

# 嵌入式系统

## An Introduction to Embedded System

### 第十一课 虚拟机系统概述

教师：蔡铭

cm@zju.edu.cn

浙江大学计算机学院人工智能研究所  
航天科技—浙江大学基础软件研发中心

# 课程大纲

 虚拟机系统发展历程

 虚拟机系统技术分类

 系统级虚拟机Bochs简介

# 什么是虚拟机—老兵新传

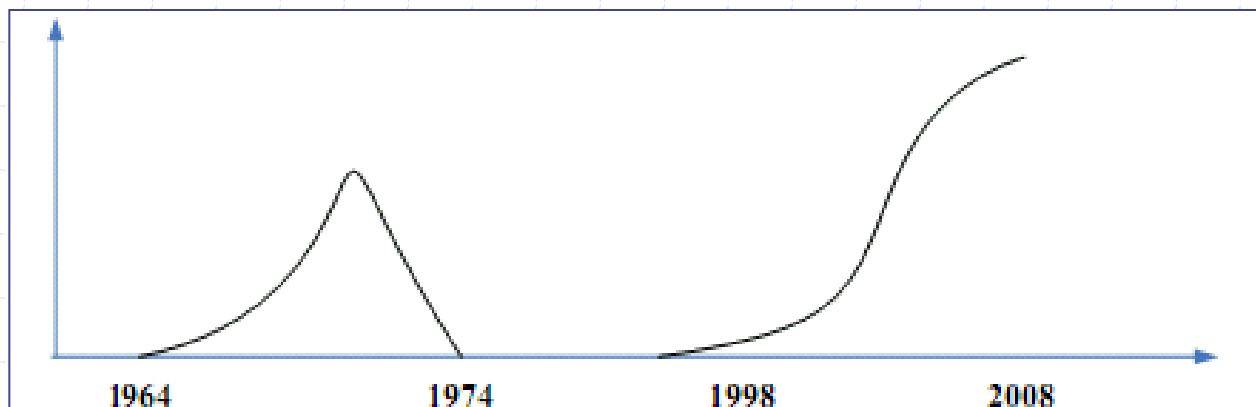
- ❑ 虚拟机：顾名思义，就是虚拟出来的计算机，这个虚拟出来的计算机，和真实的电脑几乎完全一样，拥有计算资源、内存资源、外设资源等。
- ❑ 虚拟机：提供对真实机器的软、硬件复制，并可以执行主机指令，完成将虚拟的客户映射到真实的机器中。

——Goldberg (Harvard & Honeywell, 1974)

(原文: A system...which...is a hardware-software duplicate of a real existing machine, in which a non-trivial subset of the virtual machine's instructions execute directly on the host machine. )

# 虚拟机系统的发展历程

- ❑ 虚拟机系统出现于20世纪60年代，40多年经历了一波三折，近年来，随着IT技术的发展，虚拟化技术、虚拟机系统得到蓬勃发展，市场迅猛扩大。



## ❑ 虚拟机系统发展的三个阶段

- 虚拟机系统的出现和兴起 (1965—1975)
- 虚拟机系统走向边缘化 (1976—1996)
- 虚拟机系统复兴，研发、应用纵深化发展 (1996—至今)

# 虚拟机系统的出现和兴起 (1/2)

## □ 计算机科学发展的一个思想

计算机科学中的任何问题，都可以通过增加一个中间层来解决。

(原文: Any problem in computer science can be solved with another layer of indirection.)

——David Wheeler (Cambridge)

David Wheeler (PhD. 1951)



## □ 一部计算机的历史可看做计算机技术不断虚拟化的历史。

——李国杰院士（对计算机科学的反思）

□ 计算机系统发展：虚拟地址——虚拟机器——虚拟组织

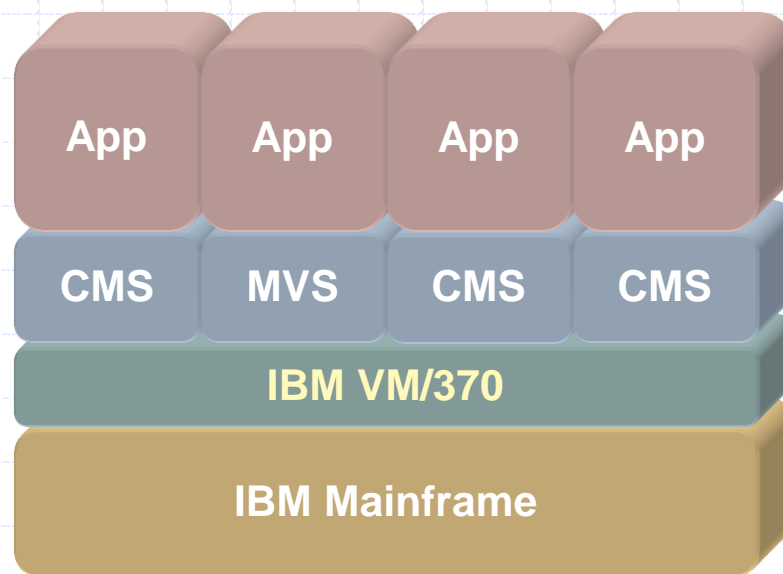
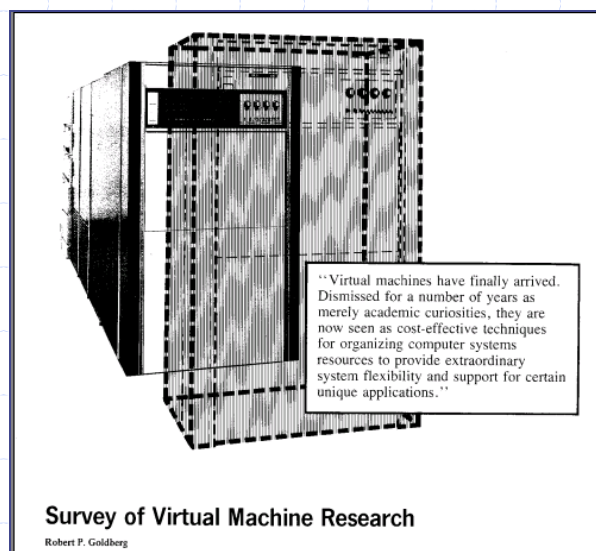
□ 计算机语言发展：机器语言——汇编语言——高级语言

### 计算机的历史是不断“虚拟化”的历史

- 一部计算机的历史可看做计算机技术不断虚拟化的历史。
- 上世纪70年代IBM 370首先使用虚拟计算机概念。
- 虚拟地址——虚拟计算机——虚拟组织 (VO)
- In his 1992 Turing Award lecture Butler Lampson: “any problem in computer science can be solved with another layer of indirection.”

# 虚拟机系统的出现和兴起（2/2）

- 60年代末期兴起虚拟机技术，随着IBM的商用IBM370主机系列的成功应用，在70年代初期达到了它的第一个高峰。
- 虚拟化原理：对大型机进行逻辑分区，形成若干独立虚拟机的一种方式。这些分区允许大型机进行“多任务处理”，同时运行多个应用程序和进程。



——Goldberg R P., Survey of Virtual Machine Research,  
IEEE Computer, 1974, 7 (6): 34245

# 虚拟机系统走向边缘化

## ❑ 虚拟机系统发展受挫，是在微处理问世之后：

- 1971年11月，Intel公司推出了第一片微处理器Intel4004，并进一步通用化，推出了4位的4040、8位的8008。

人们再也不必为设计一台专用机而研制专用的电路、专用的运算器了，只需以微处理器为基础进行设计。

- 1976年，第一个单片机Intel 8048出现。
- 1982年，第一个DSP出现，比同期的CPU快10~50倍。
- 80年代后期，第三代DSP芯片出现。

## ❑ 在80~90年代，由于价格低廉的x86服务器、台式机的出现，以及客户机/服务器的应用，成就了分布式计算技术，虚拟化实际上已被人们弃用，几乎销声匿迹。



# 虚拟机系统的复兴，走向新时代（1/3）

## □ 新的发展契机：

- 研究领域：90年代，Stanford教授Mendel Rosenblum关于虚拟机SimOS的论文，解决了x86服务器虚拟化的关键技术难题。

——为VMWare的发展奠定基础

- 产业领域：随着Windows广泛使用，Linux作为服务器操作系统的出现，奠定了x86系统的行业标准地位。x86服务器和桌面部署的增长带来了新的IT基础架构运作难题：

- ◆ 基础架构利用率低。服务器部署平均利用率仅为10%~15%。
- ◆ 基础架构成本日益攀升。耗电量、制冷和设施成本不断增加。
- ◆ 管理成本不断攀升。
- ◆ 故障切换和灾难保护不足。
- ◆ 最终用户桌面的维护成本高昂。



# 虚拟机系统的复兴，走向新时代（2/3）

- 第一阶段：1997—2005，重点是x86系统的虚拟化
  - 1997: Virtual PC for Macintosh by Connectix
  - 1998: 利用Stanford的研究成果创建了VMware公司
  - 1999: VMware Virtual Platform (Workstation) for x86
  - 2001: VMware GSX Server product
  - 2003: 微软收购Connectix, EMC收购VMware
  - 采用二进制转换，实现全系统虚拟化。



VMware共同创始人 Mendel Rosenblum(Stanford)

# 虚拟机系统的复兴，走向新时代（3/3）

## □ 第二阶段：2005—至今，硬件/操作系统辅助的虚拟化

### □ 硬件辅助的虚拟化

- 2005: Intel IVT (Vanderpool/Silverdale)

- 2006: AMD AMD-V (Pacifica)

- Native Virtualization

### □ 操作系统辅助的虚拟化 (paravirtualization, 半虚拟化)

- 2002: Denali by 华盛顿大学

- 2003: Xen by XenSource by 剑桥大学

- 2005: Virtual Machine Interface by VMWare

# 课程大纲

 虚拟机系统发展历程

 虚拟机系统技术分类

 系统级虚拟机Bochs简介

# 虚拟机系统的分类—按虚拟级别划分

## 虚拟机系统分类

### 1、进程级虚拟机：提供进程运行环境

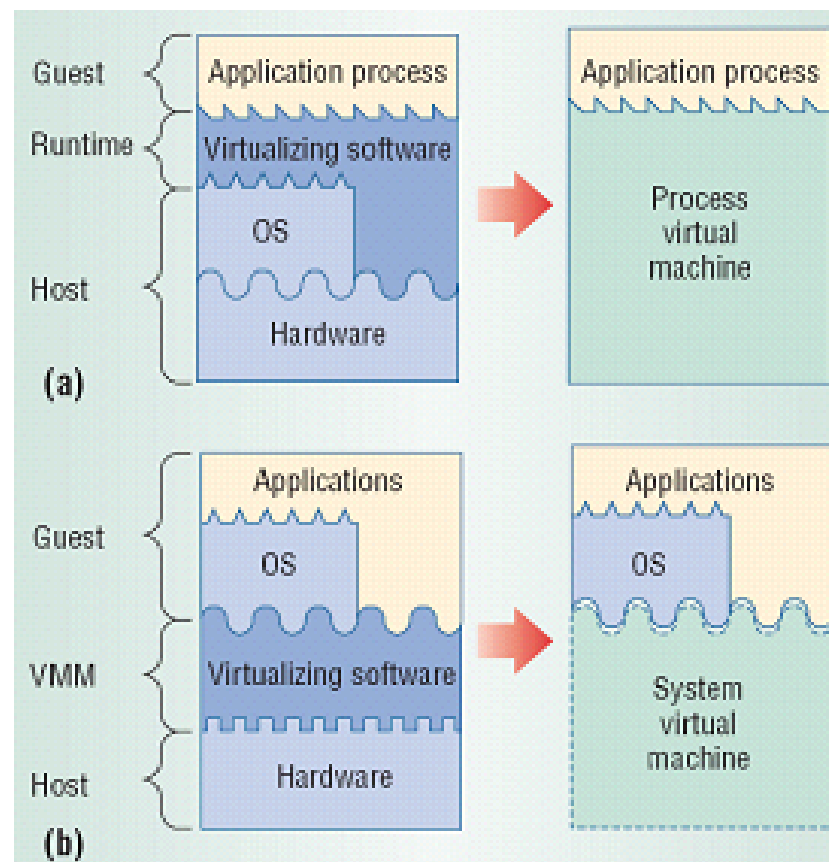
■ 同构平台

■ 异构平台

### 2、系统级虚拟机：提供系统环境

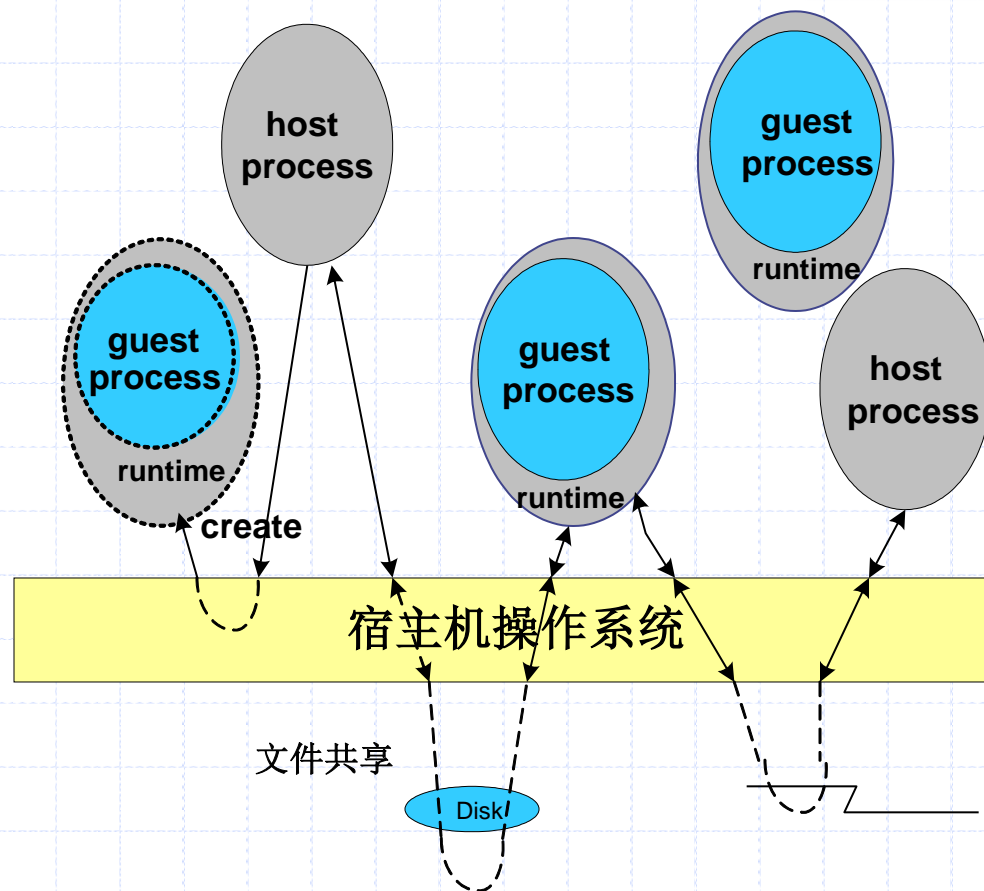
■ 同构平台

■ 异构平台



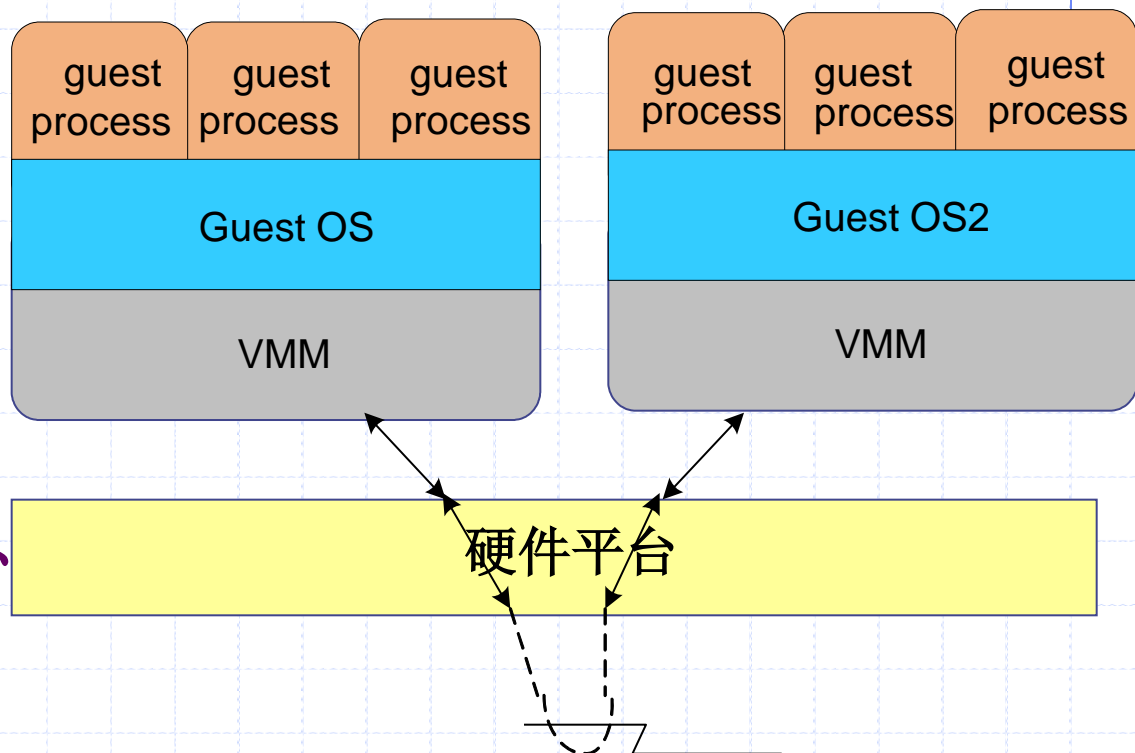
# 进程级虚拟机

- 提供应用二进制接口，ABI级别
- 运行时，系统管理客户进程
- 例子：Java虚拟机、Microsoft公共语言基础结构CLI、SQLite虚拟机

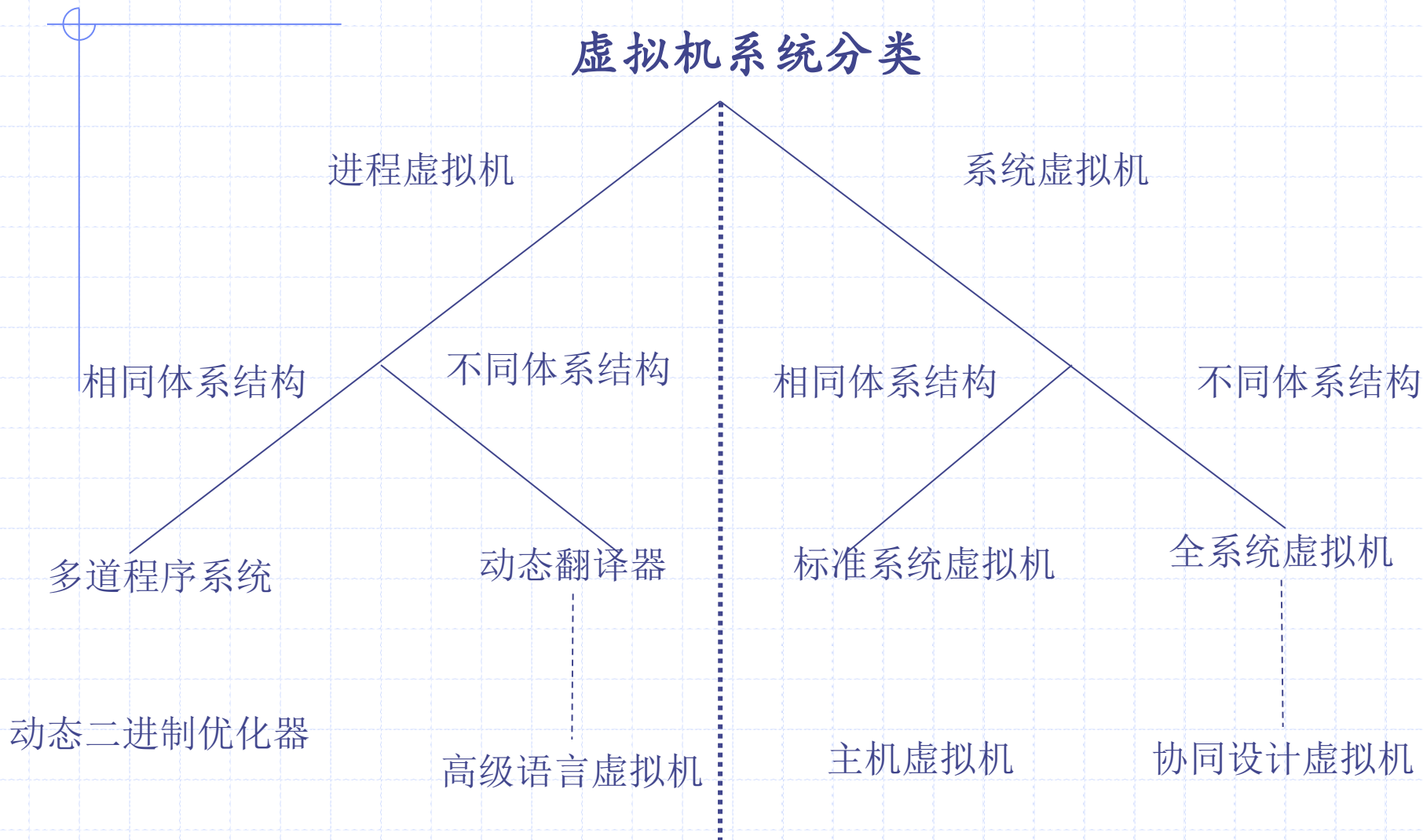


# 系统级虚拟机

- 提供指令集接口，ISA级别
- 提供系统环境，管理客户操作系统以及应用系统
- 例子：IBM VM/360，VMware，Virtual PC、Bochs、Qemu



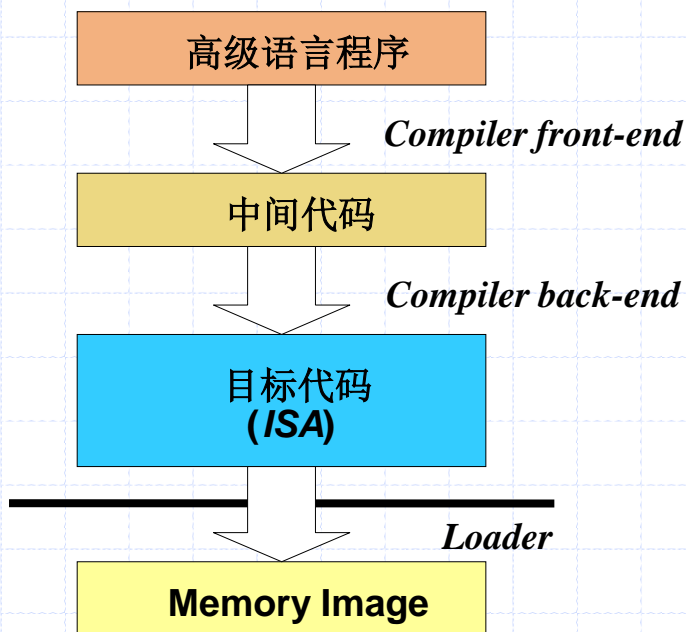
# 按虚拟级别的虚拟机系统分类



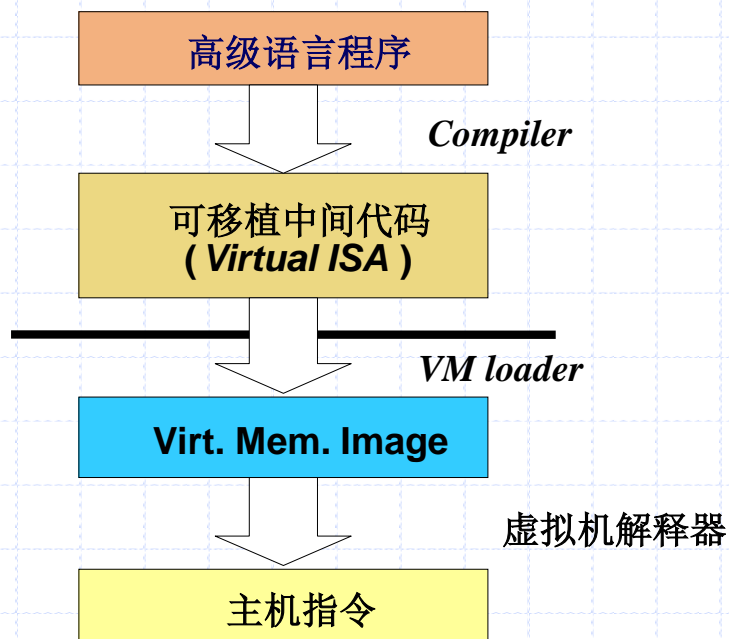


# 高级语言虚拟机 (1/4)

- 在高级语言开发级别提供支持
- 构建于应用程序接口（API）生成可移植的代码和元数据，通过虚拟机解释器运行二进制指令
- 例子：Java JVM、Microsoft CLI

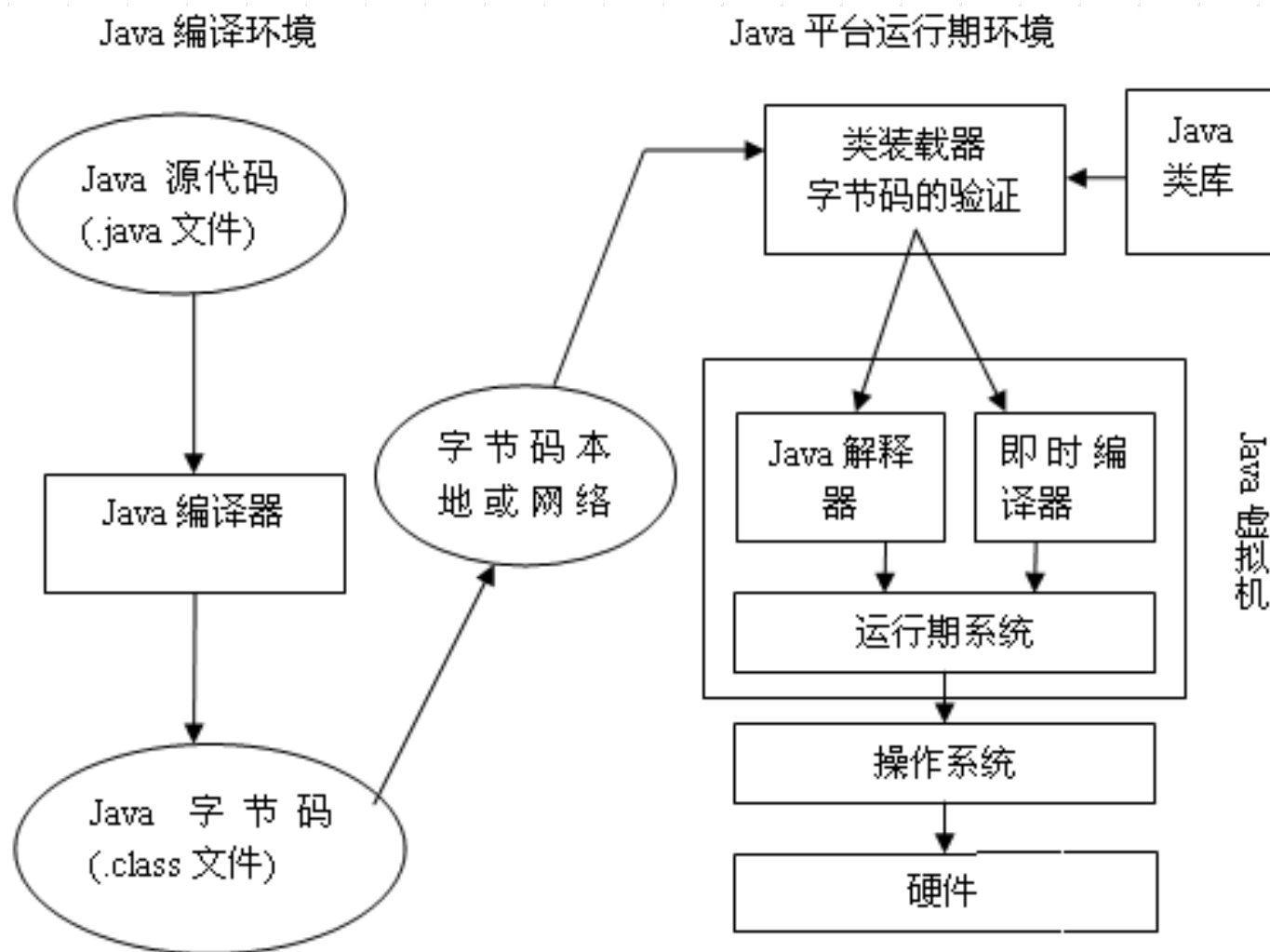


传统软件开发模式

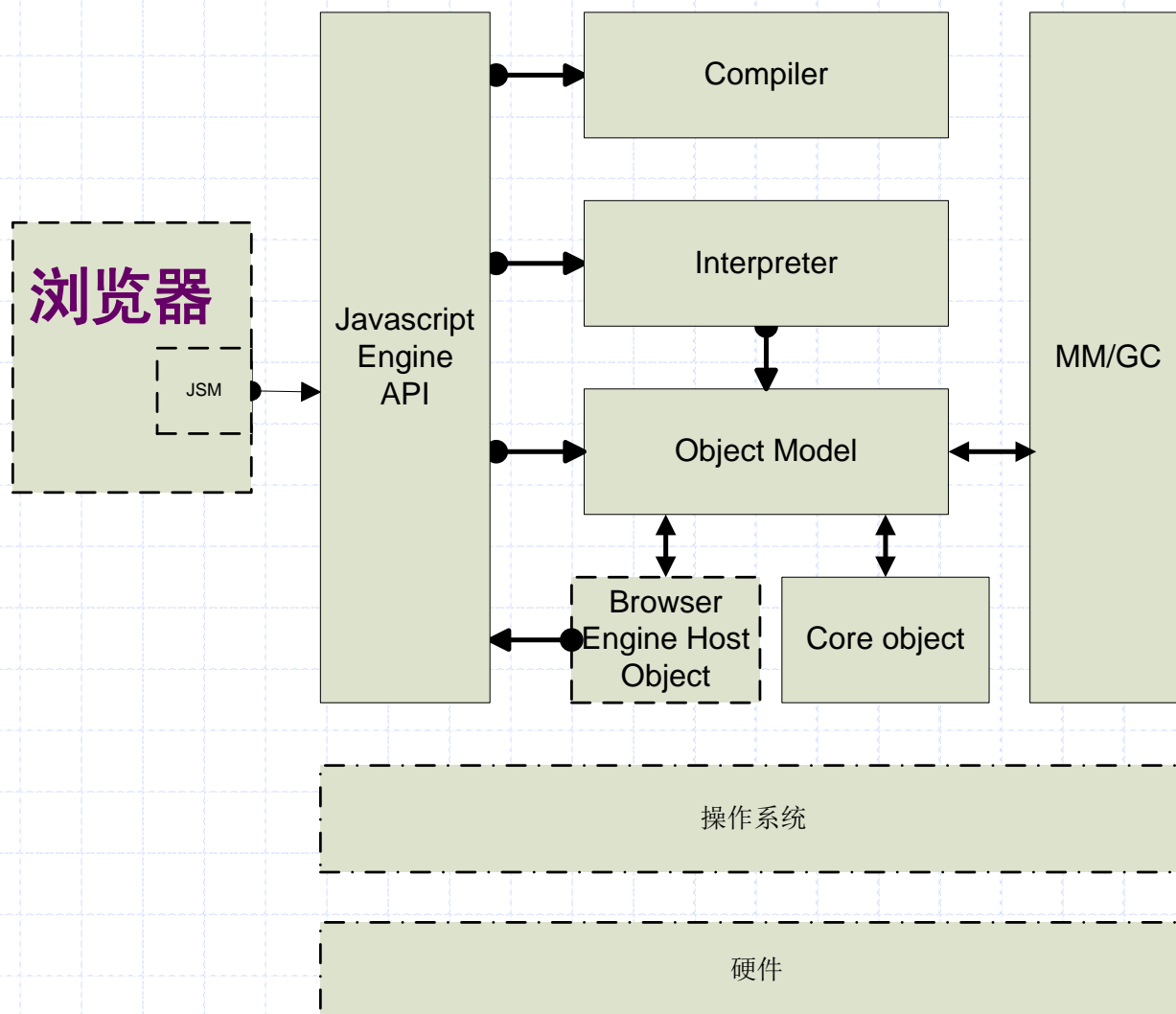


虚拟机模式

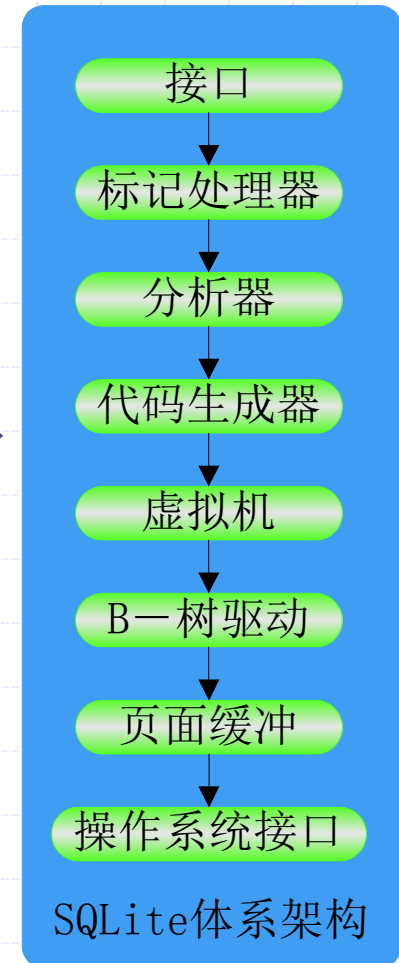
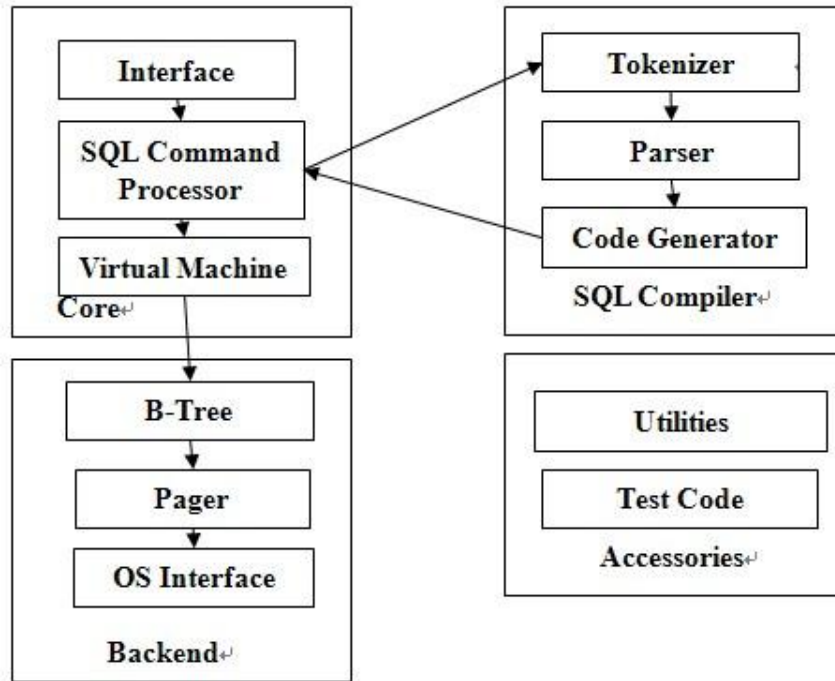
# 高级语言虚拟机—Java虚拟机（2/4）



# 高级语言虚拟机—JavaScript引擎 (3/4)

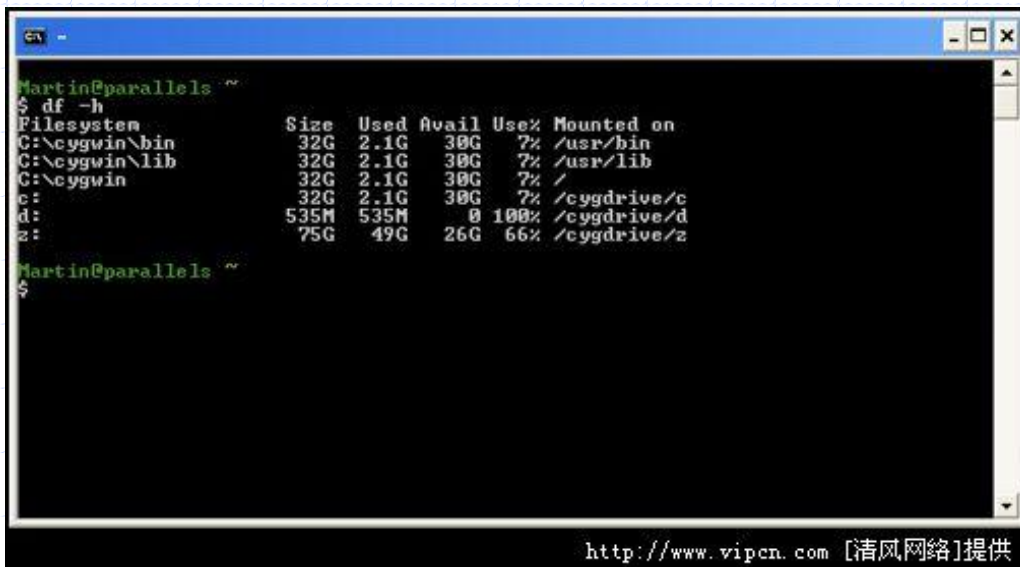


# 高级语言虚拟机—嵌入式数据库SQLite (4/4)



# 动态仿真与二进制优化

- ❑ Cygwin是cygnus solutions公司开发的自由软件，目前被Redhat公司收购。
- ❑ Cygwin是一个在windows平台上运行的unix模拟环境，提供了一个基于win32 api的unix系统库模拟层。
- ❑ Cygwin对于使用GNU工具链，在windows上进行嵌入式系统开发非常有用。

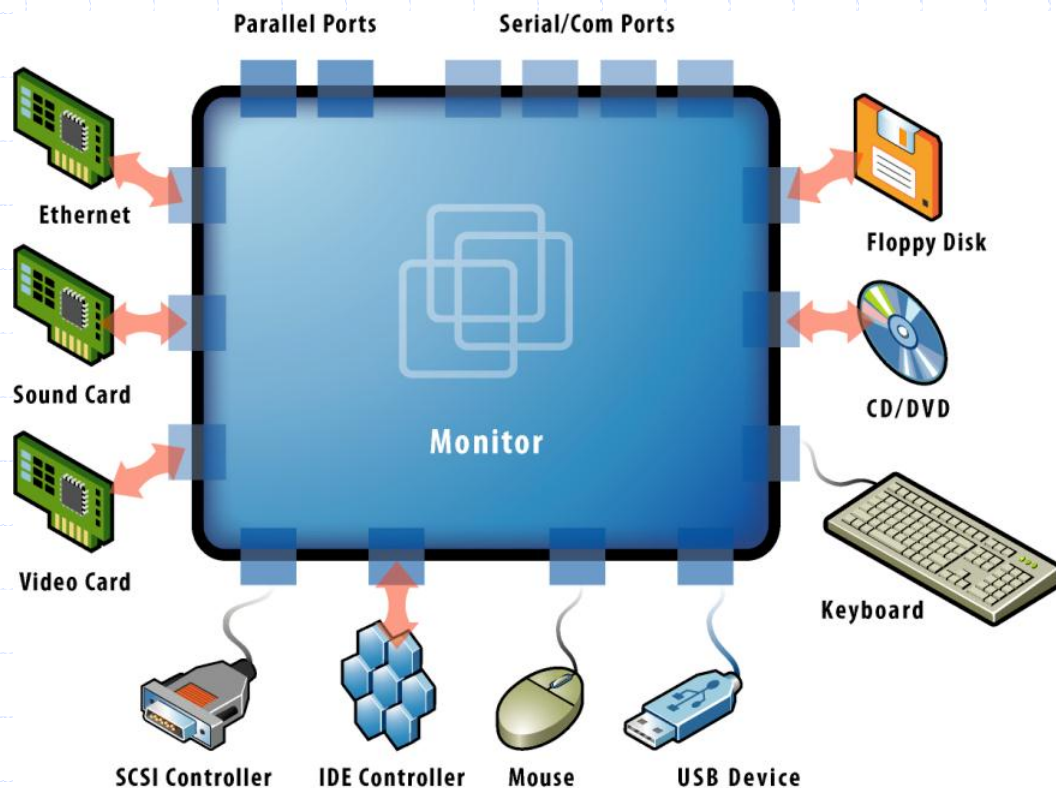


```
Martin@parallels ~  
$ df -h  
Filesystem      Size  Used Avail Use% Mounted on  
C:\cygwin\bin    32G   2.1G   30G   7% /usr/bin  
C:\cygwin\lib    32G   2.1G   30G   7% /usr/lib  
C:\cygwin        32G   2.1G   30G   7% /  
c:               32G   2.1G   30G   7% /cygdrive/c  
d:              535M  535M    0 100% /cygdrive/d  
z:              75G   49G   26G  66% /cygdrive/z  
  
Martin@parallels ~  
$
```

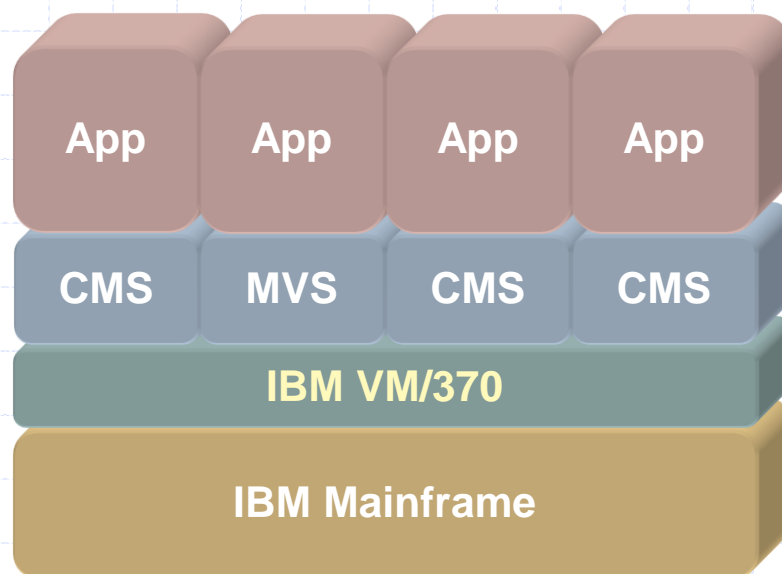
http://www.vipcn.com [清风网络]提供

# 系统级虚拟机

□基本思想：截获外设、I/O指令，进行重新定义



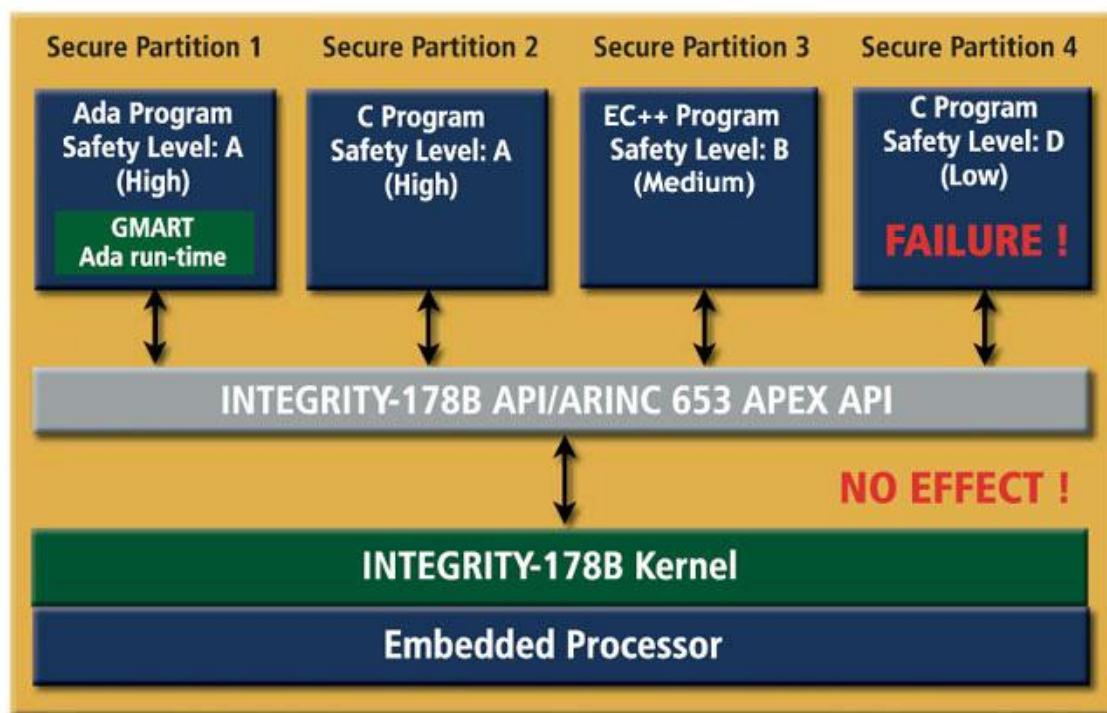
# 标准虚拟机系统—IBM 370虚拟机结构（1/2）



- 用一个虚拟机管理软件，处在操作系统和硬件之间，从而虚拟和管理所有的硬件资源。

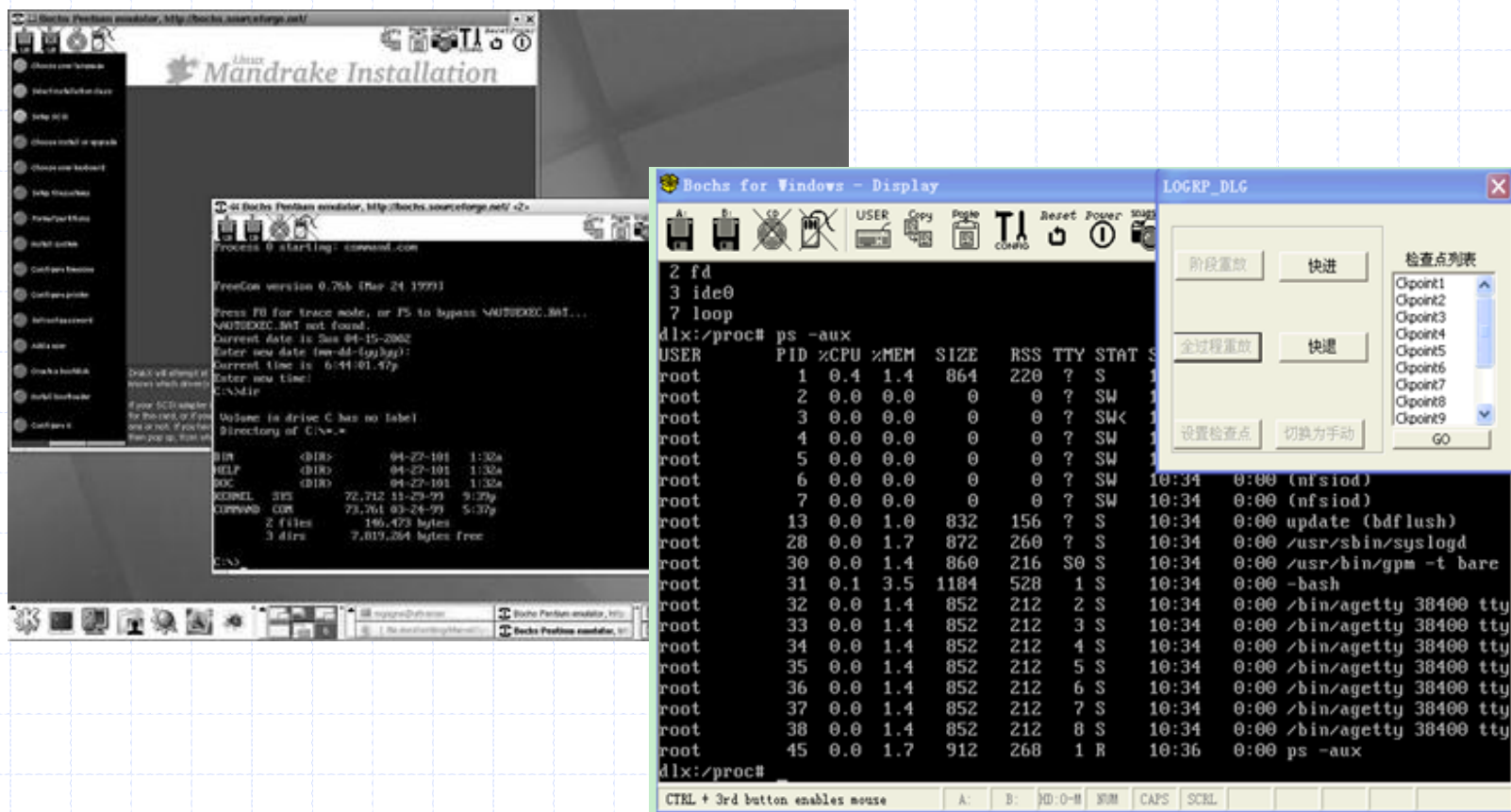


# 标准虚拟机系统—航空ARINC 653（2/2）



- 集成模块化航空电子设备软件平台，采用多层独立级别安全技术架构MILS，实现应用的安全与隔离。

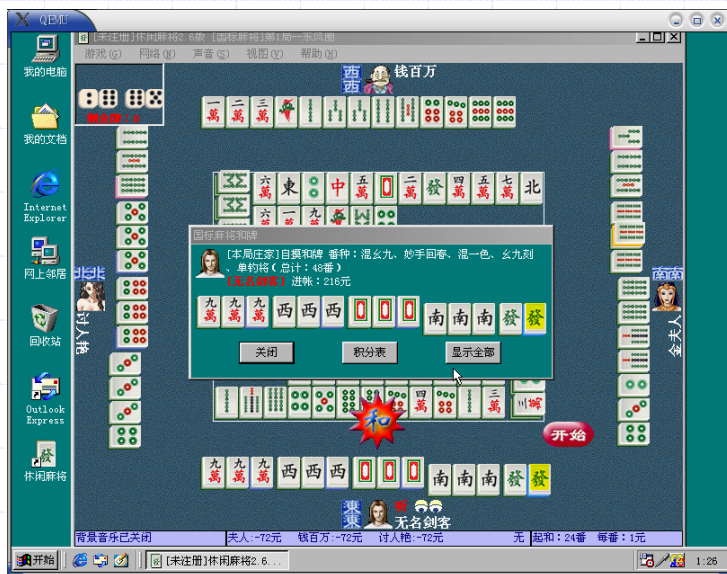
# 全系统模拟器—Bochs



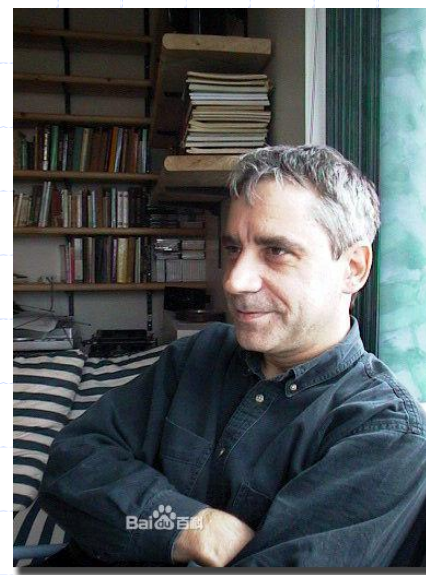
Bochs运行界面

# 全系统模拟器—Qemu

- ❑ Qemu是法国的Fabrice Bellard在Linux内核上写的一个开源仿真器。可以模拟x86、MIPS、SPARC等体系结构。
- ❑ 在Linux2.6.20内核虚拟机KVM（Kernel-based Virtual Machine）、Google Android中得到应用。



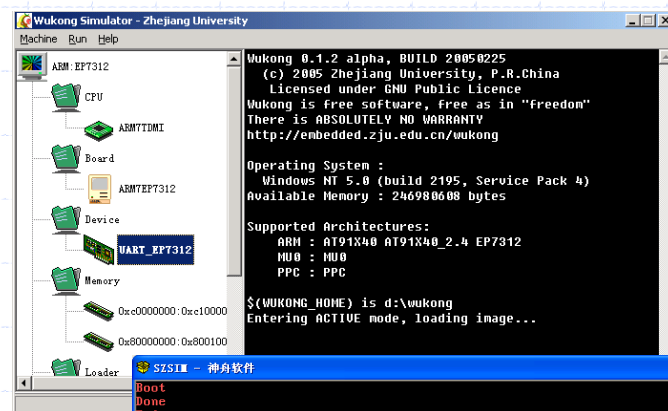
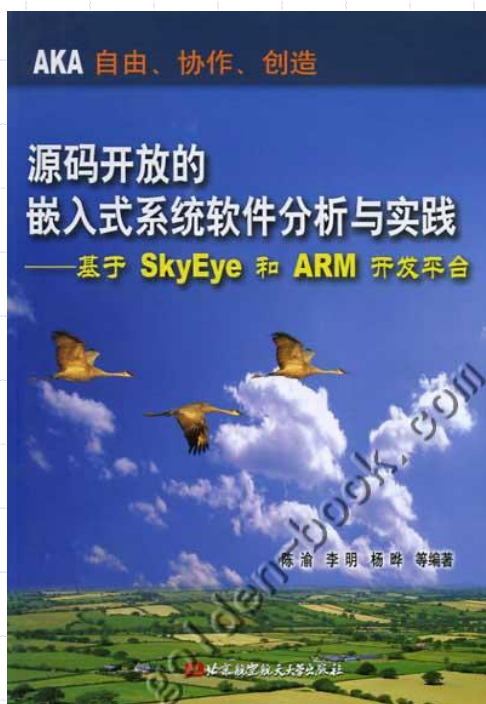
Qemu运行界面



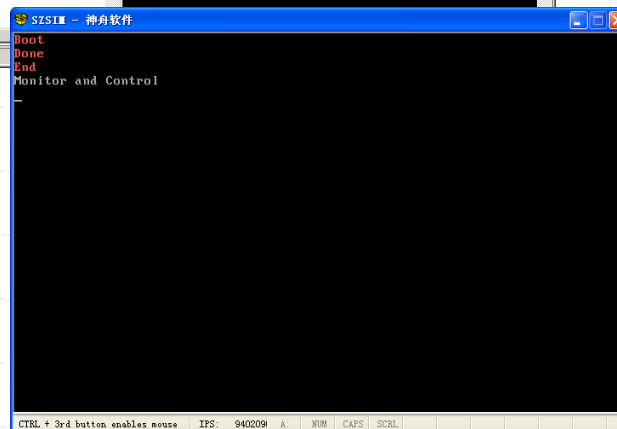
Fabrice Bellard

# 中国的软件模拟器

- ❑ **SkyEye**——清华大学的陈渝博士研制的开源模拟器。
- ❑ **Sim-Godson**——中科院计算所研制的用于评测龙芯性能的模拟器。
- ❑ **wukong**悟空——浙江大学嵌入式软件研发中心研制的模拟器。
- ❑ **SZSIM**——航天科技—浙江大学基础软件研发中心研制的模拟器。



“悟空”运行界面

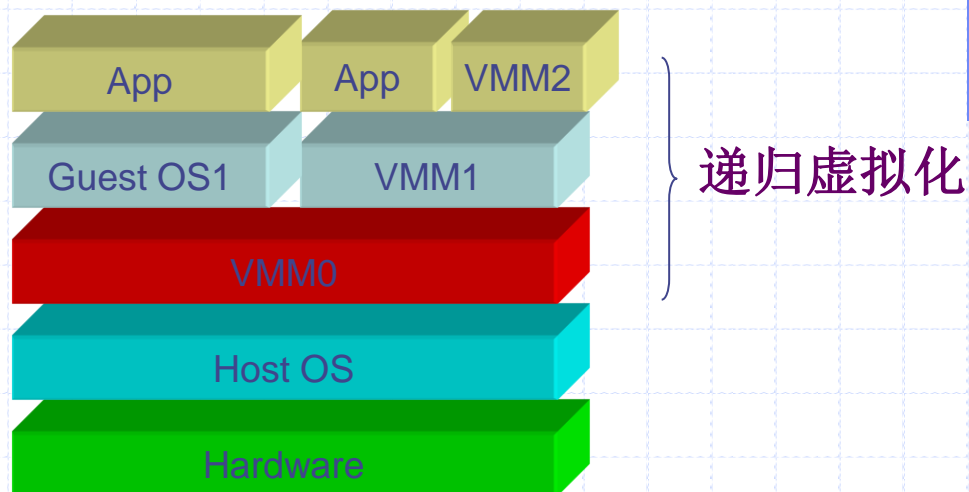


“神舟”运行界面

# 关于系统级虚拟机的两个有趣现象

## □ 虚拟机的递归问题

### ■ User Mode Linux



## □ Where am I ? — 软件如何知道自己运行在哪里？



# 虚拟机系统的分类—按虚拟对象划分

## 虚拟机系统分类



- 1: N虚拟化

- N: 1虚拟化

- N: M虚拟化

# 1: N的虚拟化

## □ 单个计算实体虚拟化为多个计算实体

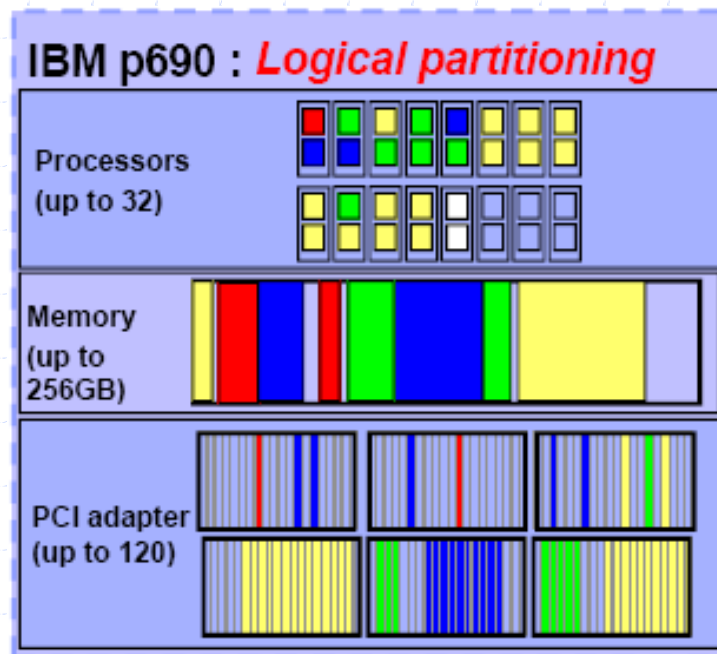
- 通过虚拟化实现不同用户之间的相互隔离，避免相互干扰

- 例如：

- 构造服务器应用

- 1个CPU虚拟化为多个CPU

## □ 实例：IBM P690服务器



- One Linux partition 1 proc, 2 PCI, 3GB
- AIX 1 partition 6 proc, 9 PCI, 4GB
- AIX 2 partition 3 proc, 18 PCI, 12GB
- AIX 3 partition 14 proc, 28 PCI, 64GB

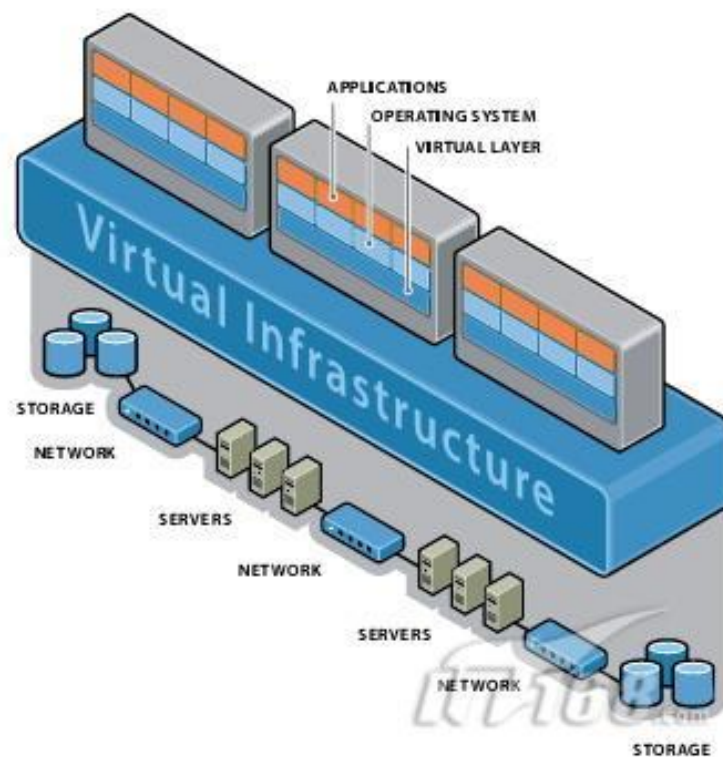


# N: 1的虚拟化

## □ 多个计算实体虚拟化为单个计算实体

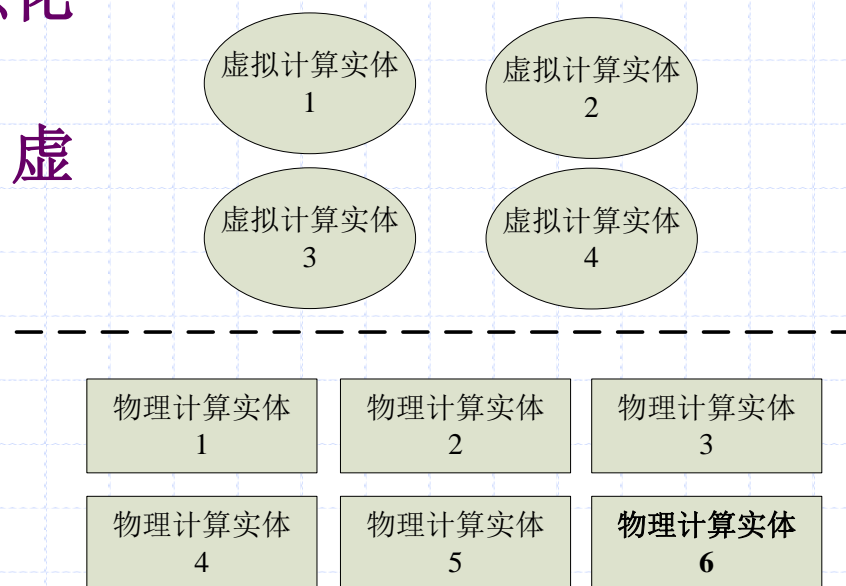
- 便于用户协同使用分散的计算资源
- 可以向用户屏蔽资源的多样性
- 例如:
  - ✓ 科学计算网格
  - ✓  $n$ 个CPU虚拟化为1个CPU

## □ 实例: VMware Infrastructure



# N: M的虚拟化

- 多个计算实体虚拟化为多个计算实体
- 有效资源整合按需动态虚拟化为多个计算实体
- 是“多到一”和“一到多”虚拟化的泛化

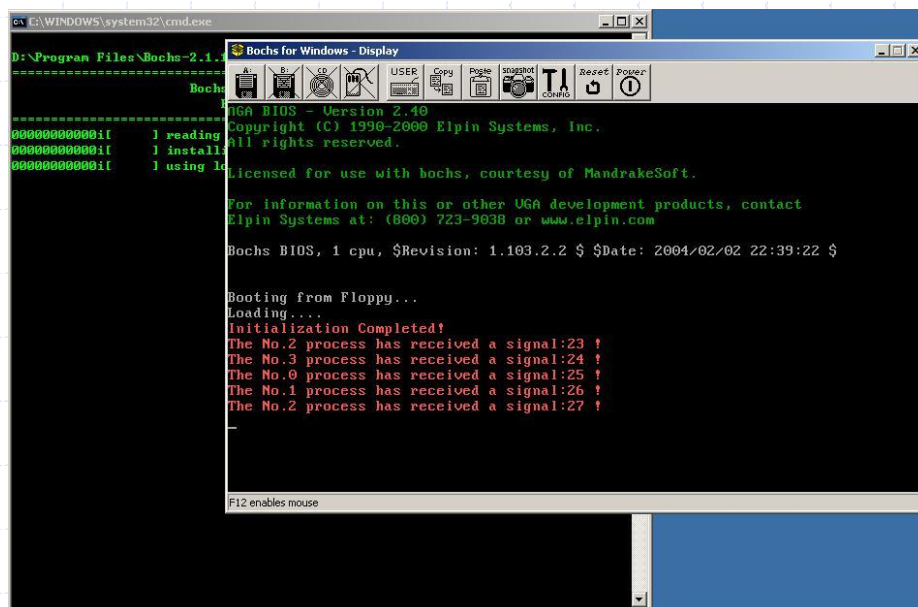


# 课程大纲

-  虚拟机系统发展历程
-  虚拟机系统技术分类
-  系统级虚拟机Bochs简介

# Bochs简介

- Bochs是一个开源、高可移植的IA-32(x86)模拟器，由Kevin Lawton用C++写成，以GNU LGPL方式分发，可通过<http://bochs.sourceforge.net>访问。
- Bochs提供了对Intel x86 CPU、内存、I/O设备、BIOS，以及对MMX、SSEx和3DNow! 指令的模拟。
- Bochs宿主平台包括：Linux、Windows。



# Bochs的运行实验

## □ bochs-2.3.6的试运行（Tinix操作系统）

✓ Hello World!

✓ 多任务运行

```
Bochs for Windows - Display
A: B: CD USER Copy Paste snapshot CONFIG Reset SUSPEND Power
Hello, OS world!gn 2.40
Copyright (C) 1990-2000 Elpin Systems, Inc.
All rights reserved.
Licensed for use with bochs, courtesy of MandrakeSoft.
For information on this or other UGA development products, contact
Elpin Systems at: (800) 723-9038 or www.elpin.com
Bochs BIOS - build: 12/20/07
$Revision: 1.193 $ $Date: 2007/12/20 18:12:11 $
Options: apmbios pcibios eltorito rombios32
Booting from Floppy...
```

```
Bochs for Windows - Display
01FF0000h 00000000h 00010000h 00000000h 00000003h
FFFC0000h 00000000h 00040000h 00000000h 00000002h
RAM size:01FF0000h
----"cstart" begins----
----"cstart" finished----
----"tinix_main" begins----
<Ticks:0xF><Ticks:0x11><Ticks:0x13><Ticks:0x15><Ticks:0x17><Ticks:0x19><Ticks:0x34><Ticks:0x36><Ticks:0x38><Ticks:0x3A><Ticks:0x3C><Ticks:0x3E><Ticks:0x40><Ticks:0x42><Ticks:0x44><Ticks:0x46><Ticks:0x48><Ticks:0x4A><Ticks:0x4C><Ticks:0x4E><Ticks:0x50><Ticks:0x52><Ticks:0x54><Ticks:0x56><Ticks:0x58><Ticks:0x5A><Ticks:0x5C><Ticks:0x78><Ticks:0x7A><Ticks:0x7C><Ticks:0x9A><Ticks:0x9C><Ticks:0x9E><Ticks:0xA0><Ticks:0xA2><Ticks:0xBE><Ticks:0xC0><Ticks:0xC2><Ticks:0xE0><Ticks:0xE2><Ticks:0xE4><Ticks:0xE6><Ticks:0xE8><Ticks:0xEA><Ticks:0x106><Ticks:0x108><Ticks:0x10A><Ticks:0x126><Ticks:0x128><Ticks:0x12A><Ticks:0x147><Ticks:0x149><Ticks:0x14B><Ticks:0x169><Ticks:0x16B><Ticks:0x16D><Ticks:0x16F><Ticks:0x18D><Ticks:0x18F><Ticks:0x191><Ticks:0x1AE><Ticks:0x1B0><Ticks:0x1B2><Ticks:0x1CE><Ticks:0x1D0><Ticks:0x1D2><Ticks:0x1EF><Ticks:0x1F1><Ticks:0x1F3><Ticks:0x20F><Ticks:0x211><Ticks:0x213><Ticks:0x22F><Ticks:0x231><Ticks:0x233><Ticks:0x250><Ticks:0x252><Ticks:0x254><Ticks:0x272><Ticks:0x274><Ticks:0x276><Ticks:0x278><Ticks:0x295><Ticks:0x297><Ticks:0x299><Ticks:0x2B6><Ticks:0x2B8><Ticks:0x2BA><Ticks:0x2D6><Ticks:0x2D8><Ticks:0x2DA><Ticks:0x2F7><Ticks:0x2F9><Ticks:0x2FB><Ticks:0x317><Ticks:0x319><Ticks:0x31B><Ticks:0x337><Ticks:0x339><Ticks:0x33B><Ticks:0x33D><Ticks:0x35A><Ticks:0x35C><Ticks:0x35E><Ticks:0x37C><Ticks:0x37E><Ticks:0x380><Ticks:0x39C><Ticks:0x39E>
T_
IPS: 496845 A: NUM CAPS SCRL
```

# Bochs的配置文件分析

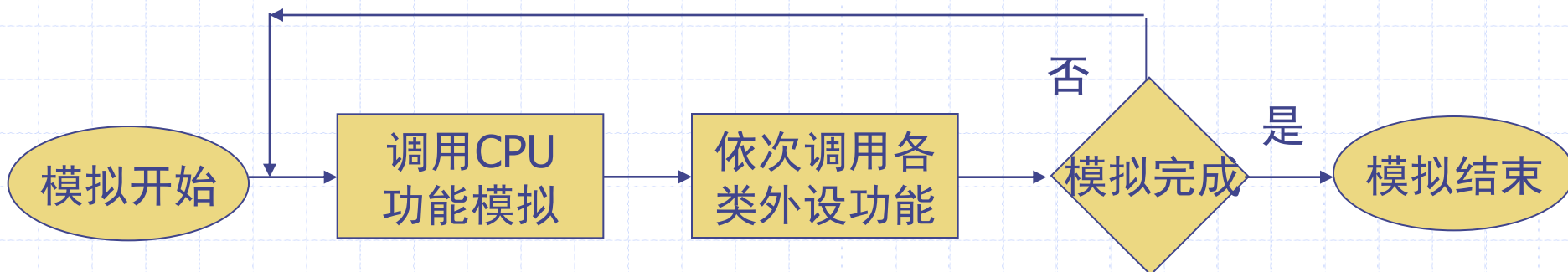
## □ bochsrc.bxrc

```
#####  
# bochsrc.bxrc file for Tinix.  
#####  
  
# how much memory the emulated machine will have  
megs: 32  
  
# filename of ROM images  
romimage: file=../bios/BIOS-bochs-latest  
vgaromimage: file=../bios/VGABIOS-elpin-2.40  
  
# what disk images will be used  
floppya: 1_44=TINIX.IMG, status=inserted  
  
# choose the boot disk.  
boot: a  
  
# where do we send log messages?  
log: bochsout.txt  
  
# disable the mouse, since Tinix is text only  
mouse: enabled=0  
  
# enable key mapping, using US layout as default.  
keyboard_mapping: enabled=0, map=
```

# 系统级虚拟机的典型实现方法

## □ 串行模拟方法

- ✓ 采用串行化的方法同步处理器和外设，即**CPU**每处理一条指令模拟后，依次检测，并调用所有外设功能。
- ✓ 例如：**Bochs**
- ✓ 优点：实现简单
- ✓ 缺点：效率较低





# Bochs系统代码简要分析

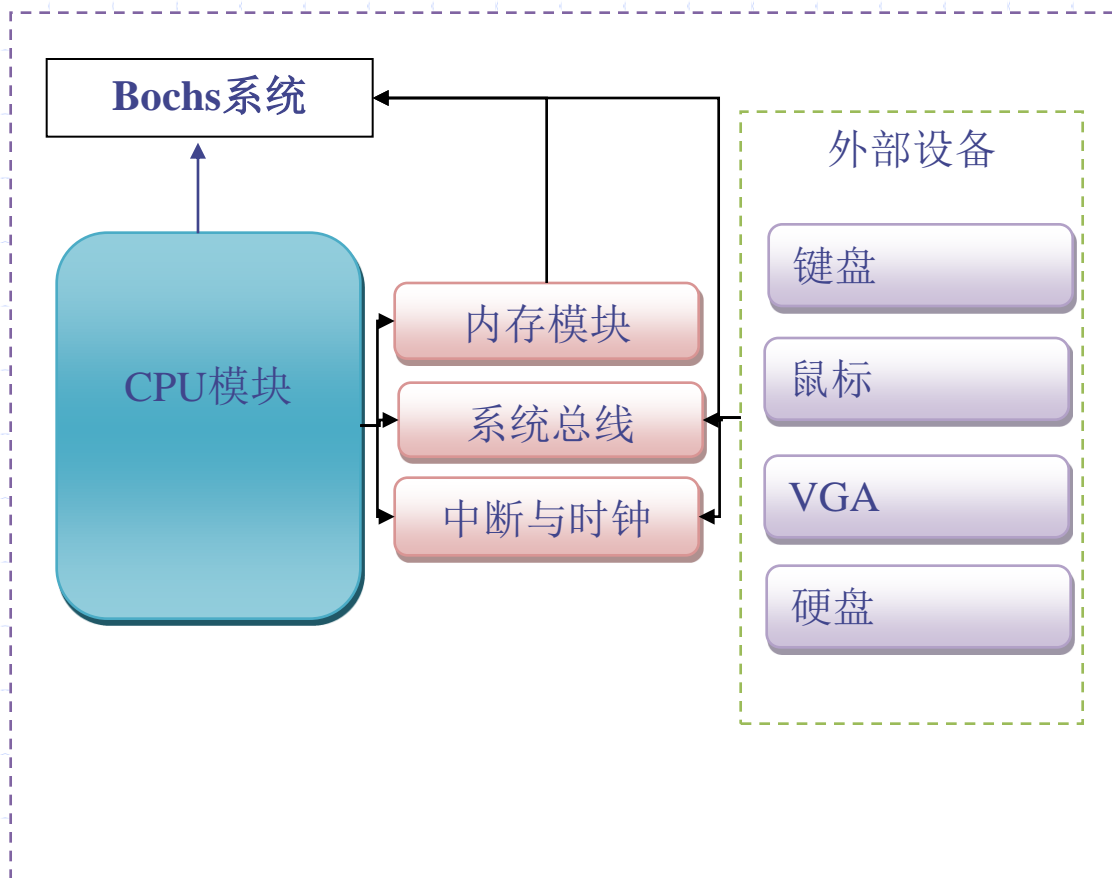
## □ Bochs系统代码分析

### ■ CPU\_loop主循环分析

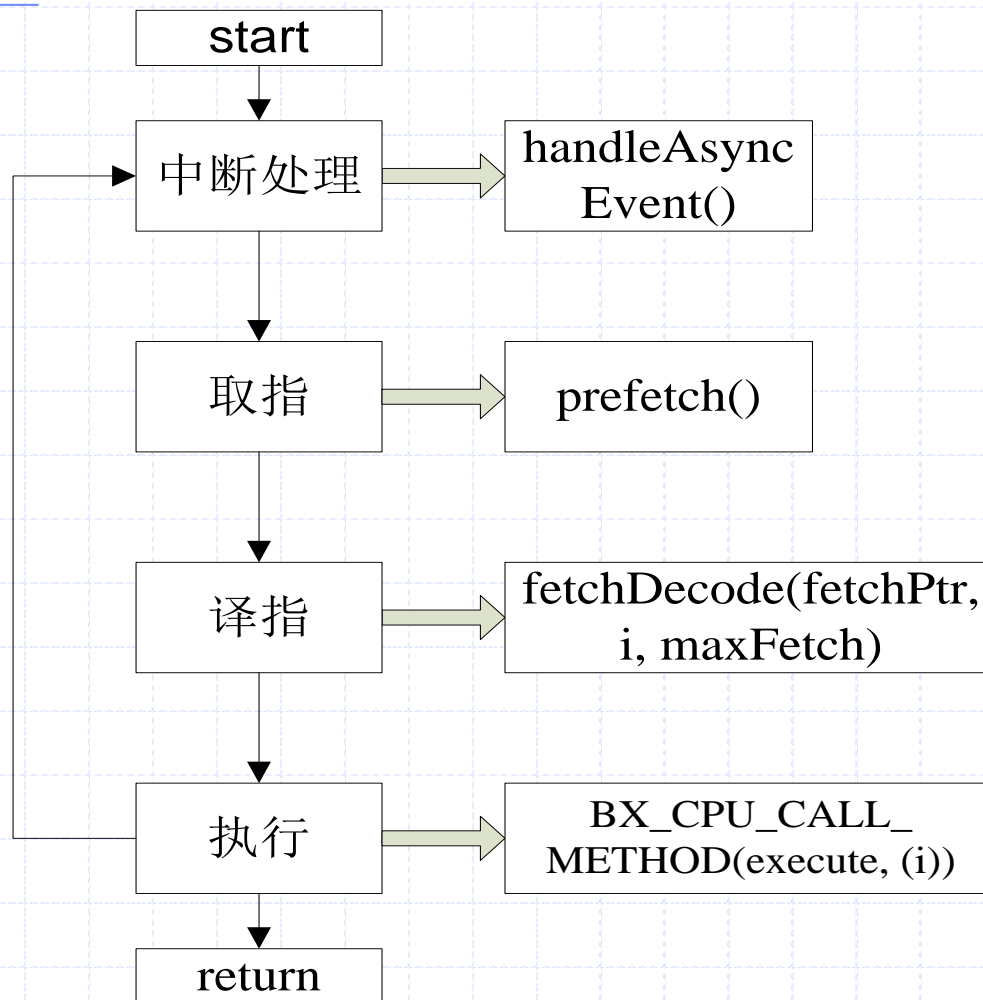
### ■ 外部设备模拟分析

✓ 定时器分析

✓ 中断分析



# CPU工作流程分析——cpu\_loop





谢谢!

