脑手机的操作界面非常不直观。为了改善用户体验，不妨通过开发界面友好的手机应用程序包，实现以下功能。不难想像，开发这样一个应用程序包，虽然有一定难度，但也并非遥不可及。

- 拨打电话：发起或接受语音电话。
- 短信管理：编辑短信，发送短信，接受短信，删除，回复或者转发短信等等。
- 通话历史
- 电话本
- 手机设置

4. 至于 PC 上其它应用程序，例如日历，记事本，计算器等等，完全可以忽视 Modem 的存在，或者仅仅把当它当作是一个能够提供数据连接的网卡。

为什么需要电脑手机？根本原因在于 Feature Phone 的功能有限，仅仅限于通话，短信，以及一些预装的多媒体应用。手机生产厂商预装的功能再多，永远无法满足所有用户的，形形色色的功能需求。 所以需要一个类似于 PC 的操作系统，能够支持第三方开发各种通用软件，并且支持用户自主下载并安装非预装的软件。

那么，我们自己做的电脑手机与 WinMobile 或 Android 等等平台的 SmartPhone 有什么区别？事实上我们的电脑手机与其它 SmartPhone 并没有本质的区别，或者说其它 SmartPhone 是更加精致的电脑手机。一印科技制作的 xpPhone，就是这样一款更加精致的电脑手机。

Figure 8.9 xpPhone outlook [5].
Courtesy http://farm3.static.flickr.com/2782/4323520907_edf2e0f14c_o.png

Figure 8.10 xpPhone applications [6].
Courtesy http://farm5.static.flickr.com/4048/4323493367_9c9d2f0fc2_o.png

Figure 8.11 xpPhone applications [6].
Courtesy http://farm5.static.flickr.com/4014/4324245812_5ef1aa6e1d_o.png

虽然一印科技的 xpPhone 外观看起来很炫，用户体验很好。但是从技术角度来讲，结构上与我们的 DIY 电脑手机同出一辙，一印科技的精力放在了外观的优化，以及应用程序的开发上。

事实上，虽然 SmartPhones 款式众多，令人眼花缭乱，但是它们的内部软硬件结构，大多十分相似。从下一章节开始，我们着手解剖 SmartPhone。

Reference，

[1] XP+MTK 双系统手机。(http://tech.163.com/mobile/10/0120/22/5TGLC8MC0011179O.html)
[2] 优派 VCP08 电脑手机。(http://it.21cn.com/mobile/ts/2009/11/24/7099464.shtml)
[3] MultiTech Modem product list. (http://www.multitech.com/en_US/products/families/multimodemgprs/)
[4] MultiModem GPRS Wireless Modem MTCBA-G-F4 manual. (http://www.multitech.com/en_us/documents/collateral/manuals/s000443b.pdf)
[5] xpPhone introduction. (http://www.xpphone.com/product/configuration.html)
[6] xpPhone applications. (http://www.xpphone.com/Product/phone.html)

【9】SmartPhone 的硬件结构

如何区别智能手机（SmartPhone）与功能手机（FeaturePhone）？

有一种观点认为，智能手机本质上是功能手机与便携式电脑（Laptop PC）的结合。功能手机的功能受限于制造厂商的预制，也就是说，用户基本上只能使用手机出厂时已经预制的功能，而不能自主下载并安装新的应用。而个人电脑出厂时，多半是裸机，用户根据自己的喜好，自主决定安装哪些软件。一言以蔽之，所谓智能手机，就是用户能够自主安装应用软件的手机。

按照这个定义，智能手机与上网本（Netbook）有什么本质区别呢？

智能手机与上网本并不存在本质区别。如果说电脑与功能手机是一段光谱的两极，那么智能手机与上网本都处于两极的中间。智能手机更接近功能手机，强调小巧，省电。而上网本更趋近与电脑，强调功能，但是代价是尺寸较大，耗电，续航时间短。例如，Apple 公司最新推出的 iPad 上网本，实际上就是放大了尺寸和功能的 iPhone 智能手机，见 Figure 9.1 并参考文献[1] 。

Figure 9.1 iPad notebook is an enlarged iPhone smartphone. [1]
Courtesy http://farm5.static.flickr.com/4063/4348114249_e5bbef101b_o.png

从硬件结构上看，不妨把智能手机粗略地概括为电脑加移动网卡。我们在上一节，“自己动手做电脑手机”一文中，大致介绍了电脑加移动网卡的具体做法。

智能手机 == 电脑 + 移动网卡，这个提法比较粗略，更精准的提法应当是，智能手机的硬件结构分为 AP 和 BP 两个部分。AP，应用程序处理器（Application Processor），负责大部分应用程序的执行。而 BP，基带处理器（Baseband Processor），也称为通信处理器（CP，Communication Processor），负责所有通讯软件的执行。

如果说功能手机的硬件结构，以 BP 为主体，添加了一些额外的应用程序和相应的硬件外设。那么智能手机 作为功能手机的进一步发展，在 BP 的基础上，增加了 AP，专门用于强化对

应用程序的支持。

但是 AP 并不等同于电脑主板，这主要体现在 CPU 的配置上。一方面智能手机 AP 的 CPU 的运算速度，应当趋近于电脑 CPU 的速度。以往智能手机 AP 的 CPU，速度通常是 200MHz 以上，而近期高档智能手机 AP 的 CPU 速度，有的已经达到 1GHz。另一方面，智能手机 AP 的 CPU 不能一味追求速度，而且要均衡 CPU 尺寸，便于携带，还要考虑省电， 延长续航时间。

在权衡了 CPU 的速度，尺寸，以及耗电量等等诸多因素以后，ARM 系列 CPU 成为智能手机 AP 的 CPU 的主流。当然，并不是所有厂商都接受这个观点，例如 Intel 就不看好 ARM 系列。

2006 年，Intel 把 ARM 指令兼容内核的 StrongARM/XScale 产品线，作价 6 亿美元，卖给了 Marvell [2]。同时，Intel 着力发展 x86 内核的 Atom CPU，与 ARM 系列争夺手机芯片市场。但是代号为 Menlow 的第一代 Intel 手机芯片，由于功耗和电源管理无法满足手机的要求，无法挑战 ARM 系列在手机芯片市场的地位，只好转战上网本 [3]。

但是在 2010 年 1 月份举办的美国家电年度展会（CES）上，韩国厂商 LG 展示了一款新手机，LG GW990，见 Figure 9.2。这款手机的看点，是使用了代号为 Moorestown 的第二代 Atom CPU 芯片。据传闻，Moorestown 的续航时间长达 24 小时 [4,5]。

Figure 9.2 LG GW990, with Intel Moorestown Atom CPU inside [5].
Courtesy
http://www.blogcdn.com/www.engadget.com/media/2010/01/intel-keynote-ces10-0175-rm-eng.jpg

虽然 Moorestown 似乎很有潜力，但是就目前而言，ARM 系列 CPU 在手机芯片市场的霸主地位，是毋庸置疑的。例如，最近几年，多款被市场热捧的智能手机，它们的 CPU 都不约而同地选用了以 ARM Cortex A8 为内核的芯片。

1. Palm 公司曾经在 1990 年代以掌中宝 Palm PDA 风光一时。后来一度沉寂，迷失了自己的定位。2009 年 1 月，在美国家电年度展 会（CES）上，Palm 高调宣布他们研制的 Palm Pre 手机即将上市。这款手机的确很炫，获得该年度 CES 大奖。

Palm Pre 手机于 2009 年 6 月正式上市，它使用的 CPU 芯片，是德州仪器（TI）于 2007 年推出的 OMAP3430 芯片，而 OMAP3430 芯片的内核，是 ARM Cortex-A8 [10]。

2. 同样在 2009 年 6 月份，Apple 公司的 iPhone 3GS 也上市，把 Palm Pre 的风头抢了过去。iPhone 3GS 的 CPU，选用的是 Samsung S5PC100 芯片，这款 CPU 的内核也是 ARM Cortex-A8 [11]。

3. 老牌手机制造商 Moto，业绩持续下滑。但是在 2009 年底，老树新花，Moto 推出以 Google Android v2.0 为操作系统的 Droid，火爆一时。与 Palm Pre 手机不谋而合的是，Droid 的 CPU 也选用了 TI 的 OMAP3430 芯片，其内核也是 ARM Cortex-A8 [12]。

4. Google 一直声称自己不介入手机制造。但是在 2010 年 1 月，由台湾 HTC 代工的 Nexus One，却是 Google 自己的品牌手机。Google Nexus One 手机，内置 CPU 芯片是高通（Qualcomm）的 Snapdragon 系列 QSD 8250 芯片。该芯片的内核也是 ARM Cortex-A8 [13]。

Figure 9.3 Palm Pre, iPhone 3GS, Moto Droid, Google Nexus One, all uses ARM Cortex-A8 CPU [10,11,12,13]。
Courtesy http://farm5.static.flickr.com/4069/4351123874_7c626a9175_o.png

智能手机的 CPU 芯片，核心是处理器内核，例如 ARM 系列内核。除了内核以外，还包括其它外设组件。下面以 TI 的 OMAP3430 芯片为例，解剖一下智能手机 CPU 芯片内部结构。Figure 9.4 是 OMAP3430 芯片的内部结构图，其中内核是 ARM Cortex-A8。

ARM 系列包括型号众多的内核，为什么大家不约而同地选择 ARM Cortex-A8？选择的要点是功能，速度，耗电量三者的权衡。

ARM Cortex-A8 使用的指令集是 ARMv7。StrongARM 系列，使用的指令集是 ARMv4。ARM7 系列和 ARM9 系列，用的是 ARMv4 和 ARMv5 指令集。ARM11 系列，用的是 ARMv6 指令集。

指令集版本号越高，一方面意味着指令的数量越多，从而导致芯片内部电路越复杂，制造难度也越大。另一方面，指令集越大，指令数量越多，也说明芯片的功能越强，运行程序的速度越快。Cortex 内核，是目前所有 ARM 系列 CPU 芯片中，功能最强，速度最快的一类。ARM9 系列 CPU 的速度是 200-400MHz，ARM11 系列是 400-800MHz，而 ARM Cortex A8/A9 高达 800-1000+MHz [7,8,9]。

ARM Cortex A8/A9 功能强，速度快，而且比较省电，这就是以 ARM Cortex A8/A9 为内核的手机 CPU 芯片，被市场推崇的原因。当然，假如 Intel 的第二代 Atom CPU，Moorestown，成功地降低了耗电量，那么就有可能冲击 ARM Cortex A8/A9 的霸主地位。

除了 ARM Cortex-A8 内核以外，OMAP3430 芯片还包含其它专用处理器内核。

1. 视频音频编码解码加速器 IVA2+，用于支持 MPEG4，WMV9，H.264 以及 RealVideo10 等等主流流媒体标准，实现视频会议，并让手机具备录制和播放 DVD 质量的视频的能力。

2. PowerVR SGX 图形内核（GPU），用于增强 2D 和 3D 图片的渲染效果和速度。支持 OpenGL ES2.0 and OpenVG。

3. 图像信号处理内核（ISP），用来实现相机系统的高画质，强性能，和低成本。支持 12M 像素相机模块；实时 JPEG 图像压缩。

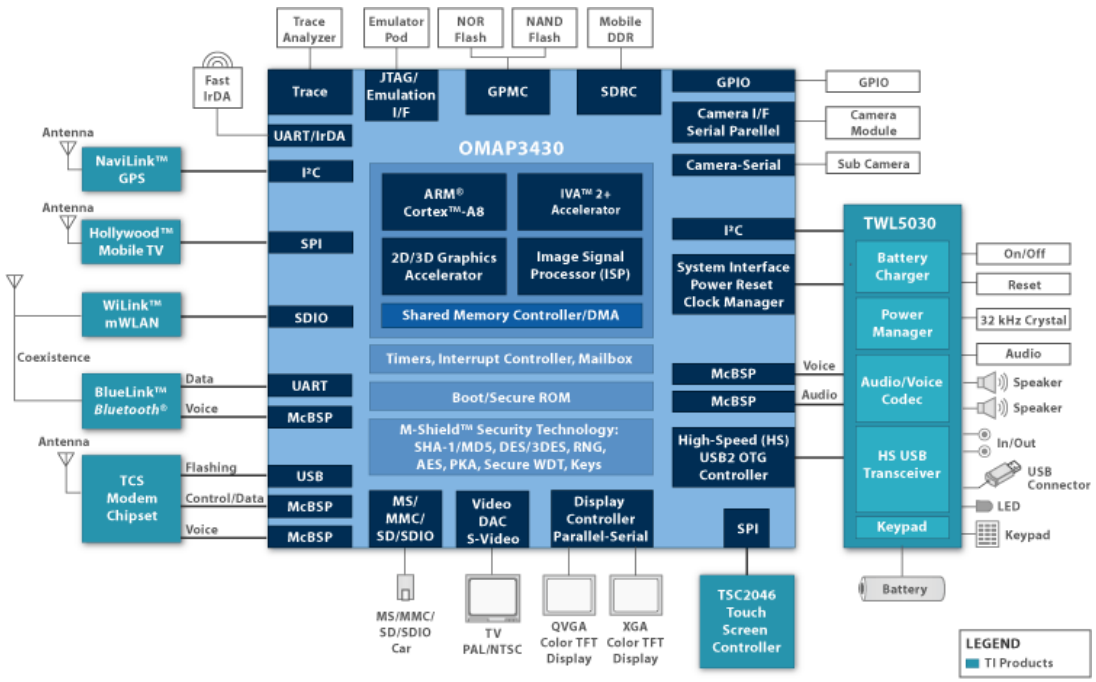


Figure 9.4 TI OMAP3430 CPU Architecture

Courtesy http://focus.ti.com.cn/graphics/wtbu/blockdiagrams/l4_omap3430.gif

选择什么样的 CPU 芯片，就基本决定了手机主板的结构。例如，TI 的 OMAP3430 芯片，本身不处理电源管理以及音频编码解码（Audio/Voice Codec），这两项工作，交给了 TWL5030 专用芯片处理，如 Figure 9.4 所示。因此，以 TI 的 OMAP3430 芯片为 CPU 的主板结构，与选用其它芯片为 CPU 的主板结构，在扬声器，耳机和话筒的连线上，有显著不同，参见 Figure 9.5 中红框标识部分。

Figure 9.5 中上图为 Moto Droid 的逻辑结构图，下图为 iPhone 3GS 的。图中央的黑色方块，显示了应用程序处理器（AP）的 CPU，Moto Droid 的 CPU 是 TI 的 OMAP3430，而 iPhone 3GS 的 CPU 是 Samsung 的 S5PC100。Samsung S5PC100 芯片自身拥有音频编码解码的功能[14]，所以 iPhone 3GS 的扬声器，耳机和话筒直接连线到 S5PC100 芯片上。

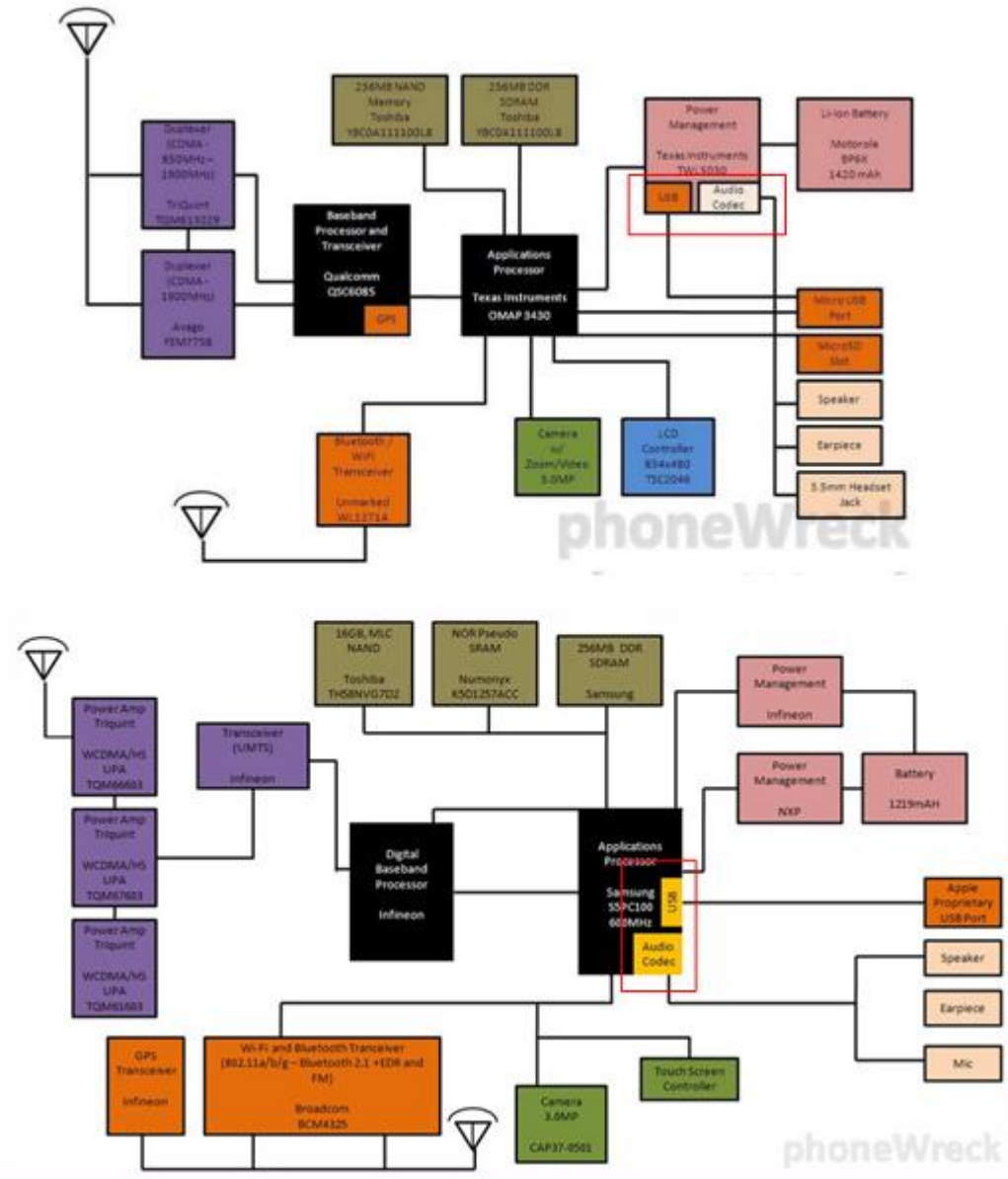


Figure 9.5　Moto Droid vs iPhone 3GS internal logical structures [15,16].

Courtesy http://farm5.static.flickr.com/4028/4351590146_a5c13eff04_o.png

Figure 9.5 中央有两个黑色方块，右边的是应用程序处理器（AP）的 CPU，左边的是基带处理器（BP）的 CPU。Moto 选用了高通（Qualcomm）的 QSC6085 芯片，作为 BP 的 CPU。而 iPhone 3GS 选用的是英飞凌（Infineon）的芯片。关于 BP 的结构，我们将在下一章介绍。

智能手机的主板，以 AP 和 BP 的 CPU 芯片为核心，理解了这两块芯片，就不难理解手机主板的逻辑结构，例如 Figue 9.5 显示的 Moto Droid 和 iPhone 3GS 两款手机的主板逻辑结构。

理解了主板逻辑结构以后，再看主板实物，就不至于眼花缭乱。Figure 9.6 显示的是 Moto Droid 和 iPhone 3GS 两款手机的主板实物照片。把 Figure 9.5 和 Figure 9.6 对照着看，有助于理解。需要注意的是，实物图中看不到 CPU 芯片，因为在主板中，CPU 和 RAM 是叠加在一起的。这个做法叫 Package on Package（PoP），它的好处主要是节省主板空间[17]。

总结一下，本章简要介绍了智能手机的硬件结构。硬件结构中，CPU 芯片是核心，其它外围设备，包括 LCD，相机，扬声器，话筒等等，都围绕 CPU 芯片这个核心布局连线。在 CPU 芯片内部，内核是关键。ARM 系列是目前主流的手机 CPU 内核。其中，最近几年很热门的是 ARM Cortex A8/A9。

下一章，我们将讨论智能手机中基带处理器（BP）的实现方式。比较各个不同的实现方式之间，有哪些差别，各自有什么优缺点, 以及 AP 与 BP 两者协作的方式。

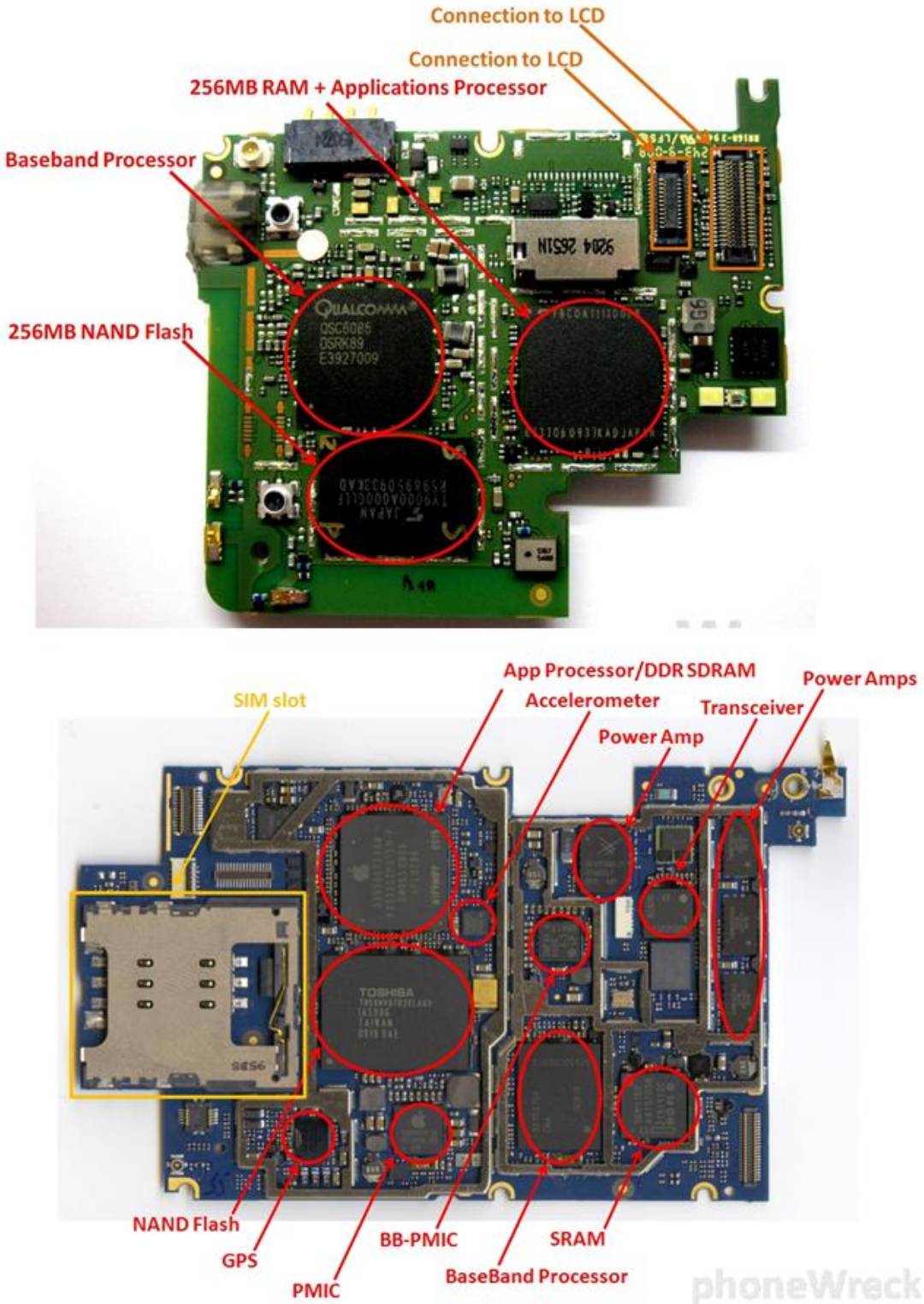


Figure 9.6 Moto Droid vs iPhone 3GS PCBs [15,16].
Courtesy http://farm5.static.flickr.com/4061/4351590148_f6a392d8b9_o.png

Reference,

[1] Comparison of iPad and iPhone technical specs.
(http://www.apple.com/ipad/specs/; http://www.apple.com/iphone/specs.html)
[2] Intel sold StrongARM/XScale to Marvell for 600 million.
(http://www.eetimes.com/news/latest/showArticle.jhtml?articleID=189601851)
[3] Intel drops Centrino Atom Brand after 5 months.
(http://www.pcworld.com/businesscenter/article/149791/intel_drops_centrino_atom_brand_after_five_months.html)
[4] Intel demonstrates Moorestown smartphone.
(http://www.anandtech.com/cpuchipsets/showdoc.aspx?i=3716)
[5] Intel Keynote CES 2010, introducing Moorestown.
(http://www.engadget.com/2010/01/07/live-from-paul-otellinis-intel-ces-keynote/)
[6] Introduction to TI OMAP3430 micro-processor.
(http://focus.ti.com.cn/cn/general/docs/wtbu/wtbuproductcontent.tsp?templateId=6123&navigationId=12643&contentId=14649)
[7] ARM Processor Survey. (http://en.wikipedia.org/wiki/ARM_architecture)
[8] ARM Processor Selector. (http://www.arm.com/products/CPUs/core_selector.html)
[9] ARM Core Overview.
(http://digital.knu.ac.kr/lecture/%EC%82%BC%EC%84%B1%ED%85%8C%ED%81%AC%EB%85%B8MBA/2_arm_core.pdf)
[10] Palm Pre technical spec.
(http://pdadb.net/index.php?m=specs&id=1688&c=palm_pre_cdma)
[11] iPhone series technical spec. (http://en.wikipedia.org/wiki/IPhone)
[12] Moto Droid technical spec. (http://developer.motorola.com/products/droid/)
[13] Google Nexus One technical spec. (http://en.wikipedia.org/wiki/Nexus_One; http://en.wikipedia.org/wiki/Snapdragon_%28processor%29)
[14] Samsung S5PC100 technical spec.
(http://www.samsung.com/global/business/semiconductor/support/brochures/downloads/systemlsi/s5pc100_brochure_200902.pdf)
[15] Moto Droid teardown and analysis.
(http://www.phonewreck.com/2009/11/12/motorola-droid-teardown-analysis/)
[16] iPhone 3GS teardown and analysis.
(http://www.phonewreck.com/2009/06/19/iphone-3gs-teardown-and-analysis/)
[17] Package on Package introduction.
(http://en.wikipedia.org/wiki/Package_on_package)

【10】SmartPhone 的通信机制（BP）

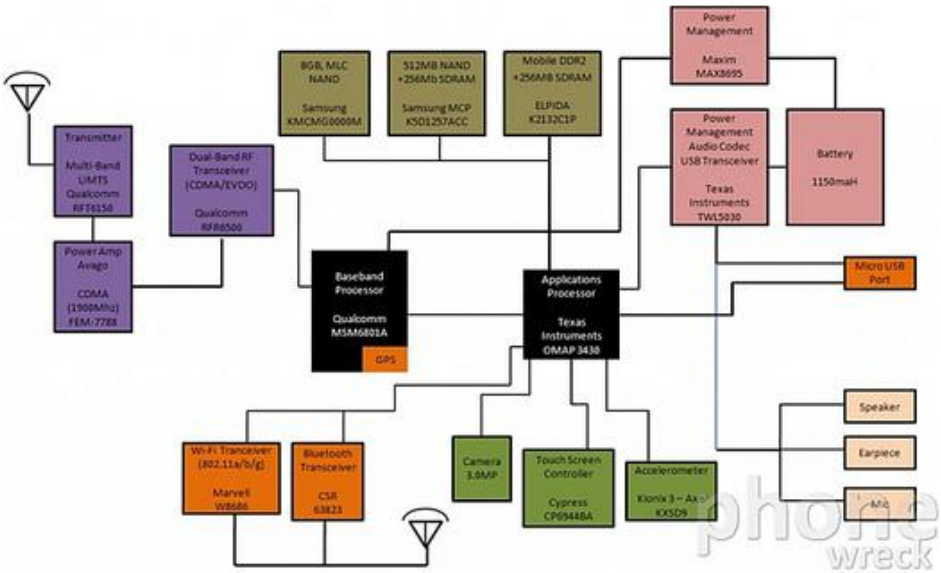
上一章我们说到，智能手机 == 电脑 + 移动网卡，这个提法比较粗略，更精准的提法应当是，智能手机的硬件结构分为应用程序处理器 AP，和基带处理器 BP 两个部分。虽然 AP 部分的功能与电脑主板基本类似，但是硬件结构有很大不同，不同之处体现在 CPU 的选择，以及整个主板的布局连线。

BP 负责所有通讯软件的执行，它的硬件结构， 也并非如网卡那么简单。基带处理器 BP 的实现，有三种方式。

1. 分立器件（Discrete Components）。

把 BP 部分的 CPU，内存，电源管理，无线收发器，功率放大器等等器件，作为散装器件组装起来的做法，称为分立器件。如 Figure 10.1 所示，Palm Pre 的 BP 部分，采用的就是分立器件的做法 [1]。有趣的是，Palm Pre 把 BP 部分与 AP 部分，分别组装在不同的电路板上。这个做法，不同于 Moto Droid 和 iPhone 3GS，参见上一章中 Figure 9.6 的手机实体图，和 Figure 9.5 的逻辑结构图。Moto Droid 把逻辑上属于 BP 的器件，以及属于 AP 的器件，统统组装在同一块电路板上。而 iPhone 3GS，虽然也把 AP 和 BP 的器件组装在同一块电路板上，但是隔离成了不同屏蔽区域。

不同的分立器件的组装方式，对于散热，抗震，重量和外观会有一定影响。各个厂商考虑这些因素时的侧重点不同，导致各自选择了不同的组装方式。


Power Management
Maxim MAX8695
8GB, MLC NAND
Samsung KMGM60000M
512MB NAND +256Mb SDRAM
Samsung MCP K5D1257ACC
Mobile DDR2 +256MB SDRAM
ELPIDA K2132C1P
Power Management Audio Codec USB Transceiver
Texas Instruments TWL5030
Battery
1150maH
Transmitter
Multi-Band UMTS Qualcomm RFT6150
Dual-Band RF Transceiver (CDMA/EVDO)
Qualcomm RFR6500
Power Amp Avago
CDMA (1900MHz) PEM-7788
Baseband Processor
Qualcomm MSM6801A
GPS
Applications Processor
Texas Instruments OMAP 3430
Micro USB Port
Speaker
Earpiece
Wi-Fi Tranceiver (802.11a/b/g)
Marvell W8686
Bluetooth Transceiver
CSR 63823
Camera 3.0MP
Touch Screen Controller
Cypress CP69448A
Accelerometer
Kionix 3 – Ax
KXSD9
phone wreck

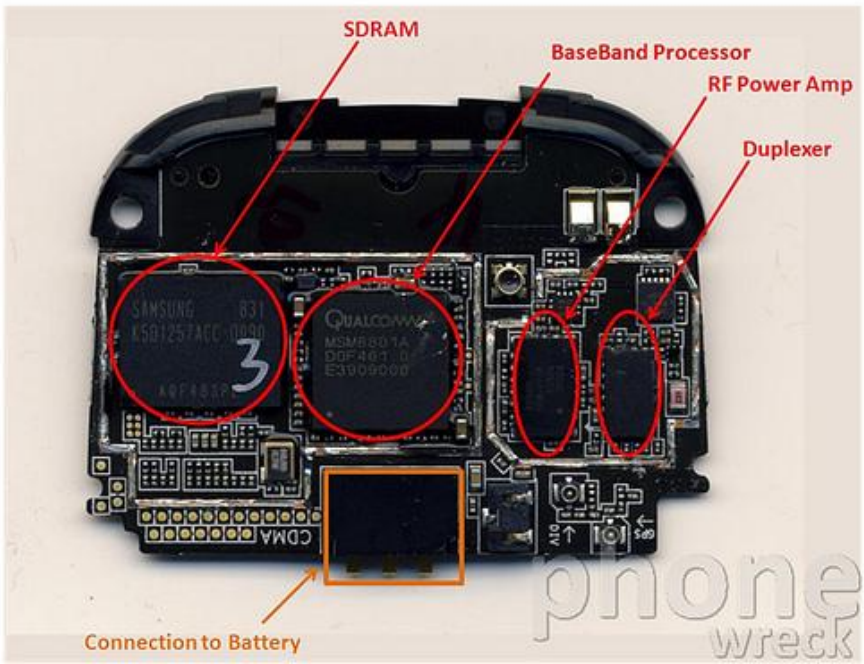

SDRAM
BaseBand Processor
RF Power Amp
Duplexer
Connection to Battery
phone wreck

Figure 10.1 Palm Pre teardown and analysis [1].
Courtesy http://farm5.static.flickr.com/4030/4359122164_0f0e8be100_b.jpg

2. BP 模块。

最接近网卡的方式，是 BP 模块。使用 BP 模块很方便。在设计电路板时，设计好相应的接口，大部分情况下是 miniPCI 接口。在制造时，只需要把外购来的完整 BP 模块，插入相应接口即可。这个做法很方便，但是方便的代价是成本，通常 3G BP 模块的单价超过 100 美元。所以，熟悉 BP 内部结构，技术积累厚实的手机制造厂商，多半不用 BP 模块，而是选择了成本低，但是技术难度大的分立器件方式。

但是，对于其它移动设备，例如电子书（eBook），考虑到作为新产品，抢先进入市场的时间，比成本更重要。而且作为投石问路的尝试阶段，对销量的期望不高。另外，eBook 的赚钱法门在于销售内容，而不是设备本身。或许是考虑到这三个因素，Amazon 的电子书，Kindle 1&2，Barns&Noble 的电子书，Nook，采用的都是 BP 模块的做法，来解决移动上网的需求[2,3,4]。

Amazon Kindle 2 有两个版本，美国国内版用的是 Novatel 出品的 E725 miniPCI 模块，国际版用的是 AnyDATA 的 DTP600W miniPCI 模块。由于两个模块都是 miniPCI 接口，它们可以很容易互换。

Figure 10.2 中，上排左边的照片是 Amazon Kindle 2 国际版的外观。上排中间和上排右边的照片是打开后盖时，看到的 AnyDATA DTP600W BP 模块的外观照片。下排左边的照片是拆解了 BP 模块以后，看到的内部实物照片，下排右边的逻辑图，是 Kindle 2 国际版的逻辑结构图，红线标识的部分，是 BP 模块所包括的构件。

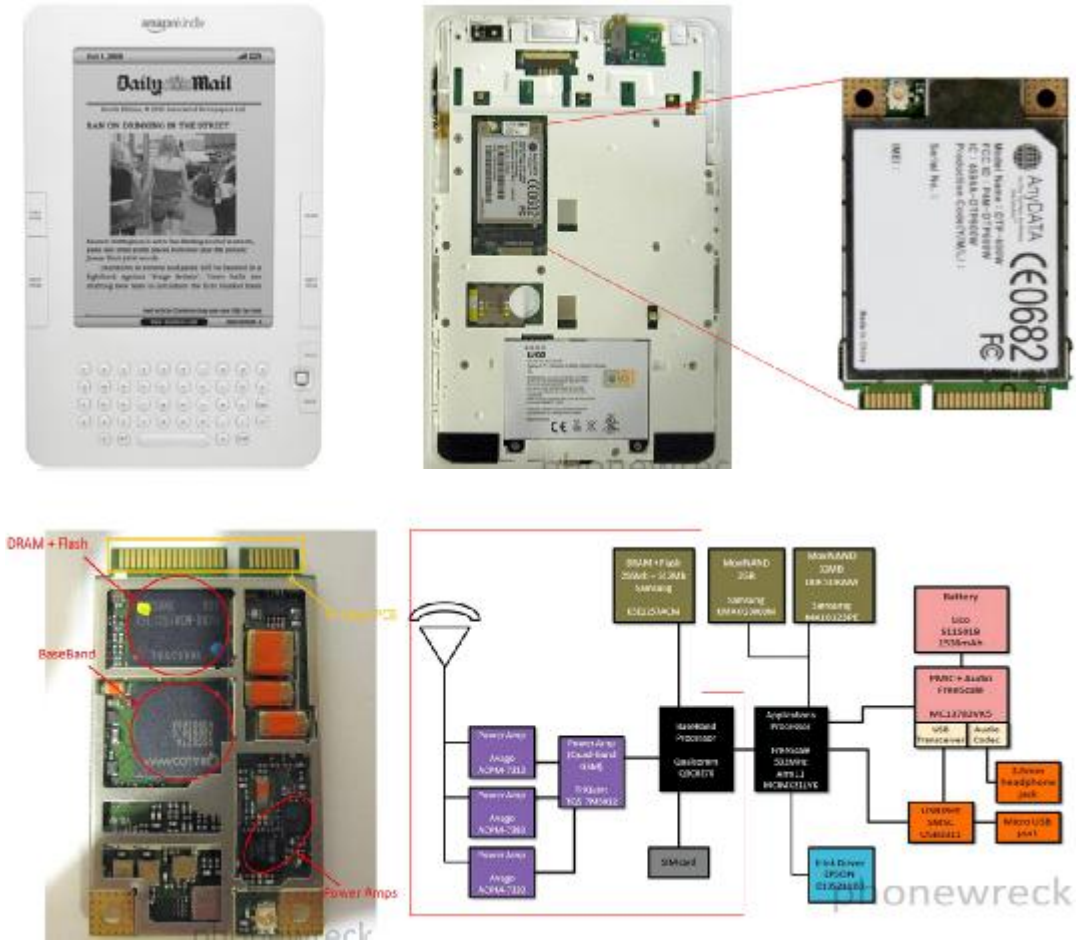


Figure 10.2 Amazon Kindle 2 and its BP module [3,5].
Courtesy http://farm5.static.flickr.com/4007/4364813490_3c6c69de64_o.png

3. SoC（System on Chip）AP+BP 二合一芯片。

不管是前面提到的分立器件的做法，还是 BP 模块的做法，AP 部分与 BP 部分都是分开的，两者之间通过 AT 命令通信 [6]。拨打电话时，AP 通过 AT 命令控制 BP，而有来电时，BP 通过 AT 命令通知 AP。

早期的手机，AP 与 BP 的物理联系，通过串口（UART）来实现，不仅需要串口，而且通常还需要通用输入输出控制线（General Purpose Input/Outpu, GPIO），来协调 AP 与 BP 之间的电源管理等等。在手机闲置时，AP 和 BP 部分都处于睡眠状态，以便省电。拨打电话时，AP 通过 GPIO 唤醒 BP，然后通过串口给 BP 发送 AT 命令。有来电时，BP 也通过 GPIO 唤醒 AP，然后也通过串口发送 AT 命令，通知 AP 启动振铃，接换手机界面等等。

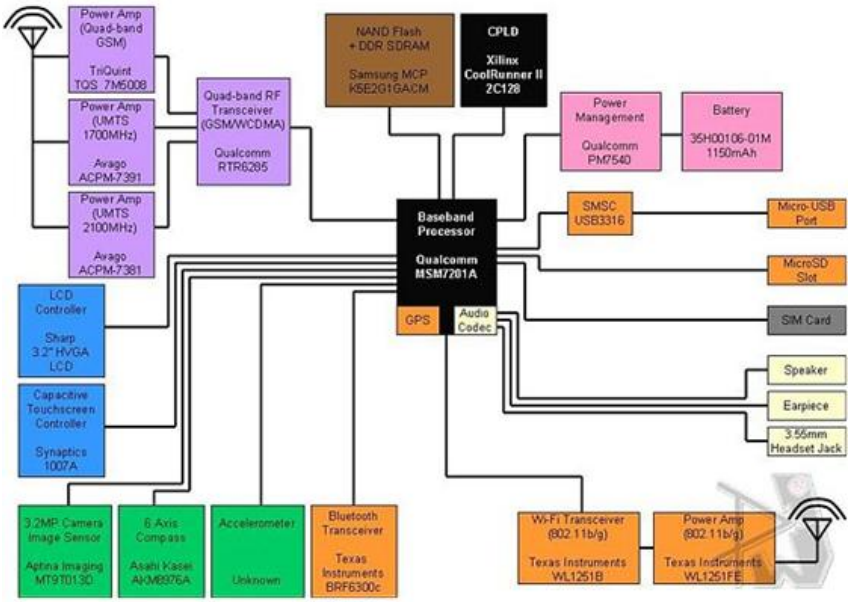
很显然，用串口（UART），GPIO，加 AT 命令的方式，来协调 AP 与 BP 的工作，效率不太高。虽然后期手机，用 USB 或 SPI 取代了 UART，效率有所 提高，但是总体上来说，AP 与 BP 的协调，仍然是整个手机工作效率的瓶颈。

AP 和 BP 各自有一块彼此独立的 CPU 芯片，不仅相互之间的通 信效率差，而且购置芯片

的成本高，占用手机电路板的面积大，同时还耗电。为了克服这些缺点，SoC 二合一芯片的出现，是大势所趋，困难在于 SoC 芯片的设计和制造难度较大[7]。例如，在 SoC 内部，AP 和 BP 分工依然明确，两者之间的通信，通常依靠内存共享（Shared Memory）。但是实现内存共享的技术难度，要比 AT 命令的方式要复杂得多[8]。

GPhone，是指内置 Google Android 操作系统的手机。例如 2008 年 10 月上市的 G1，2009 年 4 月上市的 G2，以及 2010 年 1 月份新鲜出炉的 Nexus One[9]，都是 HTC 的产品[10]。Nexus One 的 CPU 配置，是 Qualcomm 的 QSD8250 1 GHz 芯片[11]，而 G1 和 G2，都使用了 Qualcomm 的 MSM7200 系列芯片，见 Figure 10.3[12]。


T-Mobile
10:10 AM
MENU
T-Mobile
MENU


Power Amp (Quad-band GSM)
TriQuint TQS 7M5008
Power Amp (UMTS 1700MHz)
Avago ACPM-7391
Power Amp (UMTS 2100MHz)
Avago ACPM-7381
Quad-band RF Transceiver (GSM/WCDMA)
Qualcomm RTR6285
NAND Flash + DDR SDRAM
Samsung MCP K5E2G1GACM
CPLD
Xilinx CoolRunner II 2C128
Power Management
Qualcomm PM7540
Battery
35H00106-01M 1150mAh
Baseband Processor
Qualcomm MSM7201A
SMSC USB3316
Micro-USB Port
MicroSD Slot
SIM Card
GPS
Audio Codec
Speaker
Earpiece
3.55mm Headset Jack
LCD Controller
Sharp 3.2" HVGA LCD
Capacitive Touchscreen Controller
Synaptics 1007A
3.2MP Camera Image Sensor
Aptina Imaging MT9T013D
6-Axis Compass
Asahi Kasei AKM8976A
Accelerometer
Unknown
Bluetooth Transceiver
Texas Instruments BRF6300c
Wi-Fi Transceiver (802.11b/g)
Texas Instruments WL1251B
Power Amp (802.11b/g)
Texas Instruments WL1251E

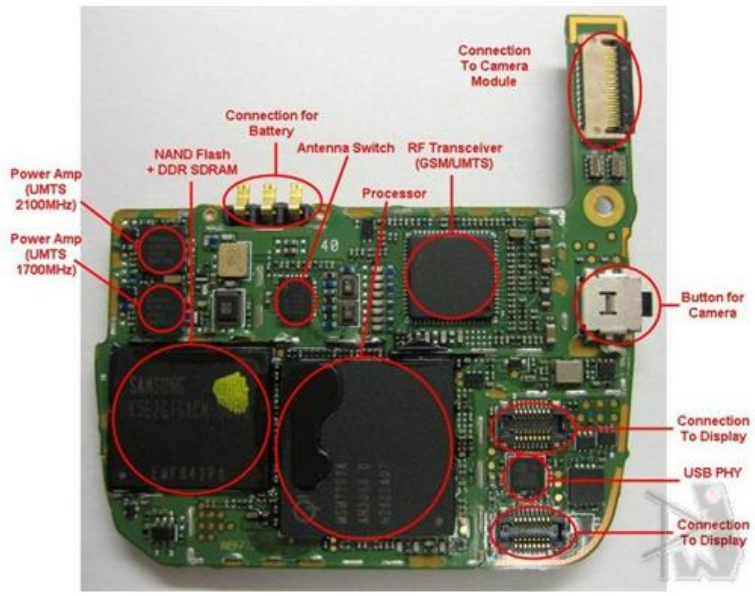

Connection To Camera Module
Connection for Battery
NAND Flash + DDR SDRAM
Antenna Switch
RF Transceiver (GSM/UMTS)
Processor
Power Amp (UMTS 2100MHz)
Power Amp (UMTS 1700MHz)
Button for Camera
Connection To Display
USB PHY
Connection To Display

Figure 10.3 HTC Android G1 teardown and analysis [12].
Courtesy http://farm5.static.flickr.com/4004/4358377359_03420dd1a7_o.png

GPhone Nexus One 所使用的 Qualcomm 的 QSD8250，以及 G1 和 G2 所使用的 Qualcomm 的 MSM7200 芯片，都是 AP 和 BP 二合一的 SoC 芯片。以 MSM7200 芯片为例，它的 AP 部分内置两枚 CPU 内核，一个是 ARM11，另一个是 DSP 专用内核 QDSP5，BP 部分也有两个 CPU 内核，分别是 ARM926 和 DSP 专用内核 QDSP4，参见 Figure 10.4 左侧，以及参考文献[13]。

Qualcomm 的 MSM7xxx 系 列 AP+BP SoC 芯片，于 2006 年左右陆续上市。其实，早在 2001 年，TI 就推出了 AP+BP SoC 芯片，OMAP710。此后，TI 又陆续推出了 OMAP730，733，750，850，1030， 1035 SoC 芯片。TI OMAP710 和 OMAP850 的内部结构图，参见 Figure 10.4 右侧。从 OMAP710 到 OMAP850，速度提高了，内存加大了，功能也有所增强[14]。

但是 Qualcomm 的 SoC 芯片系列的特色，在于积极支持 Android 手机操作系统，其用意或许类似 Intel 绑定 Windows 电脑操作系统，两者结盟形成 Wintel 软硬件共生体，共存共荣占据 PC 领域霸主地位[15]。Qualcomm 是否能够与 Google 结盟，形成 MSM 与 Android 软硬件共生体，谋求智能手机领域霸主地位，大家拭目以待。

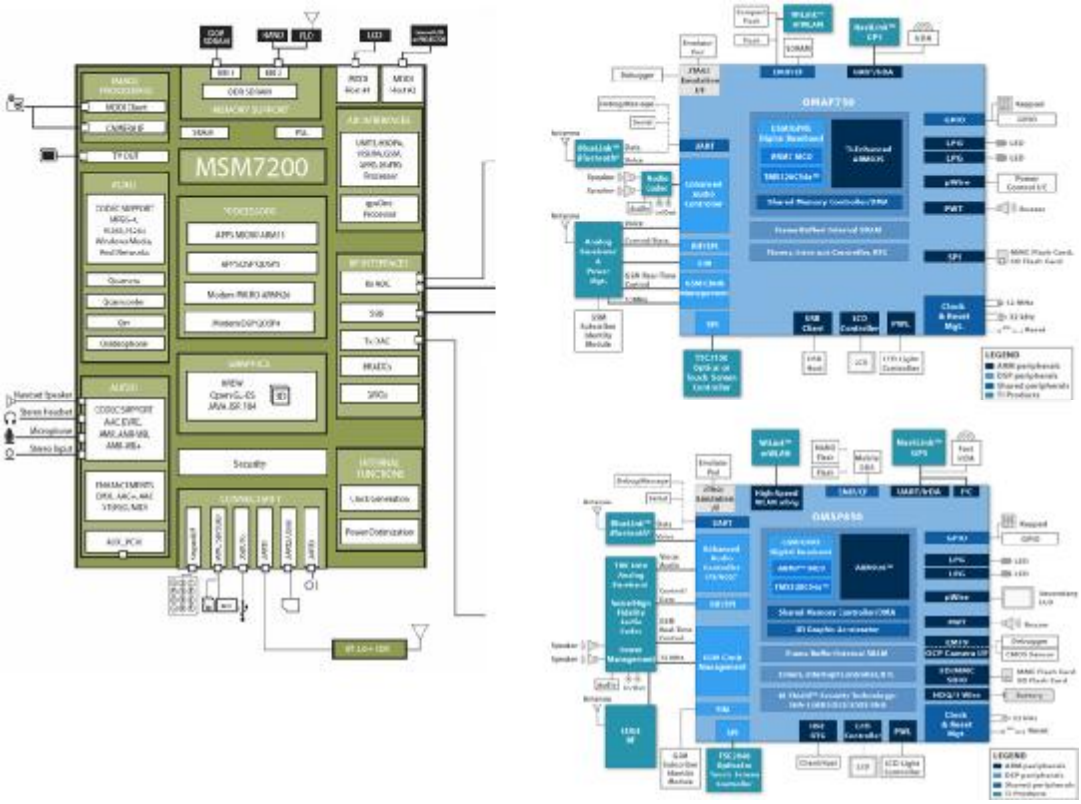


Figure 10.4 Qualcomm MSM vs TI OMAP [10,11].
Courtesy http://farm5.static.flickr.com/4054/4358401341_5b51b0037f_o.png

总结一下，智能手机的 BP 部分，功能上基本等同于功能手机，所以实际上智能手机等同于，功能手机（BP）外加新增的 AP 部分。BP 的做法有三种方式，1. 分立器件，这是早期智能手机的 BP 部分的主要实现方式，例如以 Intel PXA 系列芯片为 CPU 的手机。眼下 iPhone，PalmPre， Moto Droid 也沿袭了分立器件的结构。2. BP 模块，这个方式使用简单，但是成本较高。非手机类的移动设备，常用这种设计。3. AP+BP 二合一 SoC 芯片，技术难度最大，但利润率也最高，是目前手机最普遍使用的 BP 实现方式，例如 HTC 手机既用 TI 的 SoC 芯片，使用的是 Qualcomm 的 SoC 芯片，而 Nokia 智能手机大部分使用 TI 的 SoC。

通吃 AP 和 BP，利用 SoC 芯片的高额利润，在每一部手机上获取最大利润，是每一个芯片厂商的梦想。由于 SoC 芯片开发成本较高，为了维持经济效益，芯片厂商就必须实现大批量生产。因此芯片厂商投入很大力量来帮助手机制造厂商设计基于自己芯片的手机产品。从手机制造厂商立场出发，由于芯片厂商的大力支持，使用 SoC 芯片可以降低自己的开发难度，缩短开发周期，增加市场机会。正因为如此，SoC 成为当前 手机的硬件结构的主流。

2G 到 3G，AP+BP 二合一 SoC 芯片的竞争异常激烈。参与竞争的有 TI，ADI，西门子，Sagem, NXP， Marvell，Qualcomm 和英飞凌（Infineon）等等这些大厂商[16]，谁更有希望胜出，成为行业领袖？中小厂商芯片厂商如展讯和 MTK 以及手机设备厂商 HTC，Motorola 等等，是否能够乱世出英雄，参与分工合作，不断壮大自己？这些问题，留给后续章节讨论。

Reference,

[1] Palm Pre with WebOS teardown and analysis. (http://www.phonewreck.com/2009/06/07/palm-pre-teardown-and-analysis-review-coming-soon/)
[2] Amazon Kindle1 teardown and analysis. (http://www.rapidrepair.com/guides/amazonkindleguide/amazon-kindle-Take-Apart-Guide.htm)
[3] Amazon Kindle2 teardown and analysis. (http://www.phonewreck.com/2010/01/27/amazon-kindle-2-global-wireless-teardownin-depth-analysis/)
[4] Barns&Noble Nook teardown and analysis. (http://androidandme.com/2009/12/hacks/nook-rooted-how-to-and-teardown-pics/)
[5] Amazon Kindle2 network card teardown. (http://www.ifixit.com/Teardown/Kindle-2/624/1)
[6] Introduction to AT commands. (http://en.wikipedia.org/wiki/AT_commands)
[7] Design an optimal wireless SoC. (http://www.eetimes.com/showArticle.jhtml?articleID=49900397)
[8] Solving SoC shared memory resource challenges. (http://www.design-reuse.com/articles/5816/solving-soc-shared-memory-resource-challenges.html)
[9] Google Nexus One 评测。(http://chinese.engadget.com/2010/01/05/nexus-one-review/)

[10] A List of Android Devices. (http://en.wikipedia.org/wiki/List_of_Android_devices)
[11] Google Nexus One teardown and analysis.
(http://www.ifixit.com/Teardown/Nexus-One-Teardown/1654/2)
[12] HTC T1 teardown and analysis.
(http://www.phonewreck.com/2008/12/09/t-mobile-g1-review-and-teardown/)
[13] Android OS 与 Qualcomm MSM7200 芯片.
(http://mobile.onegreen.org/Article/HTML/15203.html)
[14] TI 的 OMAP750 与 OMAP850 两款 CPU 的比较.
(http://hi.baidu.com/sl1987/blog/item/0afb5a663d663f23ab184c1a.html)
[15] The silicon behind Android.
(http://www.engadget.com/2009/10/14/core-values-the-silicon-behind-android/)

【11】移动网络规范的合纵连横

上一章我们讨论了 SmartPhone BP 部分的硬件系统，接下去我们将讨论 SmartPhone BP 部分的软件系统。所谓 BP，指的是基带处理器（Baseband Processor），又称为通讯处理器（Communication Processor，CP），顾名思义，BP 部分负责 SmartPhone 的通信机制。

作为手机的通信机制，BP 部分尤其是软件系统，与移动网络的进化密不可分。2G 时代的移动网络，主要分为两个家族，GSM 和 CDMAOne[1]。从 1985 年，ITU 启动了制订 3G 移动通信系统规范的工作，到 1999 年，历时 14 年，国际电讯联盟（International Telecommunication Union）ITU 终于批准了四个 3G 移动网络规范，GSM/EDGE，UMTS，CDMA2000 和 DECT，总称 IMT-2000，开启了 3G 时代，3G 成为 IMT-2000 的代名词。2007 年，ITU 又批准了 WiMAX，至此 IMT-2000 共有五个 3G 规范[2]。

之所以出现多个规范并存的局面，根本原因在于采用什么样的无线射频技术来传递信息，多种技术可以完成同一个任务，而每种技术都各有长短，没有哪一个技术能够以压倒性的优势胜出，所以出现群雄争霸的局面。

移动网络要解决的核心问题，是同时支持多个手机用户双向通信，这里的关键词有两个，1. 多个手机同时通信，即 Multiple Access（MA），中文译作“多址”。2. 通信双方是双向通信，而不是广播那样我说你听，即 Double Duplex，中文译作“双向双工”。

移动通信典型的多址接入方式有三种，频分多址（FDMA），时分多址（TDMA），和码分多址（CDMA）。FDMA 的基本思路，是把可用频谱分割成若干频段，每个说话的人独占一个频段。当然这是个粗略的形象的说法，通信的内容不完全是语音，而且也包括数据包，例如短信彩信和互联网的接入。另外，通信的主体不是人，而是手机或者基站。

TDMA 的基本思路，是把同一个频段，分成若干时段，大家轮流发言，但每个时段只允许一个人发言。FDMA 和 TDMA 可以混合使用，例如先把整个可用频谱分成若干频段，这是 FD 的做法，而每个频段实行分时制，这是 TD 的做法。

CDMA 与 TDMA 相似，大家共用一个频段，但是不同于 TDMA 的分时制，CDMA 以编码（Code）来区别不同人的发言，相当于每个人在发言前，先出示自己的名牌，但是发 言时间的长短不一。CDMA 技术要比前两者复杂，原因有二，1. 需要把同一个频段的七嘴八舌的发言记录，按不同的发言人切割，然后把同一个人的发言碎片拼接到一起，2. 挤在同一个频段说话的人太多了，会相互干扰，所以需要扩频，也就是把说话人分散到不同的频段中去。与 FD 不同，每个频段不让一个人或者几个人独享，而是见缝插针，动态地分配，以便均摊在各个频段说话的人数。这个技术叫扩频（Spread Spectrum，SS），而扩频又存在多种实现方式，例如直扩扩频（DSSS）和跳频扩频（FHSS）等等。

双向双工的实现方式，与多址接入相似，也是在频段和时段上想办法。通常把从手机到基站的通信通道称为上行（Uplink），基站到手机的通信通道叫下行（Downlink）。对于语音通信来说，上行和下行的流量基本持平。但是对于数据通信来说，下行流量远远大于上行流量，

这是因为看贴的人次远远超过发贴的人次。对于 3G 来说，数据通信的份量很重，所以要保证下行的带宽大于上行的带宽。

频分双工（FDD）把整个可用频谱分成若干频段。对于数据通信，FDD 把多数频段分配给下行，少数留给上行。对于语音通话业务，FDD 给每部手机都分配两个频段，一个给上行，另一个给下行。时分双工（TDD）实施分时制，根据上行和下行的流量，按需分配时段。在 3G 时代，不对称的数据通信业务造成不对称的时段分配，更多时段分配给了下行，而只有少数时段留给了上行。码分双工（CDD） 理论上是可能的，但是或许是因为技术太复杂，所以至今没有成为现实。

FDD 擅长连续控制，适应于大区制的国家内部通信，和国际间漫游，适合于对称业务如话音通话等等，适应于手机快速移动的场景。根据 ITU 对 3G 的要求，使用 FDD 的手机的最高移动速度可达 500KM/h，而采用 TDD 的手机的最高移动速度只有 120KM/h。两者相比，TDD 系统明显稍逊一筹。TDD 的优势在于，适应于在人口高密度地区支持更多人同时通信，适应于不对称的数据业务，例如互联网的接入[3, ch 1]。

GSM 网络，多址接入方式是 TDMA，双向双工方式是 FDD。最初的 GSM 网络，基本上 是一个电路交换网络（Circuit Switched），只能提供语音和短信（SMS）服 务。GSM 的数据率只有 9.6kb/s。为了满足互联网接入和电子邮件之类的数据业务的需求，在 GSM 网络基础上增添了分组交换（Packet Switched）子网，这个子网被称为 GPRS 网络。GPRS 是 GSM Phase2.1 制订的规范，被称为 2.5G，数据率可以达到 171.2kb/s。以往短信是通过 GSM 核心网的 SS7 信令系统来传输，有了 GPRS 网络以后，短信（SMS）业务也可以经 GPRS 网络传输。2.5G 的 GSM/GPRS 网络，仍然采用 TDMA 多址接入和 FDD 双向双工，但是考虑到数据流可以方便地被切割成等长的包，所以对 TDMA 和 FDD 做了一些改进，提高数据包传输效率。后来对 GPRS 又做了进一步的改进，被称为 EDGE，称为 2.75G[4]。

源于 GSM/GPRS 的 3G 网络规范，统称为 UMTS，意思是世界移动通信系统（Universal Mobile Telecommunications System）。UMTS 的概念早在 1987 年就正式提出了。实现 3G 的技术方案有很多，例如 W-CDMA 是日本从 1993 年开始研究的 3G 方案。到了 1997 年，意见渐渐趋同，对于多址接入方式，大家都认同 CDMA，分歧之处在于双向双工，FDD 与 TDD 两种方案难分仲伯。赞同 FDD 的有欧洲的 UTRA WCDMA 和日本的 W-CDMA。1998 年，它们融合为现在的 WCDMA 系统，成为强势候选方案。赞同 TDD 的有 TD-CDMA，沦为弱势[5, pp46-47]。

1998 年，经 ITU 批准，成立了国际标准化组织 3GPP（3G Partnership Project），负责把源于 GSM 的 2G 网络逐步进化成 3G 网络，项目组的重点任务是设计与这个进化过程相关的各种 UMTS 系列网络规范。3GPP 项目组，由多个地区工作组组成，中国区工作组是中国通信标准化协会 （CCSA）[6]。在成立 3GPP 项目组的同时，ITU 又批准成立了 3GPP2 项目组，负责把源于 CDMAOne 的 2G 网络逐步进化成 3G 网络。

3GPP 项目组制订的 UMTS 3G 网络规范，包括 WCDMA，以及 TD-CDMA 和 TD-SCDMA 三种。如果不特别注明，UMTS 规范通常指的是 WCDMA，它采用 FDD 方式的双向双工。而 TD-CDMA 采用 TDD 方式的双向双工，现在已经逐渐淡出。WCDMA 的知识产权，主要把持在美国 Qualcomm 公司手里。中国通过多年努力，在技术上积累了不少创新，同时也

出于反垄断的需要，申报了 TD-SCDMA 规范，并于 2001 年获得 3GPP 以及 ITU 的认可，被接纳在 UMTS Release 4 规范中[7]。TD-SCDMA 的双向双工，采用 TDD 方式。

后 3G 时代，3GPP 项目组不断更新 UMTS 规范，称为 Release 99，Release 4，5，6 等等，最新的版本是 2010 年 2 月份发布的 Release 10。每个版本除了改进旧版的技术以外，而且还增添了新的功能和技术，其中包括对于数据传输部分的改进，HSUPA/HSDPA，以及 HSPA+，它们被称为 3.5G 以及 3.75G。3G 时代结束后，将开始普及 LTE，WiMax 等等网络，也就是 4G 网络[8]。

如前所述，2G 网络中与 GSM/GRPS 对应的，是 CDMAOne。3GPP2 项目组负责设计一系列网络规范，把 CDMAOne 逐步进化成 3G 网络。其进化历程是，CDMAOne（2G），CDMA2000 1xRTT（2.75G），和 CDMA2000 1xEVDO（3G）。EVDO 以后，大部分 CDMA 网络转向 WCDMA/HSPA[8]。

2000 年日本 NTT DoCoMo 公司率先实现了 3G 网络的商业化。2001 年，韩国 SK Telecom 和 KT 两家公司也先后完成 3G 网络的商业化。但是它们使用的是不同的 3G 规范。日本 NTT DoCoMo 使用的是 WCDMA，属于 UMTS 系列。而韩国 SK 和 KT 两家公司，使用的都是 1xEVDO，属于 CDMA2000 系列。

2009 年 1 月 7 日，中国工信部发放三张 3G 牌照，中国移动用 TD-SCDMA，中国电信用 CMDA2000，中国联通用 WCDMA，其中 TD-SCDMA 是中国 拥有自主产权的 3G 技术标准，见 Figure 11.1。从技术上讲，WCDMA 最稳健，TD-SCDMA 最爱国，而 CDMA2000 最没前途[9]。

Figure 11.1 中国 3G 格局[9]
Courtesy http://farm5.static.flickr.com/4051/4415115195_110f66d963_o.jpg

Reference,

[1] Introduction to 2G Wireless Network. (http://en.wikipedia.org/wiki/2G)
[2] Introduction to 3G Wireless Network. (http://en.wikipedia.org/wiki/3G)
[3] 3G Wireless Network, 2'nd Edition. ISBN-13: 978-0-07-226344-2.

[4] Introduction to GSM/EDGE.
(http://en.wikipedia.org/wiki/Enhanced_Data_Rates_for_GSM_Evolution)
[5] UMTS 网络技术. ISBN: 7121012006.
[6] Introduction to 3GPP. (http://en.wikipedia.org/wiki/3GPP)
[7] Introduction to TD-SCDMA. (http://en.wikipedia.org/wiki/TD-SCDMA)
[8] Introduction to UMTS. (http://en.wikipedia.org/wiki/UMTS)
[9] 中国 3G 格局。（http://news.enorth.com.cn/system/2009/01/07/003854399.shtml）

【12】3G 时代的 SmartPhone BP 部分软件系统

最成熟的 3G 网络系统，是 3GPP 项目组制订的 WCDMA。WCDMA 的网络结构，可参考 Figure 12.1，其中有几个特点。

1. 反向兼容 GSM/GRPS 网络。

原有 GSM 网络的基站子系统（BSS）保持不变，并且可以通过原有 A 协议栈和 Gb 协议栈，与改造后的核心网（Core Network）互联互通。

2. 核心网保持了原有 GSM/GRPS/EDGE 网络的 HLR，AUC，EIR，VLR，MSC，SGSN，GGSN 等等网络结构。

主要变化是把原有的 MSC，分拆为 MSC（Mobile Switching Center）和 MGW（Media Gateway）。分拆后的 MSC，仍然负责建立通话双方的电路连接，并且在通话双方在移动过程中，不断切换基站时，维持语音的连续。但是把 WCDMA 网络把电路切换的任务，交给 MGW 专司负责，既提高了系统运行效率，又便于系统的维护[1, pp134]。

3. 增设小区服务广播功能。

小区服务广播中心（Cell Broadcast Center）负责对小区内手机广播各种消息，例如天气，股票，实时交通信息等等。

4. GSM 网络原有的基站子系统（BSS）在 UMTS/WCDMA 系统中，不再被延用，取而代之的是 UMTS 陆基无线接入网（UTRAN，UMTS Terrestrial Radio Access Network）。

UTRAN 中，基站 Node B 负责与手机的无线联系，职能类似于 GSM BSS 子系统中的 BTS。而 UTRAN 中的 RNC（Radio Network Controller）的职能，与 GSM 网络中基站子系统（BSS）中的基站控制器（BSC）的职能很相似。但是由于 GSM 的多址接入方式是时分多址 （TDMA），而 UMTS/WCDMA 的多址接入方式是码分多址（CDMA），导致基站与基站监管所使用的技术也极为不同。因此，原有 GSM 的 BTS 和 BSC，很难在 WCDMA 中沿用，只好另起炉灶，用 Node B 和 RNC 来替换它们[1, pp198]。

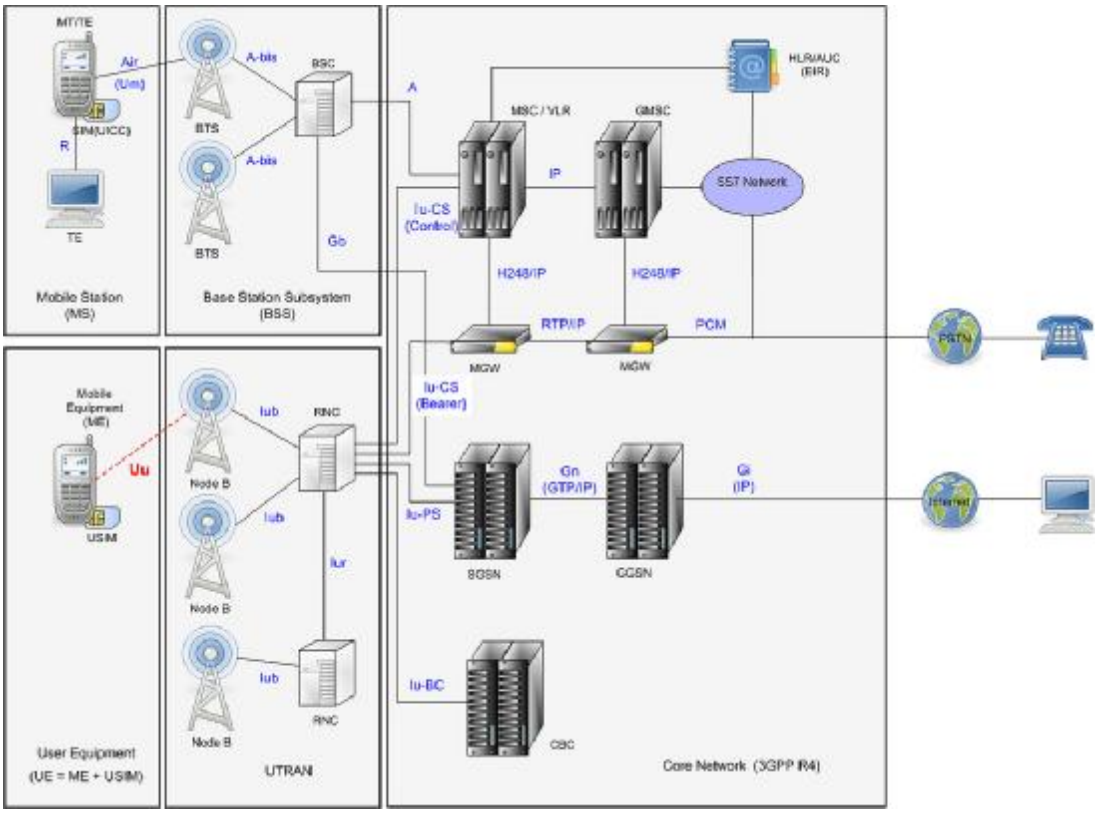


Figure 12.1　3G/UMTS/WCDMA Release 4 Network Architecture [1].
Courtesy http://farm3.static.flickr.com/2708/4403166623_f6c7790b77_b.jpg

在 UMTS/WCDMA 网络规范中，不仅有 Node B，RNC，MSC，MGW，SGSN，GGSN，和 CBC 等等网络构件，而且还有 Uu，Iub，Iur，Iu-CS，Iu-PS，和 Iu-BC 等等协议栈。所谓协议栈，是网络构件之间传输信息时，使用的一系列协议，它们层层叠叠，堆砌成一个栈结构，所以叫协议栈（Protocol Stack），如 Figure 12.2 所示。

1. Uu 协议栈负责在手机与基站 Node B 之间，通过无线方式传输信息。所以，Uu 无线协议栈直接关系到智能手机 BP 部分的技术实现。

2. UTRAN 中基站 Node B，与无线网络控制器（RNC），合称为无线网络系统（RNS）。它们之间的协议栈分别是 Iub 和 Iur，在 Figure 12.2 中，没有详细列出 Iub 和 Iur，而是把 Node B 与 RNC 合并成 RNS，重点描述 RNS 与外界，也就是手机与核心网之间的协议栈。

3. RNC 在处理语音业务时，使用 Iu-CS 协议栈。但是 Iu-CS 的用法，有控制层面（Control Plane）与用户层面（User Plane）之分。

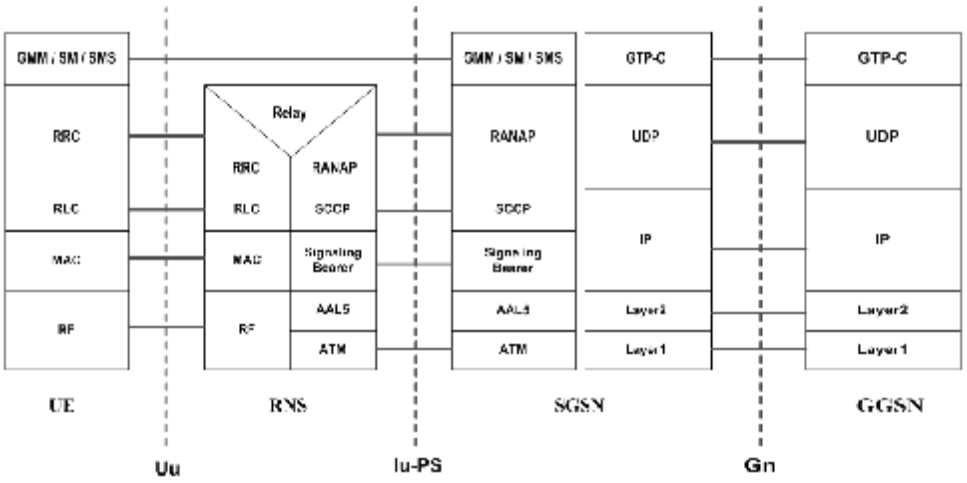
在建立联系通话双方的电路时，RNC 使用 Iu-CS 的控制层面（Iu-CS Control），与 MSC 联系。电路接通以后，在传输通话双方的语音信号的过程中，RNC 使用 Iu-CS 的用户层面（Iu-CS Bearer），与 MGW 联系，参见 Figure 12.1。

4. RNC 在处理数据业务时，使用 Iu-PS 协议栈，并且永远只与 SGSN 联系。但是联系方式也分控制层面与用户层面。Figure 12.2 描述了在处理数据业务的过程中，传输信令和数据实体的各个协议栈。

虽然同属于 Iu-PS 协议栈，但是对于控制层面和用户层面，不同的层面使用的具体协议并不相同。Figure 12.2 上半部分描述了控制层面的协议栈，负责建立数据通道，而 Figure 12.2 下半部分描述了用户层面协议栈，负责传输数据实体。

5. 智能手机的 BP 部分，需要实现 Uu 协议栈的左侧框图中，所包含的所有协议。

以数据业务为例，智能手机 BP 部分，既要实现 Figure 12.2 中上半部分的最左侧的框图中，所描绘的与手机（UE）相关的种种协议，也就是 RF-MAC-RLC-RRC-GMM/SM/SMS 各个模块所涉及 的种种协议，以便完成建立数据通道的任务，这是控制层面的工作。同时也要实现 Figure 12.2 中下半部分的最左侧的框图中，所描绘的与手机（UE）相关的种种协议，也就是 RF-MAC-RLC-PDCP-IP/PPP 所涉及的种种协议，以及相关应用程序（Applications），以便传输数据实体，这是用户层面的工作。



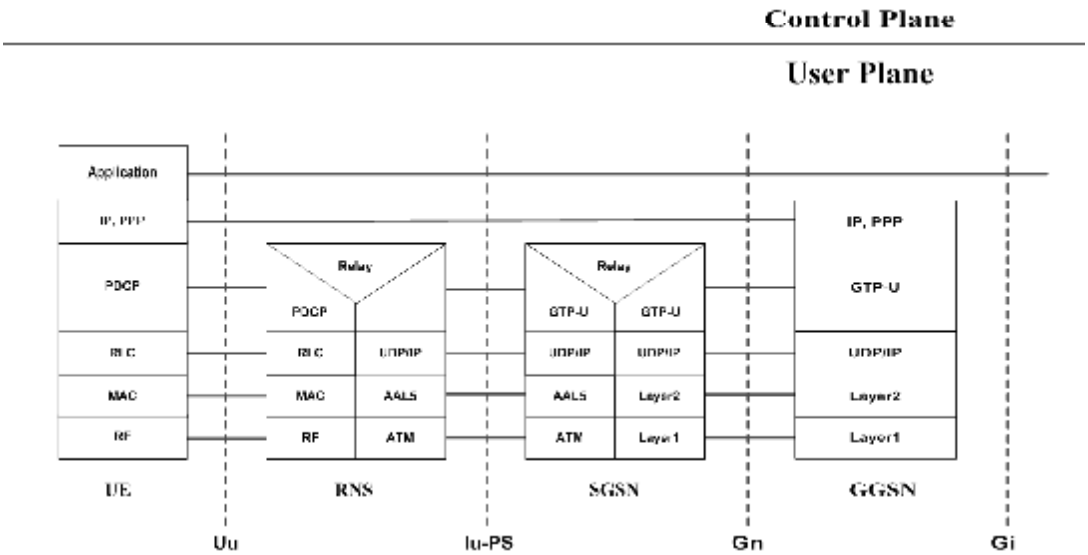


Figure 12.2 UMTS/WCDMA GRPS Protocol Stacks, Release 99.
[1, Figure 6.24, pp 237, and Figure 6.25, pp238]
Courtesy http://farm3.static.flickr.com/2731/4396349395_039ccddf6e_o.png

接下来，我们剖析智能手机的 BP 部分，在建立数据传输通道时，控制层面需要处理的工作，以及传输数据实体时，用户层面需要处理的工作。也就是 Figure 12.2 图中，上半部分最左边的框图中，与手机（UE）相关的协议，也就是 RF-MAC-RLC-RRC-GMM/SM/SMS 这五个模块所涉及的协议和彼此互动。此外还包括，下半部分最左边的框图中，与手机（UE）相关的协议，也就是 RF-MAC-RLC-PDCP-IP/PPP- Application，这六个模块所涉及的协议和彼此互动。

Figure 12.3 描绘了这些模块中包含的部分协议，以及相互关系[2,3]。

1. 各个模块可以被垂直地划分为若干层（Layer），每个模块只与上下层的对应模块发生联系，但是不与同层的其它模块联系。

自下而上，分别是物理层 RF/PHY（Layer 1），链路层（Layer 2），包括 MAC/RLC/PDCP/BMC 各模块，和网络层（Layer 3），包括 RRC 及 Network Control/AMR Voice/CS Data/PS Data 各模块。

同时，自下而上整个系统又被分为接入层（Access Stratum，AS）与非接入层（Non-Access Stratum，NAS）。非接入层的模块负责与核心网联系，例如网络控制模块（Network Control），它负责电话呼叫和来电接通（Call Control，CC），在手机切换基站时，保持通话连续（Mobility Management，MM），和保证数据包的正常传输（GPRS Mobility Management，GMM）等等。

接入层的模块负责无线网络系统（RNS）内部的局部联系，包括手机（UE）与基站（Node B），基站与基站之间，基站与基站控制器（RNC）的局部联系。此外，也包括基站控制器（RNC）与核心网之间 Iu-CS/Iu-PS/Iu-BC 协议栈所涉及的联系。接入层为非接入层提供基础服务[4]。

2. 协议栈分成控制层面（Control Plane）与用户层面（User Plane）。

Figure 12.2 分成上下两部分，上半部分描述控制层面，下半部分描述用户层面。而 Figure 12.3 把控制层面摆放在图左侧，把用户层面放在图右侧。

以非接入层为例，控制层面包括网络控制（Network Control），负责通话控制（CC），移动通话管理（MM），和数据包管理（GMM）。而用户层面负责语音和数据包实体的传输，相应地有三个功能模块，分别是负责电路交换数据传输的模块（Circuit Switched Data，CS Data），包交换数据传输模块（Packet Switched Data，PS Data），和负责语音传递的自适应多速语音编码器（AMR Voice）。

3. 无线接口与通道（Channel）

对于手机（UE）来说，物理层（Layer 1）和链路层（Layer 2）负责如何使用无线频段来传输数据，这两层协议的数据编码方式被称为通道[5]，包括以下三类，

1. Physical Channel（RF），DPCH,P-CCPCH,PRACH, S-CCPCH,AICH, PICH。
2. Transport Channel（PHY-MAC，定义数据的传输方式）, DCH, PCH, BCH,RACH,FACH。
3. Logical Channel（MAC-RLC，定义传输数据的类型）, DCCH,CCCH,BCCCH,DTCH。

网络层（Layer 3）的内容，主要是无线资源控制（RRC）协议，负责对无线资源的分配进行控制，并发送有关控制信令。

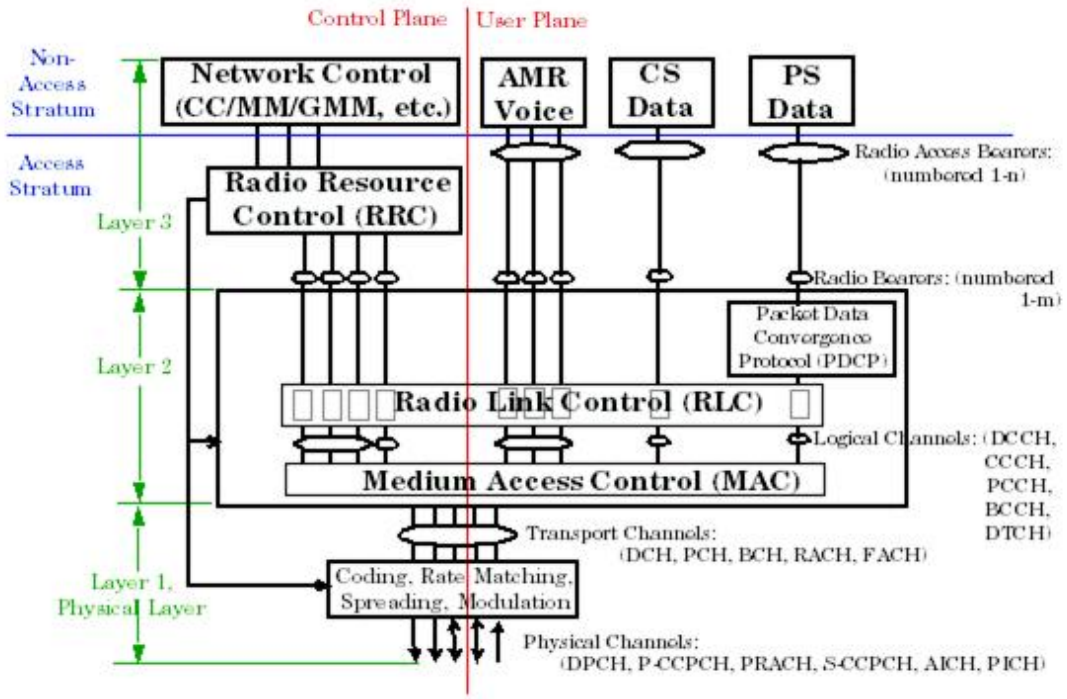


Figure 12.3 UMTS/WCDMA Uu Protocol Stacks and its internal interaction [2]. Courtesy http://farm5.static.flickr.com/4066/4397161512_e634f2f8dd_o.png

理解了 Uu 协议栈包含的各个协议，如 Figure 12.2 所示，以及它们之间的相互作用，如 Figure 12.3 所示，就不难理解智能手机 BP 部分的系统架构。Figure 12.4 是一款智能手机的 BP 部分的系统架构图，这款手机应用于 4G LTE 网络，由英国 4M Wireless Ltd 公司出品。但是这个 BP 部分的系统架构，与 3G 手机的 BP 部分，在结构上基本相似。

虽然结构相似，但是对应于不同的移动网络，例如 WCDMA 和 TD-SCDMA，每个模块的实现细节不完全相同，导致相应的硬件也可能不能通用。这就是所谓“双模双待”手机存在的意义。

具体来说，由于 3G 数据传输速度达到 2M 到 7.5Mb/s（HSPA），实时性要求远远高于 2G，

所以3G的BP 部分通常使用多个DSP硬件等等专用处理器，来处理协议数据的编码解码，而不采用软件的办法。使用硬件固然保证了速度，但是对于不同的通信协议，例如2G 的GSM/GRPS，与3G的WCDMA/HSPA，需要有不同的硬件配合。

不同国家和地区也使用不同的频段，RF 部分也就不同。2G 手机只要支持 GSM /GPRS/EDGE 850/1900 和 900/1800 就可以号称世界手机（除日本和韩国外）。而 3G 的世界手机，一般需要支持 2G 所有的协议和频段，外加 3G 的 2100/850 /1900（覆盖日本和韩国）。对比 MTK 功能手机，这些前辈手机大部分是只支持 2 个频段的 GSM/GPRS，3G 手机的 BP 部分要复杂得多。如果把 MTK 的 BP 复杂度类比成 8086，3G 手机 BP 的复杂度也许就相当于 Core2 Duo。

所有这一切都导致 3G 智能手机的 BP 部分的开发难度很大。在 2G 时代，TI+Nokia 的无敌组合，一度占据了大部分市场份额， 成为市场霸主。但是由于 MTK 的崛起，以及 3G 芯片出货的延迟，使得 TI 逐渐失去基带芯片的市场优势。至于其它 2G 时代的基带芯片制造商，NXP 被收购后苟延残喘，Broadcomm 试图用低价来争夺市场，但几乎无功而返。Marvell 的 Tavor 虽然赢得 RIM 的订单，但是后继乏力。现在只有 Qualcomm 纵横捭阖，用 AP+BP 的 SoC 芯片，牢牢占据了 3G 单芯片市场。同时，Qualcomm 用低端 3G BP 芯片，与英飞凌争夺 BP 专用芯片市场。

由于 BP 部分负责处理通话，实时性要求很高，所以 BP 部分使用的操作系统必须是实时操作系统（RTOS），例如 VxWorks，Nucleus，和 ThreadX 等等。实时操作系统负责各个 Layer 的所有功能模块的任务调度，如 Figure 12.4 中最右侧垂直黄色方框所示。

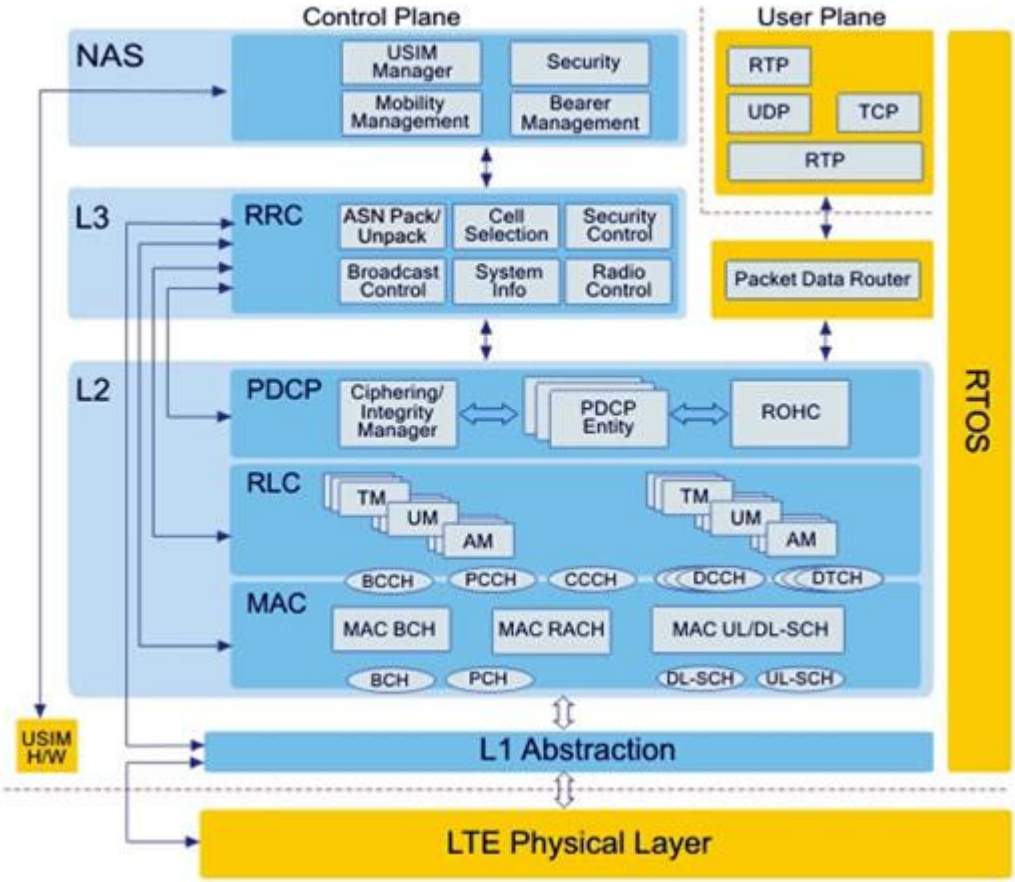


Figure 12.4 3G SmartPhone BP architecture [6].
Courtesy http://farm3.static.flickr.com/2749/4397161506_bd52c7cec9_o.png

总结一下，智能手机的 BP 部分实际上就是一个 Modem。它与功能手机的区别仅仅在于，除了 SIM/USIM 这个外设被保留以外，其它的外设和人机接口统统被去掉，取而代之以 AP 端的控制接口，类似于 MTK 系统中的 RMI，参考本系列第 7 章，MTK 手机软件系统。

智能手机 BP 部分，分为垂直分布的多个 Layers，对应不同的网络传输协议。同时又被水平分割为控制和用户两个 planes，分别负责管理信息通道，以及负责传递信息实体。

智能手机 BP 部分拥有独立的实时操作系统，为各个 Layer 各个 Plane 所包含的所有功能模块，提供任务调度，CPU 和内存管理 等等最基本的操作系统内核服务。

智能手机的 BP 部分结构相当复杂，对应于不 同类型的网络，不同地域的频段分割，软件和硬件都难以通用。

Reference,

[1] 3G Wireless Network, 2'nd Edition. ISBN-13: 978-0-07-226344-2.
[2] WCDMA Radio Access Network Concepts.
(http://wireless.agilent.com/rfcomms/refdocs/wcdma/wcdma_gen_bse_concepts.php)
[3] Wireless Protocols.
(http://www.ccpu.com/trillium-protocol-software-products/all-protocols-list/)
[4] WCDMA Radio Access Network Architecture.
(http://www.comlab.hut.fi/opetus/238/lecture5Lansisalmi001103.pdf)
[5] WCDMA Physical, Transport and Logical Channels.
(http://www.networkdictionary.com/Wireless/UMTS-WCDMA-Logical.php)
[6] BP Architecture by 4M Wireless Ltd.
(http://www.3g.co.uk/PR/Oct2008/3G_LTE_UE_Protocol_Stack_Verification_3G.htm)

【13】SmartPhone AP 部分软件系统

在第 9 章中我们提到，从功能上讲对于智能手机的一个粗略的概括是，智能手机 == 电脑 + 移动网卡，或者更准确地说，智能手机的硬件结构分为应用程序处理器 AP，和基带处理器 BP 两个部分。这里隐含着两个问题，

1. BP 部分与 AP 部分的集成。

2. 传统的功能手机只配备了出厂时预装的应用软件，而不允许用户自主下载并安装第三方应用软件，而智能手机突破了这一限制，因此智能手机的 AP 部分，必须有相应的开放机制，方便第三方软件的开发与安装，同时尽可能降低第三方软件造成对整个系统，包括其它软件的恶意伤害。更进一步说，智能手机的开放机制，不仅针对第三方软件，而且也针对手机生产厂家，允许手机生产厂家更换手机系统的部分硬件设备，或者增设其它外设硬件设备，做到一个通用平台可以出货多个手机型号，帮助手机生产厂家尽可能降低手机研发费用。

对于第一个问题，BP 部分如何与 AP 部分集成，解决方案的思路很简单。翻开任何一本操作系 统教科书，都可以看到标准的分层结构，应用软件 >> 操作系统 >> 驱动器 >> 硬件。不妨把 BP 与 AP 的集成，与操作系统中的文件系统的构成相比较。

文件系统通常包括虚拟文件系统（Virtual File System，VFS）与实际存储设备（Storage Device）两部分。实际存储设备包括闪存或者硬盘等等存储硬件，以及相应驱动器。虚拟文件系统通过驱动器操纵存储硬件，在这个基础上实现文件和文件夹的建立与删除，文件读写等等功能。虚拟文件系统之所以被称为虚拟，是因为应用软件通过标准的接口（APIs），来调用虚拟文件系统实现的文件和文件夹的功能，而与实际存储设备究竟用的是哪一家厂商出品的硬件和驱动器无关[1]。

如果把文件系统中的实际存储系统类比成智能手机的 BP 部分，那么虚拟文件系统相对应的是 AP 部分中的 Telephony Stack。Telephony Stack 提供三个功能，

1. 与 BP 部分的系统间通讯（Inter-Processor Communication，IPC），给 BP 部分下达指令，建立通信通道，发送及接受语音和数据信息。IPC 的实现方式可以是通过传递 AT-Command，也可以是利用共享内存来实现数据交换。

2. 围绕 BP 部分提供的三大基础功能，即语音通话，短信等数据通信，以及 SIM 卡管理，加上与之密切相关的电话本（Address Book），提供以下服务，
   - 拨打电话：发起或接受语音电话。
   - 短信管理：编辑短信，发送短信，接受短信，删除，回复或者转发短信等等。
   - 通话历史。
   - 电话本。
   - 手机振铃及振动设置。
   - SIM 卡管理。

3. 提供标准的调用接口（Telephony APIs， TAPI），方便应用软件调用上述服务。

Figure 13-1 描述的是 WinMobile 6 的 AP 系统中，Telephony Stack 的内部结构。图中紫色部分的模块，严格来说，并不属于 Telephony Stack，它们是应用软件，它们通过调用 Telephony APIs 来使用黄色部分模块的功能。黄色部分的模块，负责实现拨打电话，短信管理，SIM 卡管理，通话历史等等功能，称作 cellcore，由 cellcore.dll 提供，手机设计厂家不可以更改 cellcore。蓝色部分模块，主要是 RIL（Radio Interface Layer），它负责 AP 部分与 BP 部分之间的系统间通讯。RIL 部分是硬件相关的，由手机设计厂家完成。

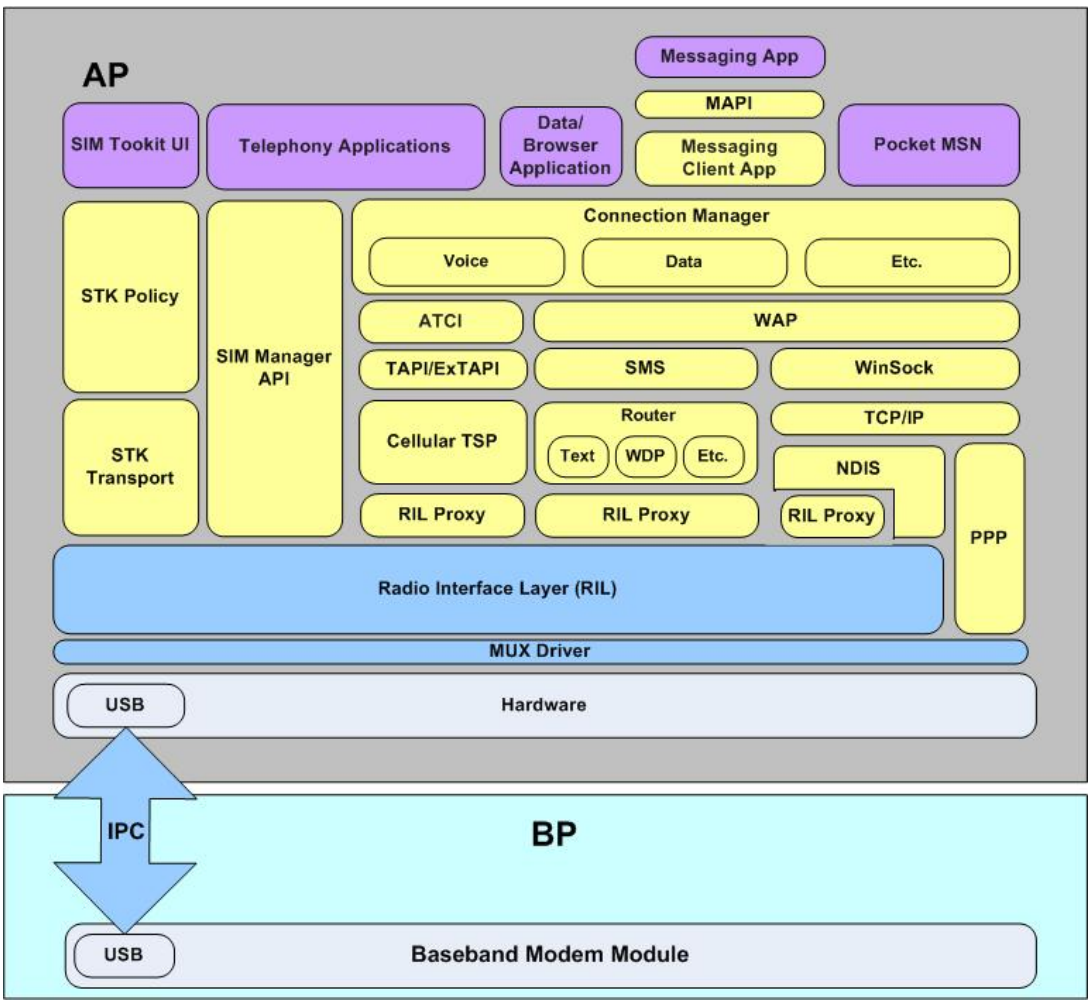


Figure 13-1. WinMobile Telephony Stack.
Courtesy http://farm5.static.flickr.com/4030/4461979382_a450147727_o.png

第一个问题，BP 与 AP 的集成，比较容易解决。第二个问题，AP 的开放机制，提供调用系统资源的标准接口，既方便第三方软件的开发与安装，同时也尽可能降低开放的风险，这个问题不太容易解决。什么方式的调用接口才算方便，什么程度的风险控制才算安全，这两个指标都缺乏公认的衡量准则。在当前情况下我们能做的，或许是比较几个智能手机的 AP 部分的设计，分析一下谁更方便更安全。

Figure 13-2 描述的是，Telephony Stack 在整个 WinMobile 系统中的位置，由红色方框界定。WinMobile 为第三方软件提供了 Win32 APIs，Win32 APIs 不仅提供了分配内存，控制

进程与线程，读写文件，连接网络等等基本功能的调用接口（APIs），也提供了开启和关闭窗口，以及控制窗口控件的 GUI 相关的 APIs。

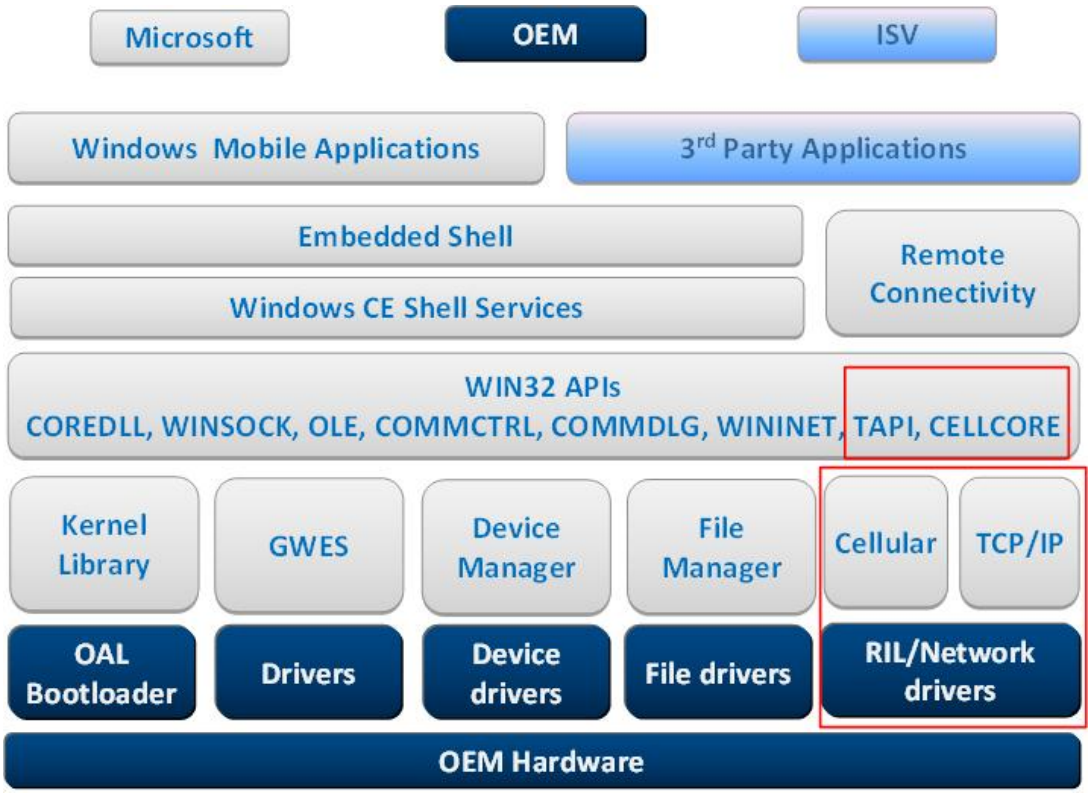


Figure 13-2. WinMobile Architecture.
Courtesy http://farm3.static.flickr.com/2756/4497998261_22aa6faf22_o.png

Win32 APIs 功能全面，但是使用难度大。很多 APIs 附带的参数很多，很多重复性的工作没有被封装，导致应用软件的开发，不仅代码量大，而且容易出错。 有鉴于此，微软把纯 C 的 Win32 APIs，用 VC++重新包装，形成 MFC（Microsoft Foundation Classes）。作为一种 Object-Oriented 语言，VC++具有封装（Encapsulation），多态（Polymorphism）， 继承（Inheritage）等等特性。MFC 利用 VC++这些特性，大大简化了对 Win32 APIs 的调用方式，程序员可以用更精简的代码，完成应用软件的开发。

微软把 MFC 称为一种 Application Framework。Application Framework 这个概念的兴起，源于寻求降低 GUI 开发的难度。GUI 的开发，涉及图形，布局，事件捕捉与响应，消息传递等等诸多技术，不仅入门难， 而且容易出错。Application Framework 借助多种编程环境（IDE），工具集，和软件系统定式，例如 MVC 定式，不仅简化了编程的复杂度，而且通过规范编程方式，降低了出错的风险[2]。

MFC 中的 Object，可以直接分配内存，所以当清除 Object 时，需要手工清除内存分配，不留残余。防范内存泄漏，不 仅是应用软件开发过程中的难点，而且也容易出 bug。如果把 MFC 中的 Object，称为原生态的 Object（Native Object），那么 Jave 和 C#/.NET 中的 Object，是受管制的 Object（Managed Object）。所谓受管制，主要体现在 Virtual Machine 中的垃圾收集器（Garbage Collector）负责管理它们占用的内存空间，而不需要编程者手工分配

内存，与清除内存。

Google 的智能手机 OS，Android，把 Telephony 功能封装成 Java Object，Telephony Manager。依此类推，把 GPS 功能也封装成 Java Object，Location Manager，此外还有 Resource Manager 等等。通过这些 Manager Java Object，把外设硬件（peripheral）的功能封装起来，提供简单的调用接口，降低了应用软件开发的难度，提高了程序员的生产力。同时，还提供 Activity Manager，Window Manager，Content Provider，View System，Notification Manager 等等，简化并规范 GUI 的开发[3,4]。

这些 Java Object 运行在 Virtual Machine 上，它们的内存占用受 Garbage Collector 管制，从而降低了内存泄露的风险。另外，Android 给每个应用软件都分配了独立的 VM 实体，如果某个应用软件出错，导致支撑其运行的 VM 实体崩溃，但是通常不会殃及运行其它应用软件的 VM 实体，从而提高了系统的整体安全。

与 MFC 相比，Android 的 Application Framework，更方便，更安全。当然也有代价，代价是损耗了运行速度。

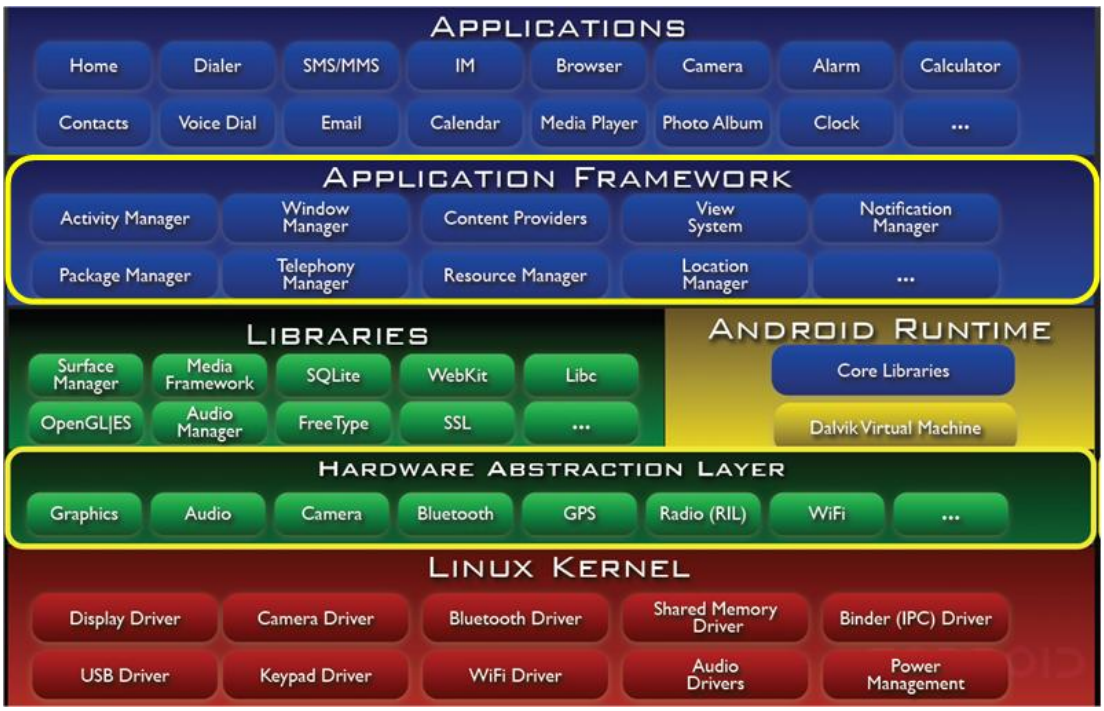


Figure 13-3. Android Architecture [4].
Courtesy http://farm3.static.flickr.com/2713/4497986885_7b1f93c360_o.png

Android 的开放机制，不仅体现在 Application Framework，而且还体现在 Hardware Abstraction Layer（HAL）。关于设置 HAL 的意义，Google 有三点说明[4]，

1. 为各种硬件器件制订标准的驱动器接口。

2. 由于 Android 的内核是开源的，服从 GPL 许可。而有些硬件器件厂商不愿意开源他们的

驱动器程序，有了 HAL 这个隔离带，就可以解决开源的内核与不开源的硬件驱动器之间的矛盾。

3. Android 对于硬件驱动器有一定要求。

这三点说明涉及手机制造产业链上的三个参与者，

1. 如果有标准的驱动器接口，最大的受益者是手机生产厂商。只要硬件外设生产商按照标准接口提供相应的硬件驱动程序，手机生产商就可以自由选择各种配件，大大简化了手机的集成的难度和时间。

2. 不必开源的驱动器程序，受益者是硬件器件生产厂商，而且不给手机生产厂商制造困扰。

3. 比较难以理解的是 Android 对硬件驱动器会有哪些要求，Android 为什么要提出这些要求。为了理解这个问题，不妨分析一个实例，看看 Android HAL 是如何处理 Telephony 的。

Figure 13-4 描述的是与 Telephony 相关的各个层次之间的协作关系。我们关心的 HAL，在图中以 Libraries（User Space）命名，Telephony HAL 的内部结构以绿色标注，包含两个构件，Radio Daemon 和 Vendor RIL。

1. Radio Daemon，它是由 Android 提供的，不随 BP 硬件的生产厂家和型号而改变。在 Android 启动时，Radio Daemon 就被激活，并一直处于运行状态，直到 Android 关闭[4]。

2. Vendor RIL（Radio Interface Layer）。Vendor RIL 由 BP 部分生产厂家提供，不同品牌的 BP，以及不同型号的 BP，绑定不同的 Vendor RIL。Vendor RIL 的存在形式是一个函数库文件，文件命名必须服从约定的规范，libril-<companyname>-<RIL version>.so，方便 Radio Daemon 查找可用的 Vendor RIL[5]。

在实时运行时，应用软件调用 Telephony Stack，而 Telephony Stack 指示 Radio Daemon 去发现当前可用的 Vendor RIL，并动态载入相应的.so 函数库。也就是说，让 Radio Daemon 去实现热拔插（Plug-and-Play）的功能。Vendor RIL 函数库负责 AP 与 BP 之间的 IPC。至此，从应用软件，到 Telephony Stack，到 HAL 中的 Radio Daemon 和 Vendor RIL，到 BP 部分的硬件和驱动器，全线贯通。全线贯通后，应用软件就可以处理拨打电话，发送短信等等通信业务了[4,5,6]。

虽然 Figure 13-4 仅仅描述了与 Telephony 相关的各个层次之间的协作关系，但是对于其它功能，各个层次之间的协作关系也大致相仿，例如音响控制，和电源管理等等。

Android HAL 隐含的意义在于，允许 Android 手机外接其它硬件设备，例如温度计，扩大手机的功能。

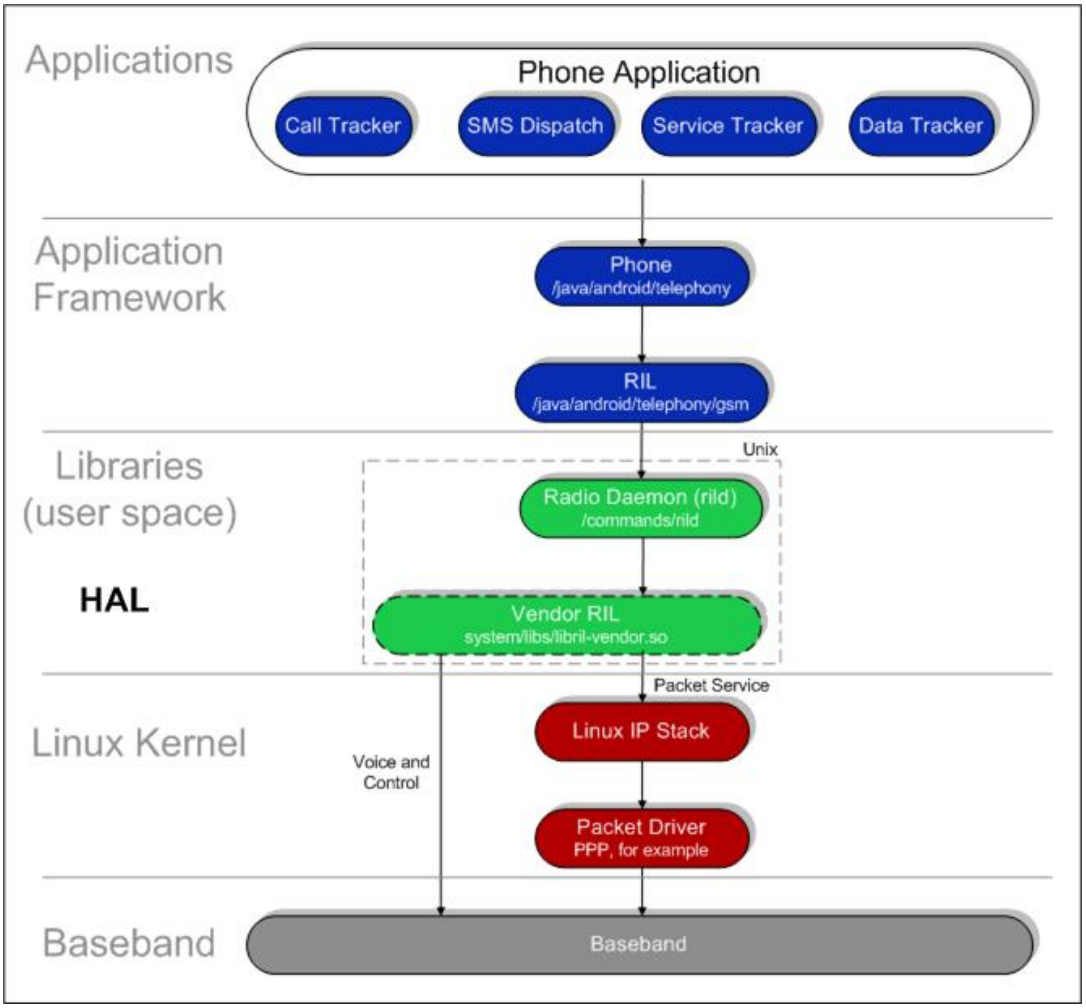


Figure 13-4. Android Telephony system architecture [5].
Courtesy http://farm5.static.flickr.com/4066/4498024565_4c10a45173_o.png

总结一下，智能手机 AP 部分与 BP 部分集成，类似于文件系统中通用的 VFS 与不同厂家提供的 Storage Device 的集成。BP 部分提供基础的通话，数据通信，和 SIM 卡功能。而 AP 部分围绕这些基础功能，提供丰富的服务，例如通话记录，短信的编辑回复和转发等等。这些服务，囊括在 Telephony Stack 函数库中。

为了方便第三方软件的安装和运行，Android 提供了 Application Framework，它以 Java Object 的形式，封装了 Telephony Stack 函数库的功能，GUI 功能，和其它外设硬件设备的功能。Application Framework 不仅降低了第三方应用软件的开发难度，而且降低了第三方应用软件出错的可能性，另外还降低了万一第三方应用软件出错，所造成的对整个系统的破坏。

为了方便集成来源广泛的硬件设备，Android 提供了 Hardware Abstraction Layer。与文件系统中 VFS 与 Storage Device 的协作方式类似，一方面，HAL 提炼出不同硬件厂商都必须提供的共同的功能，把它们囊括进通用的模块，例如 Radio Daemon，通用的模块与硬件的品牌和型号无关。另一方面，HAL 要求硬件厂商提供符合 Android 规范的 IPC 函数库，例

如 Vendor RIL，以便建立起通用的模块与不同品牌和型号的硬件设备之间的通讯渠道。

Reference，

[1] Introduction to Virtual File System. (http://en.wikipedia.org/wiki/Virtual_file_system)
[2] Introduction to Application Framework.
(http://en.wikipedia.org/wiki/Application_framework)
[3] Inside the Android Application Framework.
(http://www.slideshare.net/viswanath7/inside-the-android-application-framework-google-io-2009)
[4] The anatomy and physiology of Android.
(http://www.slideshare.net/viswanath7/anatomy-of-android-google-io)
[5] Android Telephony Porting Guide.
(http://www.kandroid.org/android_pdk/telephony.html)
[6] Android 驱动开发关键技术 HAL 及移植要领. (http://www.slideshare.net/pandodo)

【14】3G SmartPhone 时代的 MTK

分析了 SmartPhone 的里里外外以后，现在我们可以分析 MTK 的机遇和挑战了。MTK 面临的外部环境在发生变化，变化有两条，一是移动网络从 2G 演变到 3G，二是手机由 FeaturePhone 演化到 SmartPhone。

根据前文的分析，MTK 在 FeaturePhone 的产业链中的位置，原本应该只是一个 BP 芯片厂商。但是 MTK 没有局限于 BP 芯片，而是多做一步，担当了系统集成商的角色。把 BP 芯片，外围配件以及驱动器，还有 GUI 界面，和其它应用程序全面集成起来，提供给手机制造商 Turnkey 的解决方案。这样手机 制造商所需要做的附加工作很少，于是催生了大量所谓山寨手机厂商。

在 3G 网络时代，在 SmartPhone 制造领域，MTK 是否能够延续 Turnkey 的战略，把山寨手机厂商，由制造廉价的 2G FeaturePhone，转型到制造廉价的 3G SmartPhone 呢？

不妨把这个问题拆分成三个问题来讨论，1. 3G FeaturePhone 的 Turnkey 解决方案是否可行? 2. 2G SmartPhone 的 Turnkey 解决方案是否可行？3. 3G SmartPhone 的 Turnkey 解决方案是否可行？

1. 3G FeaturePhone 的 Turnkey 解决方案是否可行?

2G 芯片相对简单，但是 3G 的 BP 芯片难度非常大。 现在 3G 芯片市场，Qualcomm 是霸主，市场上 3G Featurephone 主要是采用 Qualcomm 的参考设计。而其它 3G 芯片厂商，如 ST-Ericsson，Marvell 等等，只有很小的市场份额，而 TI 和 Freescale 近乎鞠躬谢幕。

与 GSM/GPRS 等等 2G 网络技术不同，3G 的 BP 技术，涉及到大量专利，而这些专利大多数掌握在 Qualcomm 等等欧美公司手中。对于 MTK 在 2G 市场的成功，Qualcomm 无比垂涎。站在 Qualcomm 角度讲，它势必不情愿 MTK 在 3G 时代复制当年的辉煌。这一判断，可以从 MTK 与 Qualcomm 关于 WCDMA 专利许可转让的谈判中印证[1,2]。

Qualcomm 拒绝与 MTK 达成一揽子专利授权，由 MTK 代付所有 CDMA 专利费。但是给予 MTK 不需要付高通前置金(No Upfront Fee)，之后每颗 3G 芯片出货也不需付给高通 Royalty 的条件。换句话说，对于 MTK 是零使用费，但是每一个使用 MTK 出品的 3G 芯片的手机制造厂 商，都必须单独与 Qualcomm 谈判，取得专利授权。对于山寨厂商来说，与 Qualcomm 单独谈判，通过缴纳专利费，取得合法专利授权，经济上几乎是不可能的事情。所以，山寨厂商要生存，最可能的出路就是忽视 3G 专利，继续像 2G 芯片一样，在不缴纳 CDMA 专利授权的前提下，使用 3G 芯片。当然，严格来说，这是不合法的。

显然 Qualcomm 肯定会预料到这样的前景，或许 Qualcomm 的打算是，时紧时松地动用法律手段，威胁山寨厂商，威胁 MTK 的主要市场。通过这个办法，Qualcomm 间接操控 MTK 的发展，让 MTK 协助 Qualcomm 争夺低端 3G 芯片市场，压制 Broadcomm，ST-Ericsson, Infineon，Marvell 等等 Qualcomm 的竞争对手。

所以，对于 MTK 来 说，3G 功能手机不是没有前途，但是前途是否开阔，受制于 Qualcomm。

2. 2G SmartPhone 的 Turnkey 解决方案是否可行？

暂时撇开 3G 网络的专利授权问题，MTK 在 SmartPhone 制造领域，是否 能够重现它在 FeaturePhone 制造领域的成就呢？如前文所述，SmartPhone 与 FeaturePhone 不同，包含 AP 和 BP 两个部分，而且通常情况，AP 部分对于芯片的要求，比 BP 部分的要求高。另外，近年的 SmartPhone 发展表明，把 AP 部分和 BP 部分的两颗 CPU 内核，集成到同一枚芯片上，即 SoC 的做法，是大势所趋。

MTK 对于 AP 芯片，以及把 AP 和 BP 二合一集成起来的 SoC 芯片，是否做好了充分的准备呢？ 从 ARM 的网站上可以查到，MTK 直接从 ARM 购买的生产许可证，仅限于 ARM7 系列，包括 ARM7TDMI，ARM7TDMI-S，ARM7EJ- S[3]。2007 年 9 月，MTK 收购了 ADI 旗下 SoftFone 手机芯片系列，间接获得了 ARM9 和 ARM9E 系列的生产许可证[4]。从此，MTK 基带芯片产品，有两个系列，嫡系的 MT 系列与兼并来的 SoftFone 系列[5]。在 MT 系列中，编号小于 MT6235 的各款芯片，内核均为 ARM7 系列。而 SoftFone 系列各款芯片中，有的以 ARM7 系列为内核，也有的以 ARM9 系列为内核，ARM9 系列中使用最多的，是 ARM926EJ-S 这一款微处理器[6]。

2010 年 4 月初，人们翘首以待的以 MTK 芯片为平台的第一款 SmartPhone，终于上市。这款手机的代号是 A9[7]，它沿袭了山寨机的传统做法，模仿热门手机。A9 模仿的对象，是 HTC 于 2009 年 2 月推出的 Touch Diamond2 T5353 手机。所以市面上通常把 A9 称为 Touch T5353 MTK 版[8]。虽然外形相似，但是性能却有很大不同，真正的 HTC Touch Diamond2 T5353 支持 3G 网络并兼容 2G，即 GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA[9]，而 Touch T5353 MTK 版只支持 2.75G 网络，GSM/GPRS/EDGE[8]。

除了 BP 部分不相同以外，A9 的硬件性能也与真正的 Touch T5353 有差距，原因在于 A9 使用的芯片。MTK6516 是 MTK 为智能手机打造的第一款芯片，是一款 SoC 芯片，内部集成了两枚 CPU 内核，其中 ARM926EJS 内核专门给 AP 部分使用，而另一枚 ARM7EJS 内核专供 BP 部分使用，参见 Figure 14-1 左侧[10]。A9 使用的芯片，是 MTK6516，而真正的 HTC Touch T5353 使用的芯片是 Qualcomm 的 MSM7200A，这款芯片也是 SoC 芯片，内部集成了两枚 CPU 内核，其中 ARM11 专供 AP 部分使 用，ARM9 专供 BP 部分使用，参见 Figure 14-1 右侧[11]。

虽然，仅仅用 AP 的 CPU 性能来判断手机性能的方法并不全面， 但是不可否认，MT6516 的整体性能是值得怀疑的。所以，MTK 的确有能力解决 2G 智能手机的 Turnkey 方案，而且价格低廉。但是低廉的价格是以削弱功能为代价的。

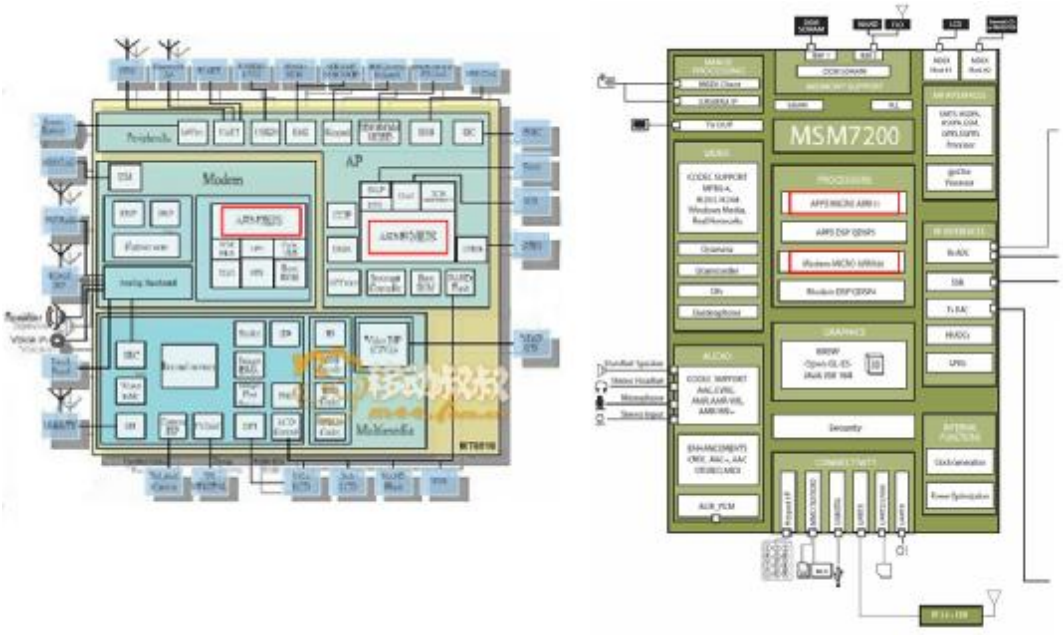


Figure 14-1. MTK6516 vs Qualcomm MSM7200 architectures [10,11].
Courtesy http://farm5.static.flickr.com/4032/4530712619_b6ccd374b8_o.png.

3. 3G SmartPhone 的 Turnkey 解决方案是否可行？

SmartPhone 与 FeaturePhone 的最大区别，在于 SmartPhone 允许用户自主下载第三方应用软件，而 FeaturePhone 只有预装的应用软件。SmartPhone 在 BP 的基础上增加 AP，2D/3D 图形加速器和视频加速器，让 AP 和各种加速器专职负责应用软件的运行。而 3G 网络，解决了无线带宽的瓶颈。有了 SmartPhone 的硬 件结构，和 3G 网络的带宽，应用软件繁荣的外部条件成熟了。

Figure 14-2 是一张截图，取自摩根斯坦利 2009 年底做的移动互联网趋势分析报告。图中红条表示的是全球 iPhone 用户总人数，到 2009 年 9 月，大约是 3 千 4 百万（57-23 == 34MM），AppStore 上可供用户自主下载的第三方软件总数是 10 万个，而用户下载人次是 20 亿次，平均每个软件的下载人次是 2 万（2,000MM/0.1MM==20K）。这个数字是惊人的。如果摩根斯坦利的报告是准确的话，结论非常明确，第三方软件非常受用户欢迎。

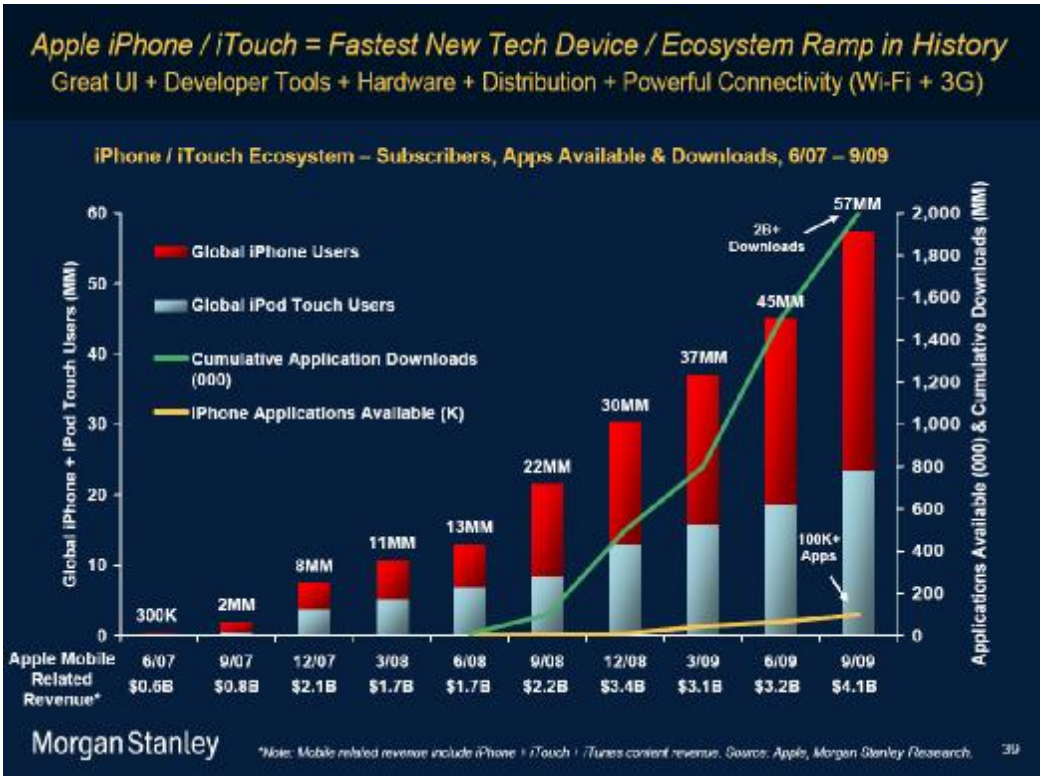


Figure 14-2. iPhone and applications growth.
Courtesy http://farm5.static.flickr.com/4059/4504551471_85fe7265bf_o.png

但是同样是摩根斯坦利的这份报告，另一张图却显现着相反的景象。Figure 14-3 是 2009 年第三季度与 2008 年同期，世界各大市场 SmartPhone 的市场份额。摩根斯坦利乐观地认为，SmartPhone 的市场份额在快速成长，商业前景明朗。

其中值得特别关注的是日本的 SmartPhone 市场现状。日本 3G 网络从 1990 年代初开始推广，迄今已经接 近 20 年，所以日本的 3G 市场的成长情况，对于包括欧美的整个世界范围而言，有领先示范的意义。令人意想不到的现象是，日本的 SmartPhone 市场份额只有 50%左右，也就是说，在 3G 网络普及了近 20 年，在用户普遍富裕的日本，居然还有将近一半的用户，仍然还在使用传统的 FeaturePhone。

摩根斯坦利没有详细分析这一怪异的现象。或许日本没有出现 iPhone 这样抢眼的手机？或许日本没有出现 Google Map，YouTube 和 Facebook 这样有人气的第三方应用软件？或者是日本的 Feature phone 上已经预置足够的应用程序？

也许，最可信的解释是 SmartPhone 的应用软件虽然热闹，但是到目前为止，尚没有出现杀手级的应用，让用户不得不用。而对于一半左右的用户而言，他们对于手机的依赖，还停留在通话和短信这些基础功能。他们没有足够的动机，花费超过功能手机一倍甚至几倍的价钱，仅仅为了时尚，去购买对于他们而言华而不实 的 SmartPhone。这也许可以解释为什么 K3 在 900 元的价位仍然没有达到预计的热买。

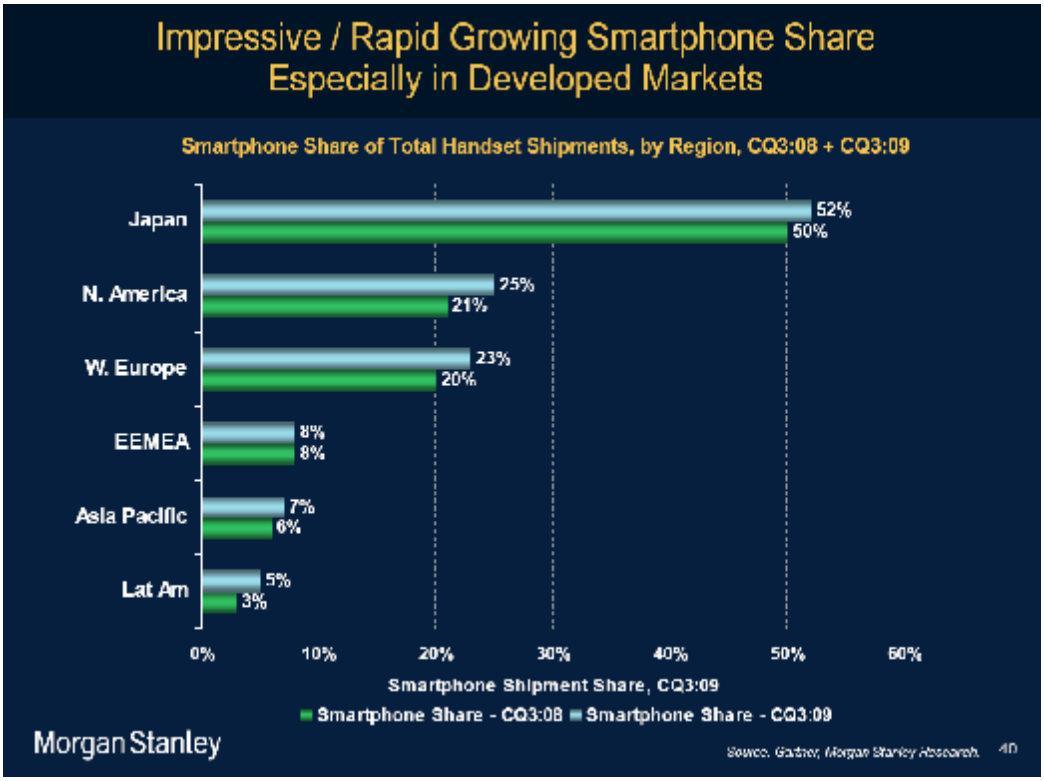


Figure 14-3. Global SmartPhone market shares.
Courtesy http://farm3.static.flickr.com/2678/4504551503_87b1f2fe45_o.png

什么是杀手级应用？针对不同的市场，杀手级应用也应该是不同的。对于中国市场而言，用户热衷的通信服务是 QQ，搜索是百度，消遣是人人网和开心网，购物是淘宝，等等。要开拓中国的 SmartPhone 市场，或许可以从移植这些应用入手。

总结一下，在 3G 网络时代，在 SmartPhone 闪亮登场的当下，对于 MTK 而言，或许值得注意以下几点。

1. 牢牢把握 FeaturePhone 市场。FeaturePhone 不仅目前占据中国市场的绝大多数份额，而且在未来几年，仍然是中国手机市场的主流。

2. 对于 SmartPhone，因势利导，以低端 SmartPhone 芯片为主攻方向。所谓低端 SmartPhone，就是外形像流行的 SmartPhone，预装了中国用户热衷的 QQ，百度，淘宝等等软件，允许用户自主更新这些软件的版本，但是不鼓励用户下载更多应用软件的手机。这种手机介于传统 FeaturePhone，和高端 SmartPhone 之间。有限满足用户对于 SmartPhone 的热情，但是更强调照顾用户的购买能力。

Figure 14-4. MTK iPhome3G, an enhanced feature phone mimicking smartphone outlook, and MTK A9, an entrylevel smartphone mimicking HTC's Touch Diamond2 [13,14]. Courtesy http://farm5.static.flickr.com/4044/4533965082_70eae21b9a_o.png

Reference，

[1] MTK and Qualcomm enter into patent arrangement. (http://www.mediatek.com/en/news/info.php?sn=26)
[2] 高通给联发科零授权金是另有打算。(http://forum.eet-cn.com/BLOG_ARTICLE_2345.HTM)
[3] ARM Processor Licensees. (http://www.arm.com/products/licensing/licencees.html)
[4] MTK 收购 ADI 手机芯片产品线。(http://www.esmchina.com/ART_8800078804_1400_2101_3101_4300_b1c7f2ad.HTM)
[5] MTK Product Lines. (http://www.mediatek.com/en/product/list.php?cata1=1)
[6] MTK SoftFone Product Line. (http://www.mediatek.com/en/product/list.php?cata3=2)
[7] 第一款 MTK 平台山寨手机，代号 A9。(http://www.me189.com/article-notice-84.html)
[8] 第一款 MTK 平台山寨手机视频。(http://www.m8cool.com/article/view-113-18793.aspx)
[9] HTC Touch Diamond2 T5353 Spec. (http://product.pcpop.com/000153932/Detail.html)
[10] MTK6516, HI3611, PXA310 智能平台对比。(http://www.mobileuncle.com/thread-16086-1-1.html)
[11] Qualcomm MSM7200 architecture. (http://mobile.onegreen.org/Article/HTML/15203.html)
[12] Morgan Stanley's Mobile Internet Report, 12/2009.

(http://www.morganstanley.com/institutional/techresearch/mobile_internet_report122009.html)
[13] iPhome 3G with MTK chip.
(http://chinese.engadget.com/2009/06/22/mtk-iphome-3g-fake-os/)
[14] Fake Touch Diamond2 T5353 with MTK chip.
(http://tech.163.com/mobile/10/0409/06/63QDR5P500112K8F.html)

【15】 结束语

去年 11 月，与人讨论山寨版 Android 智能手机的前景，最初觉得这个问题很容易回答。但是三言两语之后，不仅听者茫然，而且言者自己也意识到条理紊乱，说服力不强。于是决定写几篇文章，把这个问题展开说说。所谓展开说说，当时预计也不过是三五篇的规模。

没曾想， 刚刚写到第 2 章的时候，就引来不少争议和批评。考虑再三，觉得蜻蜓点水般的浅尝辄止，难以把问题说透。于是改弦更张，从头梳理传统功能手机的软硬件系统， 以此为基础，分析当今智能手机的软硬件系统。

写到第 7 章，关于 MTK 功能手机的软件系统的时候，不可避免地涉及到 2G 网络结构。在与网友的讨论中，谈到开源基站项目（OpenBTS）。这个话题很有意思，值得花点笔墨多说几句，同时为了避免影响山寨手机系列文章的主轴，于是另开一个系列， 专门讨论 OpenBTS。

当时的计划是这样的，把 OpenBTS 作为一个引子，引出 Cognitive Radio 这一前沿技术，进而切入真正的主题，三网融合（Triple Play）和 MBMS（Multimedia Broadcast Multicast Service）。但是这个系列写到第 2 章的时候，觉得两条作战，负担之重难以承受。于是踩了一个急刹车，连虎头蛇尾这种形式上的善始善终也顾不上了。

后来写到第 11 章和第 12 章关于 3G 网络的时候，遇到这样一个问题：对于互联网而言，有 Akamai 这样的内容分发网络（Content Delivery Network），对于移动互联网，内容分发网络也势在必行。。但是，移动互联网的 Akamai 在哪里？这个问题也十分有趣，展开说说十分必要。但是挖坑容易填坑难，前车之鉴后事之师，所以决定坚持集中精力，避开分枝话题。

完成了第 13 章，关于智能手机的 OS 的初步讨论以后，本来打算横向比较 WinMobile, iPhoneOS, Android, Palm WebOS 等等时下流行的智能手机操作系统。但是智能手机的操作系统的设计，已经不再是一个纯粹的技术问题，而是涉及到手机研发制造产业链的分工协作，以 及各个厂商的竞争战略。产业链，竞争战略，这又是一个值得仔细探讨的话题。

无论好坏，作为技术分析，这个系列写到第 14 章，基本可以告一 段落。

移动互联网，作为一个新鲜事物，存在很多商业和技术上的问题，在我们看来，任何难题，都是机会，机会在于是否能够找到行之有效的解决方案。下一个系列，我们就顺着这个思路，对移动互联网做一番粗浅的经济分析。

Sunny & Kan
April 20，2010