硬件接口开发系列

THE UNDOCUMENTED PC

A Programmer ' s Guide to I/O,CPUs,and Fixed Memory Areas

PC 技术内幕

I/O、CPU和固定内存区程序员指南

【美】Frank van Gilluwe 著

精英科技 译

ADDISON-WESLEY

中国电力出版社

www.infopower.com.cn

硬件接口开发系列

THE UNDOCUMENTED PC

A Programmer's Guide to I/O,CPUs,and Fixed Memory Areas

PC 技术内幕

I/O、CPU 和固定内存区程序员指南

【美】Frank van Gilluwe 著

精英科技 译

中国电力出版社

内 容 提 要

本书共有 18 章和两个附录，系统而详尽地讲述了有关 PC 机的 I/O、CPU 和固定内存区等硬件的知识和许多未公开发表的鲜为人知的内部技术和相关资料，并提供了大量的源代码。该书原著出版后大受欢迎，被广大读者认定为“是有关 PC 机硬件的详尽的终极资源”、“PC 硬件发烧友的利器”、“硬件核心技术的宝库”，还被 PC 杂志评论为“是系统级程序员的圣经”。

本书对于从事 PC 机硬件和软件设计的技术人员有极重要的参考价值，也可供关心 PC 技术的爱好者们参考。

图书在版编目（CIP）数据

PC 技术内幕/（美）奇鲁威著；精英科技译.-北京：中国电力出版社，2000

ISBN 7-5083-0503-5

Ⅰ.P… Ⅱ.①奇…②精… Ⅲ.个人计算机-基本知识 Ⅳ.TP368.3

中国版本图书馆 CIP 数据核字（2000）第 86338 号

著作权合同登记号 图字：01-2000-1695

中国电力出版社出版、发行

（北京三里河路 6 号 100044 http://www.infopower.com.cn）

实验小学印刷厂印刷

各地新华书店经售

*

2001 年 4 月第一版 2001 年 4 月北京第一次印刷

787 毫米×1092 毫米 16 开本 65 印张 1486 千字

定价 **99.00** 元

前　言

第二版《PC 技术内幕》在对第一版作了较大修改的基础上，提供了广泛而全新的资料。我仍然对过去两年来的变化感到惊讶:MCA 系统被无情的淘汰了,与 PC 发展的最初 10 年相比，出现了更多的新型处理器和更多的新型操作系统。

本书有什么新内容?

本书第二版对每一章都作了修改。某些章只是简单地作了些更新，例如加入了一些最新的 Windows95 键盘键。另外一些章节,比如硬盘系统这一章,看起来就像每页都作了修改。我还加入了大量的资料来处理某些新型的 CPU,这些 CPU 在第一版中尚未涉及。其中包括 Intel 的 Pentium Pro 和 MMX 系列，AMD 的 5x86、Cyrix5x86 和 6x86，以及那些过时了的 NexGen CPU。

我还对许多在第一版中出现的程序加以改进和更新。跟第一版一样，我们公开了全部的源代码（感兴趣的读者可以访问 www.infopower.com.cn——编者注）。这些新特征包括：检测 PCI 及其相关信息、BIOS 供应商和日期、以及一个详细显示和描述 BIOS 数据的工具。键盘视图程序也作了修改，以适应更多的工作环境和用任意键来显示未译扫描码和译毕扫描码。

CPU 检测程序将检测是否带有 MMX，并标识真正的指令集(这些指令集通常和你所想象的并不一样)。我还进一步详细地查阅了许多与 CPU 供应商相关的资料，以获取 CPU 速度及其内部信息。型号专用寄存器程序按名词顺序描述了许多尚未公布的寄存器，并且实现了对隐藏寄存器的快速访问。

为什么将这本书取名为《PC 技术内幕》?

如果你是第一次阅读此书，可能会被书名〈〈PC 技术内幕〉〉所吸引。但是我希望你和我一样对此持有怀疑的态度，因为过去有许多技术书籍给人以很大的希望，但实际上仅仅只是一个老调重弹的作品，比如一张和以前相同的老式表，谈论一些关于中断、OS 命令，ASCII 码表等的信息。但是你不会对这本书感到失望的。

你会发现,这本书与现在的其他书籍很少有相同之处。在一些相关的问题上,我加入许多信息和代码例,而不是仅仅作一些比较深入的阐释。

那么,这本书到底有什么地方吸引人呢？我并非无所不知，在本书所涉及的内容之外还有许多 PC 尚未说明的领域。我仅仅只是关注那些非常有用的领域，这些领域以前尚未说明或者阐明得不够，但是对目前许多开发项目非常有用。

在每一个新系统的设计当中，生产商的目的似乎是要将它做成一个最不可靠的平台，这个平台可能存在于一个复杂软件的区域内。我为何说出如此难以置信的话？因为这些制造商及其协会所提供的说明文档是令人难以置信的。对于早期的 PC 机，至少你可以获得完整的原理图和 BIOS 列表，当说明文档缺乏关键的信息时，你却可能会用到这些信息。但是即使如此，如果你对读懂原理图和关键的汇编代码感到困难，你可能很难用好这些信息。

今天，说明文档提供的信息少得可怜。显然，准备这些文档时他们很少考虑到软件和固件开发人员的实际需要。这些粗劣的文档的价格也变得越来越昂贵，简直令人望而却步。例如，如果你对支持基于 EISA 和 MCA 总线的机器感兴趣，那么你就不得不花几百美元来购买有关 EISA 和 MAC 的说明书。这也是为什么这些开发平台很少成功的一个原因。即使你对整个技术工作比较熟悉，你还是会发现许多地方不够精确、信息缺损，或者很多地方标有“保留”而隐藏了相关信息。

我努力保证本书高度精确。为了做到这一点，我开发了一些工作程序来检验这本书中的有关信息。另外，我还花了大量的时间来确认最低层的信息，包括仔细检查原理图、隐藏的 BIOS 列表和 IC 源清单。

或许你刚刚才开始理解本书所讨论的问题，但是你仍然马上可以使用这些信息。除此之外，我还汇集了一些信息，涉及那些过时的和现行的系统标准，包括 PC、XT、AT、ISA、MCA、EISA 和 PCI 系统。其中许多过时的系统，如 MCA 机，现在仍然在使用，并且不费多大劲就可以轻易地获得支持。

通过操作系统或者一些详细说明的标准功能，通常可以高效地处理软件任务，适宜的时候使用接口不失为明智之举。当这些接口没有提供任务所需要的属性和工作时，有必要深入底层，充分发挥那些制造商特意隐藏起来的系统潜在功能。

现在，我给那些制造商们一些喘息的机会，他们创造了一台多功能的机器，出于竞争的考虑，他们隐藏了一些信息是可以理解的。同时从一个实用的软件视角来解释操作也不是一件容易的事情。如果某些功能设计没有加以说明，那么更新它们就显得容易些，因为这样的话，理论上没有人会使用他们。今天的市场要求开放的界面，大多数供应商声称他们的系统是透明的，但是不要期望能够从他们那里获得非常有用而廉价的信息。

本书的结论会令你感到满意的，对于这一点我充满了信心。我知道每天有许多新的设计推向市场，这些设计都有相应的说明文档。但是我相信，这本书的确为程序员们提供了详尽的信息，而这些信息被长久的忽略了。

Frank van Gilluwe (74000.635@Compusurve.com)

目　录

第1章

简　介

内幕信息可能会非常有趣并激起读者的兴趣，但是我只会关注那些软件和硬件开发人员初次接触的 PC 领域。可能你想知道，有关 PC 的技术书籍何止成百上千，还会留下什么内幕！不错，在过去的几十年中，似乎有数不尽的重要领域都涉及到了 PC，但是它们往往未加说明或者阐明得很不够。许多重要的区域，例如系统 BIOS 和输入/输出端口，就很少被详细阐述，所以人们常常难以真正理解和使用系统这些重要的领域。

特别值得指出的是，输入/输出端口往往是系统环境中阐述得最不清楚的地方。我尽力阐明每一个端口及其定义位，这一点与那些提及 I/O 的用户手册的单线描述有很大不同。在许多情况下，我还提供了关于其用法的例子和可能出现的问题。

在为新的硬件选择端口位置时，这本参考书对开发人员的作用是无法估量的，有一整章专门从软件的视角讨论了一些与适配卡有关的问题。

你可能会问，这本《PC 技术内幕》完整吗？我曾经编写了一个流行的反汇编程序，Sourcer,在它的帮助下，过去的十年中我一直在收集有用的资料，以便充实我所写的这本内幕书籍。作为一个反汇编器，Sourcer 将一些可执行文件和 BIOS ROM 转化成可读的汇编代码，并对中断、I/O 端口等做出注释。为了保证 Sourcer 能够跟上时代，我仔细检查了说明文档和列表，并深入理解了 BIOS 功能和 I/O 端口的使用方法及原理。

综上所述，本书对于系统的每个功能块都有一章专门论述。每章都从最底层解释了每个 BIOS 功能，并对相关 I/O 端作出了详细的阐述。许多章节还提供了一些有趣的程序，来说明如何访问这些功能。这些程序包含有完整的源代码，因此将它们改成你自己的程序语言并不难。

最有趣的论述还包括如何开发第 2 章所论述的技术内幕。第 3 章讲述了大量尚未说明的指令。第 5、6、7 章阐释了适配卡的开发、BIOS 数据区以及中断向量表。剩下的章节则对每一个子系统作出详细说明。

资料的来源

在我开始写这本书时，我知道现在有大量的信息要么论述得不够充分，要么就是缺损的，或者根本就从未阐释过。为了获得本书的相关资料，我做了大量非同寻常、细致深入的工作。大多数情况下，我首先回顾了一下制造商为子系统提供的 IC 数据源清单，然后仔细察看这些芯片在标准的主板上是如何具体连接的。做到这一点需要用到系统的原理图，在某些情况下，还要查看系统的电路图。我也仔细研究了不同制造商提供的反汇编 BIOS 代码，以便在这些较低的层次上考察它们与了系统的联系。我还生成了一些测试程序来检验某些子系统的操作。最后，我才去看那些“正式”的文档，包括 IBM 的技术参考资料，当然它也是许多其他技术书籍的资料来源。

IBM 的技术参考资料对可靠的底层信息来说，是一个差劲的资料来源，对于这一点我并不感到惊讶。显然，IBM 的说明文档直接源于各种 IC 数据清单中的程序注解。令我感到吃惊的是，在实际应用中这些信息常常要么是错误的，要么就容易引起误解。例如，在硬件具体执行时，某些芯片的性能根本不可能得到发挥，然而某些说明文档却对此加以详细地阐述，似乎有人真的实际应用过它们。在许多情况下，对功能的解释过于简单，对程序员毫无用处。

当然，我并不是说，IBM 的技术参考资料一点用处也没有。其实，他们也提供了许多有用的信息。当然，这带来了你一定会遇到的第二个问题。这些说明文档对开发各种系统很有必要，例如开发 PC、XT、AT、ISA、MCA、EISA，许多说明文档都谈到了 PCI 系统。为了易于掌握，我列出了每个 BIOS 功能和端口描述的差别。这些正是程序员所需要的。

许多技术参考资料喜欢用“保留”一词，来避免谈及一些具体细节，然而，“保留”的真正含义并不太清楚。我认为，供应商指的是下面所列的某个意思：

- 现在未用到，但是将来可能用到
- 现在未使用，也可能从未使用过
- 在一些功能中用到，但 PC 结构不支持这个功能
- 在一些隐藏的功能中用到
- 在某些功能中用到，但这些功能会产生意想不到的效果
- 在老式的 PC 中用到，但现在过时了
- 供应商也不知道它的用处。

本书中我尽量不使用“保留”一词。但是坦白的说，我也不能讲清楚某些保留功能有什么用处。大多数情况下，你可以认为，在我的分析中“保留”指的就是“未使用”。

系统类型

在本书的许多地方，我特别列出一些机器类型的缩写形式，如 AT，EISA 等等。它们代表了一个特定的系统家族系列，这些系列的硬件设计相同、BIOS 功能类似。一个加号（+）表明该家族系列以及其后的家族系列都支持该特定的功能和 I/O 端口。例如：AT+表示所有的 AT 机器都支持该功能，同时，EISA、PCE 和过时了的 MCA 机器也都支持。

类 型	描 述
PC	早期的基于 8088 的计算机。
XT	早期的基于 8088 的计算机，带有硬盘，但没有内置的 CMOS 时钟和 CMOS 配置内存。
AT	基于 80286、386、486 以及一些 Pentium+ CPU 的系统，工业标准结构（ISA）总线。
MCA	基于 80286、386、486 以及一些 Pentium+ CPU 的系统，带有微通道结构（MCA）总线。所有的 IBM PS/2 50 型以及更高级的机器都使用 MCA 总线。
EISA	基于 386、486 和 Pentium+ CPU 的系统，带有扩展工业标准结构（EISA）总线。
PCI	基于 486、Pentium 以及 PentiumPro CPU 的系统，带有外围部件互联（PCI）总线。

程序员的系统框图

尽管你可能对基本系统有深入的理解，但是我认为从编程的角度来考虑系统而不去考虑实际的处理器和总线设计仍是非常有用的。虽然许多程序设计依赖于 CPU 和总线结构，但是仍然有许多编程系统并不依赖于这些独特之处。许多硬件性能，例如总线宽度、高速缓存内存、局部总线，与编程一点关系也没有，也没有编程接口。

图 1-1 被我称为程序员的系统框图，它列出了系统的所有硬件块，并指出了彼此之间的连接关系，同时还标出了这个硬件块在系统内的中断和 I/O 端口。每个方框中还指出了对这个子系统作出深入阐述的章节。

记住，不同的供应商和平台提供的硬件的连接方法有所不同，但是功能性的软件总是相同的。任意编程上的差别都在子系统所用到的中断和端口中加以了注明。如果一个供应商偏离了基本标准，那么众多的软件就不能在该机器上正常运行。早期，由于供应商偏离了基本标准，从而阻碍了兼容 PC 的发展。那些遵守基本标准，并且真正兼容的机器的供应商今天依然存在，而其他的已成为历史。

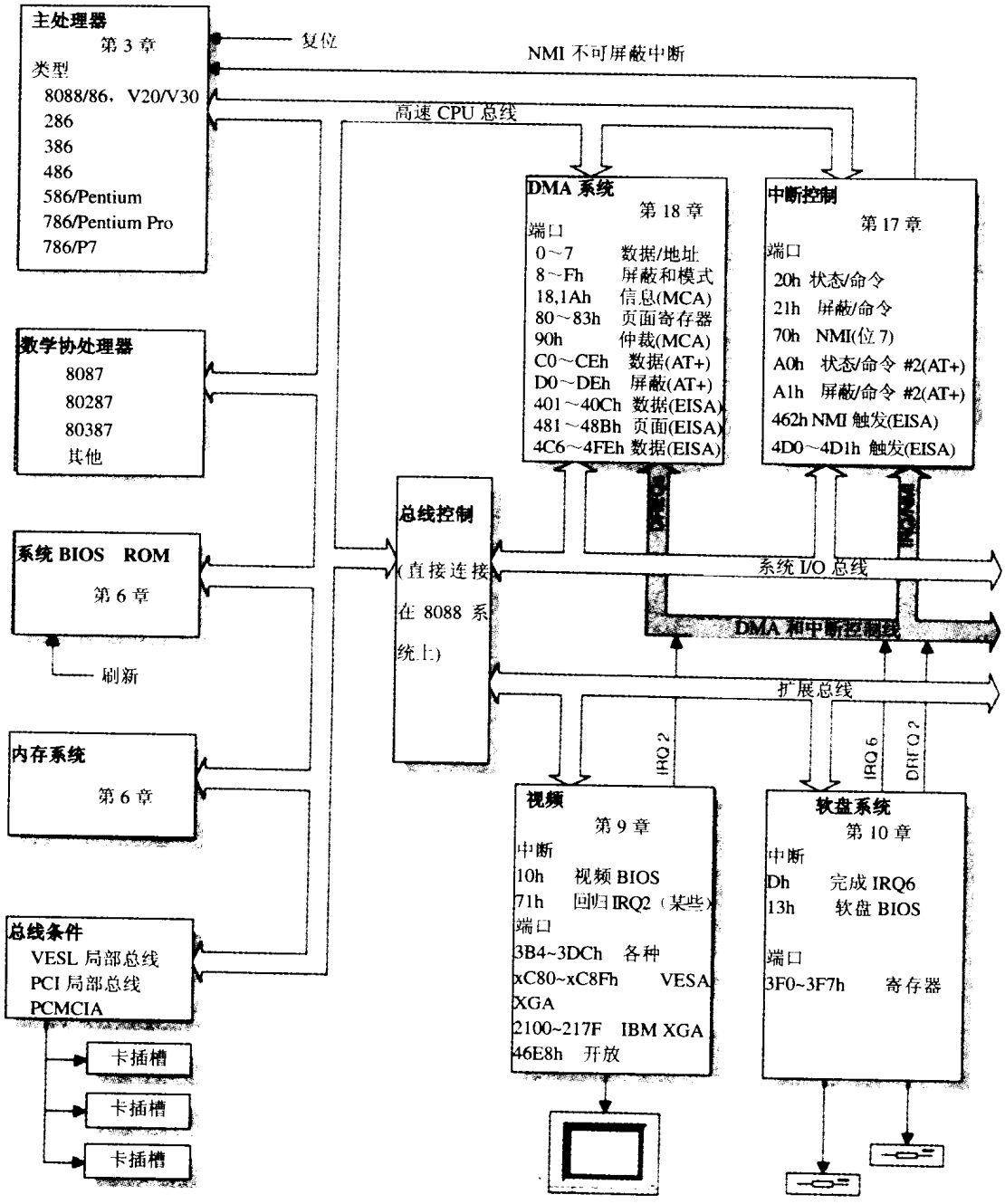
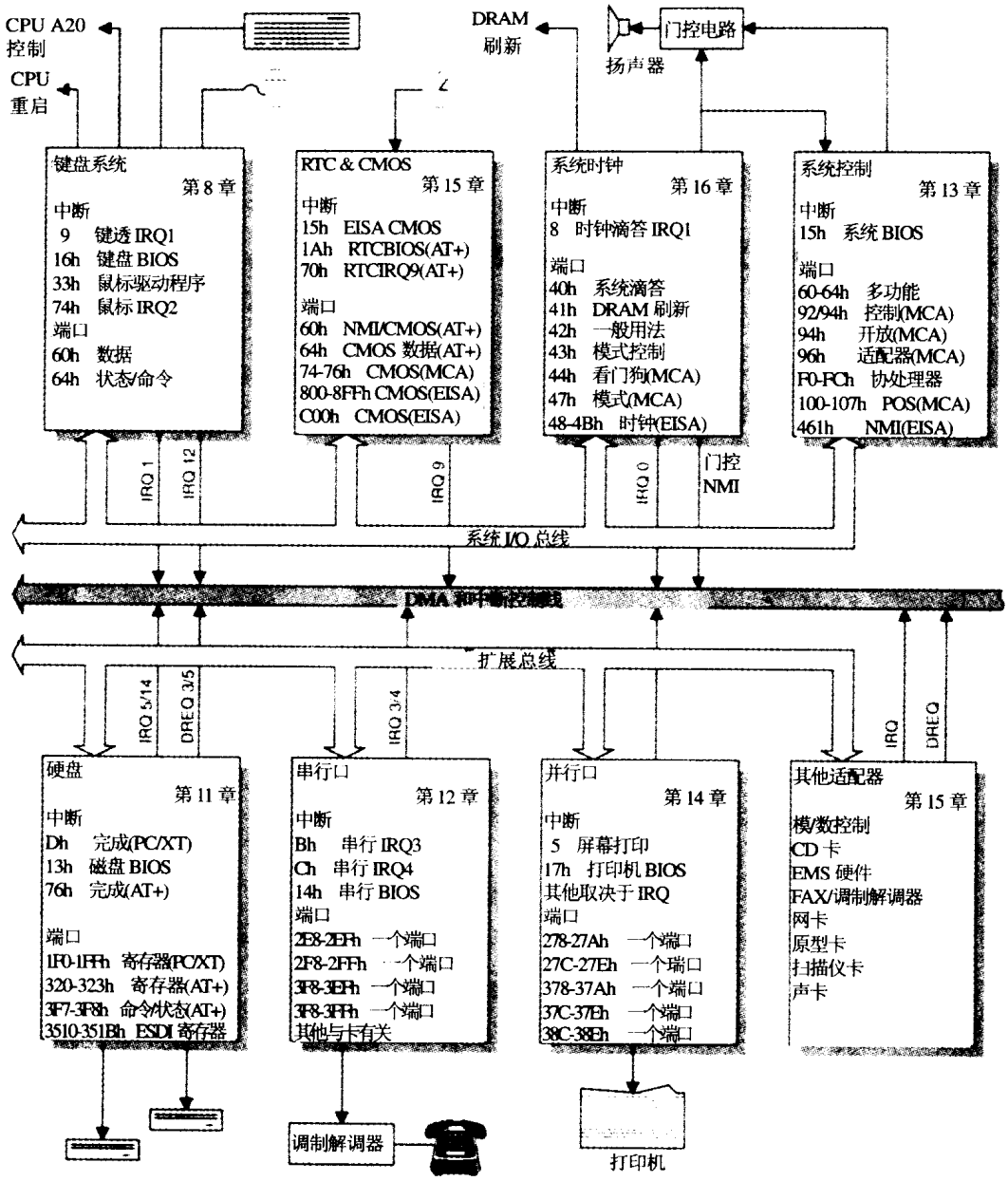


图 1-1 程序员的系统框图


CPU A20
控制
CPU
重启
DRAM
刷新
门控电路
扬声器
键盘系统
第 8 章
中断
9 键透 IRQ1
16h 键盘 BIOS
33h 鼠标驱动程序
74h 鼠标 IRQ2
端口
60h 数据
64h 状态/命令
RTC & CMOS
第 15 章
中断
15h EISA CMOS
1Ah RTCBIOS(AT+)
70h RTCIRQ9(AT+)
端口
60h NMI/CMOS(AT+)
64h CMOS 数据(AT+)
74-76h CMOS(MCA)
800-8FFh CMOS(EISA)
C00h CMOS(EISA)
系统时钟
第 16 章
中断
8 时钟滴答 IRQ1
端口
40h 系统滴答
41h DRAM 刷新
42h 一般用法
43h 模式控制
44h 看门狗(MCA)
47h 模式(MCA)
48-4Bh 时钟(EISA)
系统控制
第 13 章
中断
15h 系统 BIOS
端口
60-64h 多功能
92/94h 控制(MCA)
94h 开放(MCA)
96h 适配器(MCA)
F0-FCh 协处理器
100-107h POS(MCA)
461h NMI(EISA)
IRQ 1
IRQ 12
IRQ 9
IRQ 0
门控
NMI
系统 I/O 总线
DMA 和中断控制线
扩展总线
IRQ 5/14
DREQ 3/5
IRQ 3/4
IRQ
DREQ
硬盘
第 11 章
中断
Dh 完成(PC/XT)
13h 磁盘 BIOS
76h 完成(AT+)
端口
1F0-1FFh 寄存器(PC/XT)
320-323h 寄存器(AT+)
3F7-3F8h 命令/状态(AT+)
3510-351Bh ESDI 寄存器
串行口
第 12 章
中断
Bh 串行 IRQ3
Ch 串行 IRQ4
14h 串行 BIOS
端口
2E8-2EFh 一个端口
2F8-2FFh 一个端口
3E8-3EFh 一个端口
3F8-3FFh 一个端口
其他与卡有关
并行口
第 14 章
中断
5 屏幕打印
17h 打印机 BIOS
其他取决于 IRQ
端口
278-27Ah 一个端口
27C-27Eh 一个端口
378-37Ah 一个端口
37C-37Eh 一个端口
3BC-3BEh 一个端口
其他适配器
第 15 章
模/数控制
CD 卡
EMS 硬件
FAX/调制解调器
网卡
原型卡
扫描仪卡
声卡
调制解调器
打印机

第2章

开发PC内幕

简　介

生产商总是对许多新的 PC 领域未加说明，当然，这并一定是故意的，但是相对于迅速发布的系统适配器或软件而言，有关的文档总是相对落后。特别是当要从底层实现设备功能而需要这些文档时更是如此。即使提供了相关文档，对专业化软件来说也常常是毫无用处的。

通过我在这里阐述的一些例子，你可以拨开制造商提供文档的面纱，加深对关键接口、操作和数据区的理解。我也会告诉你如何避免落入充满了误解的陷井和使用一些并不精确的文档信息。

要诀#1：找到最初的源文档

针对你所感兴趣的子系统请选择那些最初的源文档作参考，其中包括原理图、IC 使用说明清单、IC 应用注释以及 IC 程序员参考手册。如果手头有这些文档，并且你对硬件和软件有所了解，那么你就能透彻地理解大多数子系统的本质。记住，每台 PC 中都使用了许多复杂的 IC。在许多情况下，它们拥有一些特性和功能，然而这些特性和功能在 PC 设计中却是不可能实现的。例如，8254 可编程时钟 IC 虽有许多模块供每个计数器编程使用，但却因为时钟 IC 与 PC 硬件连接方式，许多模式不可能实现或者没有任何意义。彻底理解 IC，同时仔细查看具体的原理图，将有助于消除这些限制。当然我已经为 PC 子系统完成了这项工作，然而你仍然可以仔细研究一些新型的设计和适配卡。

通常，许多技术参考资料只是从一本 IC 用户手册中取出一些资料而并不考虑其实际应用效果。经常会出现这种情况：许多技术手册中列出的功能和模式在 IC 手册中也有，然而对任意一个 PC 的设计并不适用。

不幸的是，在将这些技术应用到子系统时存在着许多问题。很少有制造商提供其内部的原理图。IBM 最近一次在《技术参考资料—AT 个人计算机》中公布原理图是在 1985 年。即使在这本参考资料中，IBM 也删去了大量的信息，并且使用了许多难解的术语，使这本书越发难以理解。许多程序员发现一个普通的原理框图都很难理解，更不用说那些重要信