目录

1

2

嵌入式系统概论

3

内容提要

4

1.1 嵌入式系统的定义

- 嵌入式系统是一个较复杂的技术概念，目前国内外关于嵌入式系统尚无严格、统一的定义。
- 根据美国电气与电子工程师学会（IEEE：Institute of Electrical and Electronics Engineers）的定义：嵌入式系统是用于控制、监视或辅助操作机器和设备的装置。
- 一般认为嵌入式系统是以应用为中心，以计算机技术为基础，并且软/硬件可裁剪，可满足应用系统对功能、可靠性、成本、体积和功耗有严格要求的专用计算机系统。

5

1.1 嵌入式系统的定义（续）

- 简单地讲：嵌入式系统就是嵌入到对象体系中、用于执行特定功能的专用计算机系统。
- 三要素
  - ◆嵌入性：嵌入到对象体系中，有对象环境要求
  - ◆专用性：软、硬件按对象要求裁减
  - ◆计算性：实现对象的智能化功能

6

1.1 嵌入式系统的定义（续）

- 特征
  - 面向特定应用，具有功耗低、体积小、成本低、高可靠性特点。
  - 硬件和软件都必须高效率地设计，量体裁衣，力争在有限的硅片面积上实现高的性能，完成功能、可靠性、成本和功耗的苛刻要求。
  - 实时操作系统支持，尽管嵌入式系统的应用程序可以不需要操作系统的支持就能直接运行，但是为了合理地调度多任务，充分利用系统资源，用户可以自行选配实时操作系统开发平台。
  - 嵌入式系统与具体应用有机地结合在一起，升级换代也是同步地进行。因此嵌入式系统产品一旦进入市场，具有较长的生命周期。
  - 嵌入式系统中的软件一般都固化在存储器芯片中。
  - 专门开发工具的支持。嵌入式系统本身不具备自主开发能力，必须有一套开发工具和环境才能进行嵌入式系统开发。

7

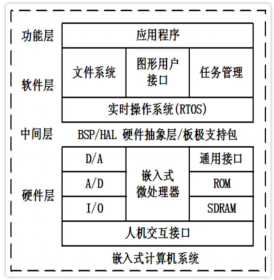
1.1 嵌入式系统的定义（续）

嵌入式系统：

以应用为中心，以计算机技术为基础，软硬件可裁剪，适用于对功能、可靠性、成本、体积、功耗有严格要求的专用计算机。

与常见计算机系统的区别

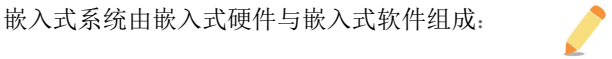
嵌入式系统的部件根据主体设备及其应用的需要，嵌入在主体设备内部，不以独立设备的物理形态出现，发挥着运算、处理、存储及控制的作用，是“用于控制、监视或者辅助操作机器和设备的装置”。



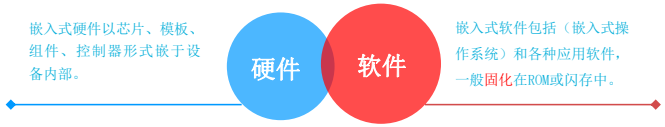
8

1.2 嵌入式系统的组成

嵌入式系统由嵌入式硬件与嵌入式软件组成：



嵌入式硬件以芯片、模板、组件、控制器形式嵌于设备内部。



嵌入式软件包括（嵌入式操作系统）和各种应用软件，一般固化在ROM或闪存中。

常见组成部件有：微处理器、定时器、中断控制器、I/O设备、存储器、传感器、接口等。嵌入式硬件结构以嵌入式处理器为核心，集成度高。

软件与外部硬件和设备联系紧密，具有灵活的适用性。由于嵌入式系统存储空间有限，要求软件代码紧凑、可靠，对实时性有严格要求。

9

1.2 嵌入式系统的组成(续)

- 嵌入式系统一般由嵌入式微处理器、外围支撑硬件、嵌入式实时操作系统以及用户应用软件四个部分组成。
- 嵌入式微处理器
  - 嵌入式微处理器通常把通用PC机中许多由板卡完成的任务集成到芯片内部，这样可以大幅减小系统的体积和功耗，具有重量轻、成本低、可靠性高等优点。
  - 由于嵌入式系统通常应用于比较恶劣的工作环境中，因此嵌入式微处理器在工作温度、电磁兼容性（EMC: Electro Magnetic Compatibility ）及可靠性要求方面比较高。
  - 嵌入式微处理器可按数据总线宽度划分为8位、16位、32位和64位等不同类型，目前比较流行的有80C51、PIC、ARM等系列。主流是8位、32位。

10

1.2 嵌入式系统的组成(续)

- 电磁兼容性（EMC: Electro Magnetic Compatibility）包含两个要素：

1、能在一定的干扰环境下工作；

2、不产生不可容忍的干扰。

11

1.2 嵌入式系统的组成（续）

- **嵌入式微处理器的体系结构**
  - **冯·诺依曼 (von neumann)/普林斯顿(Princeton)体系结构**
    - 程序存储器和数据存储器共用一个存储空间，统一编址；
    - 采用统一的地址及数据总线，指令和数据的宽度相同；
    - 使用灵活（例如 代码远程更新OTA）。
  - **哈佛体系结构**
    - 程序存储器和数据存储器是独立编址的两个存储空间；
    - 这种分离的程序总线和数据总线可允许在一个机器周期内同时获取指令码（程序存储器）和操作数（数据存储器），从而提高执行速度，提高数据的吞吐率，**可靠性高**（大部分程序存储器是只读存储器）。

12

1.2 嵌入式系统的组成（续）

- 嵌入式微处理器指令系统
  - **复杂指令集系统**(Complex Instruction Set Computer, **CISC**)
    - 早期的计算机采用复杂指令集计算机(**CISC**)体系，如Intel公司从8086到Pentium系列CPU
    - 采用**CISC**体系结构的计算机各种指令的使用频率相差悬殊。统计表明，大概有20%的比较简单的指令被反复使用，使用量约占整个程序的80%；而有80%左右的指令则很少使用，其使用量约占整个程序的20%，即**指令的2/8规律**。
    - 在**CISC**中，为了支持目标程序的优化，支持高级语言和编译程序，增加了许多复杂的指令，用一条指令来代替一串指令，简化了软件设计，却增加了硬件的复杂程度。而且**这些复杂指令并不等于有利于缩短程序的执行时间。**
    - 在VLSI(Very-large-scale integration)制造工艺中要求CPU控制逻辑具有规整性，而CISC为了实现大量复杂的指令，控制逻辑极不规整，给VLSI工艺造成很大困难

13

1.2 嵌入式系统的组成（续）

- 嵌入式微处理器指令系统
  - **精简指令集系统**(Reduced Instruction Set Computer，**RISC**)
    - **RISC**是在CISC的基础上产生并发展起来的；
    - **RISC**简化指令系统使计算机的结构更加简单合理，提高运算效率；
    - 优先选取使用频率高的、很有用但不复杂的指令，避免使用复杂指令；
    - 固定指令长度，减少指令格式和寻址方式种类；
    - 指令之间各字段的划分比较一致，各字段的功能也比较规整；
    - 采用Load/Store指令访问存储器，其余指令都在寄存器之间进行；
    - 增加通用寄存器数量，算术/逻辑运算的操作数都在寄存器中存取；
    - 大部分指令控制在一个或小于一个机器周期内完成；
    - 以硬布线控制逻辑为主，不用或少用微码控制。

14

1.2 嵌入式系统的组成（续）

- **CISC**与**RISC**之间的主要差异
  - **指令系统**：RISC设计者把主要精力放在那些经常使用的指令上，尽量使它们具有简单高效的特色。对不常用的功能，常通过组合指令来实现。而CISC的指令系统比较丰富，有专用指令来完成特定的功能。
  - **存储器操作**：RISC对存储器操作有限制，使控制简单化；而CISC机器的存储器操作指令多，操作直接。
  - **程序**：RISC汇编语言程序一般需要较大的内存空间，实现特殊功能时程序复杂，不易设计；而CISC汇编语言程序编程相对简单，科学计算及复杂操作的程序设计相对容易，效率较高。
  - **CPU**：由于RISC CPU包含较少的单元电路，因而面积小、功耗低；而CISC CPU包含丰富的电路单元，因而功能强、面积大、功耗大。
  - **设计周期**：RISC微处理器结构简单，布局紧凑，设计周期短，且易于采用最新技术；CISC微处理器结构复杂，设计周期长。
  - **易用性**：RISC微处理器结构简单，指令规整，性能容易把握，易学易用；CISC微处理器结构复杂，功能强大，实现特殊功能容易。
  - **应用范围**：RISC更适用于嵌入式系统；而CISC则更适合于通用计算机。

15

1.2 嵌入式系统的组成（续）

- 外围硬件设备
  - 嵌入式硬件系统通常是一个以嵌入式微处理器为中心，包含有电源、时钟、复位、输入输出及驱动、存储、其他电路模块，其中操作系统和应用程序都固化在模块的ROM/Flash/OTP中。
  - 外围硬件设备指在嵌入式硬件系统中，除微处理器外的完成输入、输出、存储、显示、通信、调试等部件及电源。
  - 根据外围硬件设备的功能可分为存储器(SRAM、DRAM、Flash、E2PROM、OTP 、ROM等)和输入输出接口(GPIO口、串口、红外接口、I2C、I2S、USB、CAN、Ethernet、LCD、键盘、触摸屏（键）、A/D、D/A、RTC、CAP、PWM等)两大类。

16

1.2 嵌入式系统的组成（续）

- ROM/Flash/OTP/E2PROM

	开发成本	制造成本	可靠性	可修改性	产品周期	功耗
ROM	高	低	高	无	长	低
OTP	中	中	中	无	短	中
FLASH	低	高	低	有	短	高
E2PROM	低	高	中	有	短	高

17

1.2 嵌入式系统的组成（续）

- 嵌入式操作系统（有些系统只是简单的调度器）
  - 由于存储器容量有限，嵌入式操作系统内核通常较小
  - 嵌入式操作系统，都有一个内核(Kernel)和一些系统服务(System Service)。嵌入式操作系统必须提供一些系统服务供应用程序调用，包括**内存分配、I/O存取、中断、任务、定时、延时、信号量、互斥量、邮箱、消息、消息队列、事件组**等服务等，**文件系统、设备驱动**程序则是建立在I/O存取和中断服务基础之上的，有些嵌入式操作系统也提供多种通信协议以及用户接口函数库等
  - 嵌入式操作系统的性能通常取决于内核程序，而内核的工作主要在任务管理(Task Management)、任务调度(Task Scheduling)、进程间通信(IPC)
  - **嵌入式操作系统不是必需的。**

18

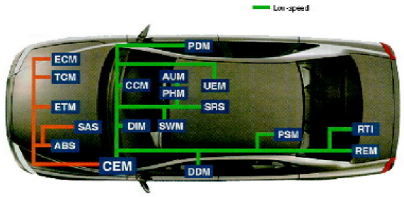
1.2 嵌入式系统的组成（续）

- 应用软件
  - 设计人员针对专门的应用领域而设计的应用程序
  - 把嵌入式操作系统和应用软件组合在一起，作为一个有机整体
  - 嵌入式系统软件的要求与PC机有所不同，其主要特点有：
    - 软件固化存储，修改不易，要有较高的正确率和可靠性；
    - 软件代码要求精简（受成本、体积和功耗存储空间限制）、高效（受主频、功耗限制）、高可靠性（容错）
    - 数据结构简洁（代码优化时，数据结构占80%，编程技巧占20%）

19

1.3 嵌入式系统的应用与发展

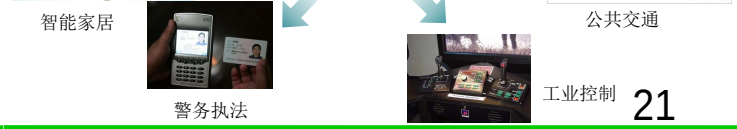
- 嵌入式系统的应用已逐步渗透到金融、航天、电信、网络、信息家电、医疗、工业控制、军事等各个领域，以至于一些学者断言嵌入式系统将成为后PC时代的主宰。形式多样的嵌入式系统与移动通信、传感器网络等技术一道，改变了现有的计算环境。



20

1.3 嵌入式系统的应用与发展(续)

嵌入式系统以其结构简单、功耗小、可定制等特点，逐步成为日常生活与基础行业建设的核心组成部分，极大促进了生产生活的发展。



21

1.3 嵌入式系统的应用与发展(续)

- 各种**信息家电**产品，如数字电视机、机顶盒，数码相机、音响设备、网络设备、洗衣机、冰箱、空调、智能玩具以及其他消费类电子产品等。

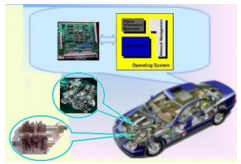
- 智能垃圾桶i.Master

- DangerBomb闹钟

- 配备电子食谱的锅铲

22

1.3 嵌入式系统的应用与发展(续)



- 汽车电子

处理器个数可达三位数

-车载：娱乐、定位等

-车控：ABS、EBD等

- 改装遮阳板 DVD / TV / MP3

- 月球车

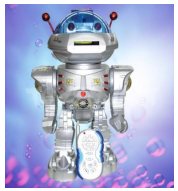
- 航空航天

- 汽车立体声音响
  HD Radio扩展包

23

1.3 嵌入式系统的应用与发展(续)

- 各种智能测量仪表、数控装置、可编程控制器、控制机、分布式控制系统、现场总线仪表及控制系统、工业机器人、智能机器人、智能传感器、机电一体化机械设备等。



24

1.3 嵌入式系统的应用与发展(续)

- 各种**武器控制系统**（火炮控制、导弹控制、智能炸弹制导引爆装置）、坦克、舰艇、轰炸机等陆海空各种军用电子装备，雷达、电子对抗军事通信装备，野战指挥作战用各种专用设备等。我国嵌入式计算机最早用于导弹控制。

21世纪部队旅及旅以下作战指挥系统夜视扫描、全球定位、指挥通信

25

1.3 嵌入式系统的应用与发展(续)

- 复印机、打印机、传真机、扫描仪、其他计算机外围设备、安全监控设备、智能手机、通信终端、程控交换机、网络设备（路由器、交换机等）、视频会议设备等。

26

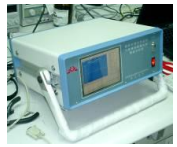
1.3 嵌入式系统的应用与发展(续)

- 医疗电子仪器，X光机、超声诊断仪、计算机断层成像系统、心脏起博器、监护仪、辅助诊断系统、远程医疗、专家系统等。

- 辅助诊断系统

- 手持仪

- 中医指套传感器脉象虚拟仪



- 便携式多参数监护仪

- 动态心电图仪

27

1.3 嵌入式系统的应用与发展(续)

穿戴设备

- Nike的Speed+手表
  - --结合iPod和运动计测
- Martin Frey手表
  - --日程表
  - --和手机联动
  - --获取网络连接和GPS定位信息
- GTX公司定位的运动跑鞋
  - --内置的GPS接收器和可充电电池

28

1.3 嵌入式系统的应用与发展(续)

结论：

嵌入式系统和我们的生活、工作紧密相关，嵌入在各种设备中。

29

内容提要

30

2.1 嵌入式微处理器分类

- 按字符宽度分：8位、16位、32位

  8位一般是哈佛结构，成本低，可靠性高。

  32位一般是冯·诺依曼 /普林斯顿体系结构，成本高，灵活性好。

- 从应用的角度来划分
  - 嵌入式微处理器 （Embedded Microprocessor Unit，EMPU）
  - 嵌入式微控制器（Micro Controller Unit，MCU）
  - 嵌入式DSP处理器（Digital Signal Processor，DSP）
  - 嵌入式片上系统（System on Chip，SoC）

31

2.1 嵌入式微处理器分类（续）

- 嵌入式微处理器 EMPU（计算处理能力强，接口相对简单）
  - 嵌入式微处理器是由通用微处理器演变而来。仅保留与嵌入式应用紧密相关的功能部件，配备必要的外围扩展电路，如存储器扩展电路、I/O扩展电路及其他一些专用的接口电路等，以很低的功耗和资源满足嵌入式应用的特殊需求。
  - 由于嵌入式系统通常应用于比较恶劣的环境中，因此嵌入式微处理器在工作温度、电磁兼容性以及可靠性方面的要求较高。
  - 嵌入式微处理器组成的系统具有体积小、重量轻、成本低、可靠性高的优点。

32

2.1 嵌入式微处理器分类（续）

- 嵌入式微控制器 MCU （接口功能强大，计算处理能力相对弱）
  - 又称单片机，它将整个计算机系统集成到一块芯片中
  - 一般以某种微处理器内核为核心，根据某些典型的应用，在芯片内部集成了ROM/EPROM、RAM、总线、总线逻辑、定时/计数器、看门狗、I/O、串行口、脉宽调制输出、A/D、D/A、Flash ROM、EEPROM等各种必要功能部件和外设
  - 为适应不同的应用需求，可对功能的设置和外设的配置进行必要的修改和裁减定制，使得一个系列的单片机具有多种衍生产品，每种衍生产品的处理器内核都相同，只是存储器和外设的配置及功能的设置不同。这样可以使单片机最大限度地和应用需求相匹配，从而减少整个系统的功耗和成本
  - 和嵌入式微处理器相比，微控制器的单片化使应用系统的体积大大减小，从而使功耗和成本大幅度下降，可靠性提高

33

2.1 嵌入式微处理器分类（续）

- 嵌入式DSP处理器 （处理连续的数据流）
  - 在数字信号处理应用中，各种数字信号处理算法相当复杂，一般结构的处理器无法实时地完成这些运算.由于DSP处理器对系统结构和指令进行了特殊设计，因此它更适合于实时地进行数字信号处理。
  - 在数字滤波、FFT(fast Fourier transform)、频谱分析等方面，DSP应用正从在通用单片机中以普通指令实现DSP功能，过渡到采用嵌入式DSP处理器。
  - 在有关智能方面的应用中，也需要嵌入式DSP处理器，例如各种带有智能逻辑的消费类产品，生物信息识别终端，带有加/解密算法的键盘，ADSL接入，实时语音压缩解压系统，虚拟现实显示等。这类智能化算法一般运算量都较大，特别是向量运算、指针线性寻址等较多，而这些正是DSP处理器的优势所在。
  - 嵌入式DSP处理器有两类：一是DSP处理器经过单片化、EMC改造、增加片上外设成为嵌入式DSP；二是在通用单片机或片上系统中增加DSP协处理器。
  - 嵌入式DSP处理器的设计者通常把重点放在处理连续的数据流上。如果嵌入式应用中强调对连续的数据流的处理及高精度复杂运算，则应该优先考虑选用DSP器件。

34

2.1 嵌入式微处理器分类（续）

- 嵌入式片上系统 SoC（软硬件一体化的专用产品）
  - 随着VLSI设计的普及和半导体工艺的迅速发展，可以在一块硅片上实现一个更为复杂的系统，这就是片上系统（SoC）
  - 各种通用处理器内核和其他外围设备都将成为SoC设计公司的标准库中的器件，用标准的VHDL等硬件描述语言描述，用户只需定义出整个应用系统，仿真通过后就可以将设计图交给半导体工厂制作芯片样品
  - 这样，整个嵌入式系统大部分都可以集成到一块芯片中去，应用系统的电路板将变得很简洁，这将有利于减小体积和功耗，提高系统的可靠性

35

2.2 ARM嵌入式微处理器

- ARM 即Advanced RISC Machines的缩写，既可以认为是一个公司的名字，也可以认为是对一类微处理器的通称，还可以认为是一种技术的名字
- 1985年4月26日，第一个ARM原型在英国剑桥的Acorn计算机有限公司诞生，由美国加州San Jose VLSI技术公司制造。20世纪80年代后期，ARM很快开 发出Acorn的台式机产品，形成英国的计算机教育基础
- 1990年成立了Advanced RISC Machines Limited（后来简称为ARM Limited，ARM公司）。ARM公司既不生产芯片也不销售芯片，它只出售芯片技术授权

36

2.2 ARM嵌入式微处理器（续）

- 采用ARM技术知识产权（IP: Intellectual Property）核的微处理器，即通常所说的ARM嵌入式微处理器，已广泛应用于如下领域：
  - **工业控制**：作为32位的RISC架构，基于ARM核的微控制器芯片不但占据了高端微控制器市场的大部分市场份额，同时也逐渐向低端微控制器应用领域扩展，ARM微控制器的低功耗、高性价比，向传统的8位/16位微控制器提出了挑战
  - **无线通讯**：目前已有超过85%的无线通讯设备采用了ARM技术，ARM以其高性能和低成本，在该领域的地位日益巩固。
  - **网络系统**：采用ARM技术的ADSL(Asymmetric digital subscriber line)芯片正逐步获得竞争优势。
  - ARM在**语音及视频处理**上进行了优化，对DSP的应用领域提出了挑战消费类电子产品：ARM技术在目前流行的数字音频播放器、数字机顶盒和游戏机中得到广泛采用。
  - **成像和安全产品**：现在流行的数码相机和打印机中绝大部分采用ARM技术。手机中的32位SIM智能卡也采用了ARM技术

37

2.2 ARM嵌入式微处理器（续）

- 特点
  - 体积小，低功耗，低成本，高性能；
  - 支持Thumb（16位）/ARM（32位）双指令集，兼容8位/16位器件；
  - 使用单周期指令，指令简洁、规整；
  - 大量使用寄存器，大多数数据操作都在寄存器中完成，只有加载/存储指令可以访问存储器，以提高指令的执行效率；
  - 寻址方式简单灵活，执行效率高；
  - 固定长度的指令格式

38

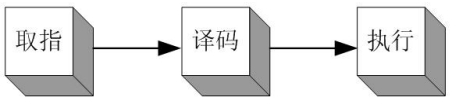
2.2 ARM嵌入式微处理器（续）

- 有ARM7、ARM9、ARM11、Cortex、SecurCore等系列
- ARM7系列，优化了用于对价位和功耗敏感的消费应用的低功耗32位核
  - 嵌入式ICE-RT (In Circuit Emulation-Real Time)逻辑
  - 三级流水线和冯·诺依曼体系结构，提供0.9MIPS/MHz (Million instructions per second)。流水线是RISC处理器执行指令时采用的机制。使用流水线，可以在取下一条指令的同时译码和执行其他指令，从而加速指令的执行。可以把流水线想象成汽车生产线，每个阶段只完成一项专门的生产任务

39

2.2 ARM嵌入式微处理器（续）

- ARM7的三级流水线
  - 取指(Fetch)：从存储器中装载一条指令；
  - 译码(Decode)：识别将被执行的指令；
  - 执行(Execute)：处理指令并把结果写回到寄存器



40

2.2 ARM嵌入式微处理器（续）

- ARM9系列，提供高性能和低功耗领先的硬宏单元
  - 5级流水线
  - 哈佛体系结构提供1.1MIPS/MHz
  - ARM920T和ARM922T内置MMU(Management Memory Unit)、指令和数据cache和高速总线接口。ARM940T内置指令和数据cache、保护单元和高速AMBA(AMBA: Advanced Microcontroller Bus Architecture)总线接口
  - ARM9E系列是一种可综合处理器，带有DSP扩充和紧耦合存储器/紧致内存(TCM)接口，使存储器以完全的处理器速度运行，可直接连接到内核上

41

2.2 ARM嵌入式微处理器（续）

- ARM10系列 带有
  - 64位AHB指令和数据接口；
  - 6级流水线；
  - 1.25MIPS/MHz；
  - 与同等的ARM9器件相比，其性能提高50%
- ARM11系列，提供了两种新型节能方式，功耗更小

42

2.2 ARM嵌入式微处理器（续）

- Cortex系列（ARM新的命名体系）
  - ◆Cortex-A：高性能，丰富的功能
  - ◆Cortex-R：高可靠性，高实时应用
  - ◆Cortex-M：低功耗，代替微控制器（单片机）
- SecurCore：安全应用

43

2.3 嵌入式微处理器选型

ARM微处理器内核的选择：

- ARM微处理器包含一系列内核结构以适应不同的应用领域。如果用户希望使用WinCE或标准Linux等操作系统以减少软件开发时间，需选择ARM720T以上带有MMU（Memory Management Unit）功能的ARM芯片
- 系统工作频率：在很大程度上决定了ARM微处理器的处理能力
- 片内存储器容量：大多数的ARM微处理器片内存储器的容量都不大，需要用户在设计系统时外扩
- 片内外围电路的选择：除ARM微处理器核以外，几乎所有的ARM芯片均根据各自不同的应用领域，扩展了相关功能模块，并集成在芯片之中，称之为片内外围电路，如USB接口、IIS接口、LCD控制器、键盘接口、RTC、ADC和DAC、DSP协处理器等

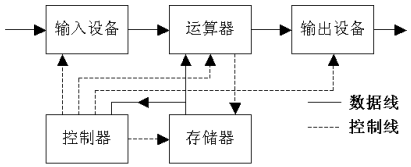
44

2.3 嵌入式CPU架构

- CPU发展出来三个分枝：DSP、MCU和MPU。
- DSP运算能力强，擅长很多的重复数据运算，而MCU则适合不同信息源的多种数据的处理诊断和运算，速度并不如DSP。
- MCU区别于DSP的最大特点在于它的通用性，反应在指令集和寻址模式中。
- MCU(micro controller unit)微控制器单元，MPU (micro processor unit)微处理器单元，其中,MCU集成了片上外围器件,而MPU不带外围器件(例如存储器阵列)。
- DSP与MCU的结合是DSC。DSC就是数字信号控制器，在处理许多需由微控制器(MCU)和数字信号处理器(DSP)共同完成的复杂问题上得到应用。

45

2.3.1 冯诺依曼结构

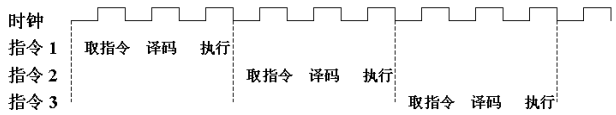


- 冯·诺依曼结构也称普林斯顿结构，是一种将程序指令存储器和数据存储器合并在一起的存储器结构。程序指令存储地址和数据存储地址指向同一个存储器的不同物理位置，因此程序指令和数据的宽度相同，如英特尔公司的8086中央处理器的程序指令和数据都是16位宽。

46

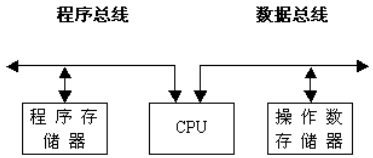
2.3.1 冯诺依曼结构

- 如下图所示，指令1至指令3均为存、取数指令，对冯.诺伊曼结构处理器，由于取指令和存取数据要从同一个存储空间存取，经由同一总线传输，因而它们无法重叠执行，只有一个完成后再进行下一个。



47

2.3.2 哈佛结构



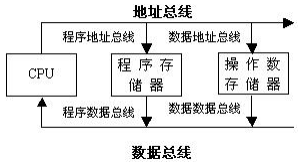
- 数字信号处理一般需要较大的运算量和较高的运算速度，为了提高数据吞吐量，在数字信号处理器中大多采用哈佛结构。
- 与冯.诺伊曼结构处理器比较，哈佛结构处理器有两个明显的特点：
  - ◆ 使用两个独立的存储器模块，分别存储指令和数据，每个存储模块都不允许指令和数据并存；
  - ◆ 使用独立的两条总线，分别作为CPU与每个存储器之间的专用通信路径，而这两条总线之间毫无关联。

48

2.3.2 哈佛结构

- 由于取指令和存取数据分别经由不同的存储空间和不同的总线，使得各条指令可以重叠执行，这样，也就克服了数据流传输的瓶颈，提高了运算速度。
- 哈佛结构强调了总的系统速度以及通讯和处理器配置方面的灵活性。
- 哈佛机构的高性能体现在在单片机、DSP芯片平台上运行的程序种类和花样相对PC机这种通用计算机较少，因为各个电子娱乐产品中的软件升级相对较少，应用程序可以用汇编作为内核，最高效率地使用流水线技术，获得最高的效率。

2.3.3 改进的哈佛结构



- 使用两个独立的存储器模块，分别存储指令和数据，每个存储模块都不允许指令和数据并存，以便实现并行处理；
- 具有一条独立的地址总线和一条独立的数据总线，利用公用地址总线访问两个存储模块（程序存储模块和数据存储模块），公用数据总线则被用来完成程序存储模块或数据存储模块与CPU之间的数据传输；
- 两条总线由程序存储器和数据存储器分时共用。

2.3.4 处理器结构小结

- 8086、ARM7是冯氏结构，ARM9、ARM11是哈佛结构。
- 冯氏结构简单、易实现、成本低，但效率偏低；
- 哈佛结构效率高但复杂，对外围设备的连接与处理要求高，十分不适合外围存储器的扩展。
- 现在的处理器，依托CACHE的存在，已经很好的将二者统一起来了。
- 现在的处理器虽然外部总线上看是诺依曼结构的，但是由于内部CACHE的存在，因此实际上内部来看已经类似改进型哈佛结构的了。

内容提要

3 嵌入式操作系统

常见嵌入式操作系统有：Linux、Windows CE、μC/OS、Palm OS和Vx Works等

内容提要

4 嵌入式系统安全简介

嵌入式系统安全事件频发

随着工作环境的网络化和系统处理能力不断增加，嵌入式系统也面临着众多的安全挑战。除了传统的僵尸网络以及嵌入式木马程序与后门，还有针对嵌入式系统的缓冲区溢出攻击以及注入代码攻击，ROP(Return-oriented programming)攻击，旁路攻击，近年来还出现的攻击嵌入式系统的震网病毒、火焰病毒、Duqu病毒，影响了公共交通、工业控制、能源、军工等重要基础行业,对资源环境、基础设施以及生命财产造成巨大威胁。

55

4 嵌入式系统安全简介（续）

嵌入式系统安全事件频发

01 波兰城市轨道交通脱轨事件

- 2008年，一少年攻击了波兰Lodz的**城铁系统**，通过电视遥控器改变轨道扳道器，导致四节车厢脱轨。

56

4 嵌入式系统安全简介（续）

嵌入式系统安全事件频发

02 Stuxnet震网病毒

- 2010年，西门子首次监测到专门攻击公司工业控制系统的Stuxnet病毒，也称为震网病毒。
- 2010年，伊朗政府宣布Stuxnet病毒感染布什尔核电站员工电脑，直接破坏了纳坦兹浓缩铀工厂的近千台离心机，导致核电站延期启动，对伊朗**国家核计划**造成重大影响，严重威胁核反应堆安全运营。

57

4 嵌入式系统安全简介（续）

嵌入式系统安全事件频发

03 安全会议上展示的嵌入式攻击

- 2010年在加州奥克兰召开的安全会议上，加州大学圣地亚哥分校和华盛顿大学的研究者展示了攻击车载嵌入式系统的技术，该技术能够恶意篡改车载自适应刹车控制器、速度表等重要的嵌入式控制模块，对**车载嵌入式系统**造成重大的安全威胁，甚至会导致严重的交通事故；
- 2012年在加州召开的设计年会西部会议上，Mocana高级分析师Robert Vamosizhan介绍了针对**打印机、数字机顶盒**的攻击；
- Jay Radcliffe通过侵入**胰岛素泵的控制系统**，从而能够肆意篡改其运行状况。

58

4 嵌入式系统安全简介（续）

嵌入式系统安全事件频发

04 美国伊利诺伊州水利供水系统受损

- 2011年，美国伊利诺伊州一家水厂的**监控及数据采集系统（SCADA）**因遭到黑客攻击，其中一个水泵被频繁开关导致停止运转。
- 美国国土安全部门和联邦调查局调查指出目前许多控制重要行业的工业SCADA系统存在脆弱性，具有很大的安全隐患。

59

4 嵌入式系统安全简介（续）

嵌入式系统安全事件频发

05 Havex病毒

- 2014年6月，安全厂商F-Secure发现“Havex病毒”，ICS-CERT发布安全通行，该病毒主要攻击**能源行业(水电大坝、核电站、电网)**。
- Havex被编写来感染SCADA和工控系统中使用的工业控制软件，这种木马可能有能力禁用水电大坝、使核电站过载、甚至可以做到按一下键盘就关闭一个国家的电网。
- 近来被用于从事工业间谍活动，主要攻击对象是欧洲的许多使用和开发工业应用程序和机械设备的公司。

60

嵌入式系统安全事件频发

06 攻击电力系统的攻击

- 2015年12月，乌克兰的**国家电网**中被植入了恶意软件BlackEnergy，导致发电站意外关闭，造成地区大规模电力瘫痪；
- 2016年1月，以色列**国家电力局**网络受到勒索软件ransomware攻击，攻击者通过发送钓鱼邮件诱骗收件人执行恶意代码，加密电脑中相关内容，电力供应系统受到重大网络攻击侵袭，近70万民众遭受停电困扰。

61

嵌入式系统安全事件频发

07 手机病毒“幽灵推“

- 截至2015年9月，一种名为“幽灵推（Ghost Push）的病毒感染了全球大量**安卓手机**，每日有超过60万台手机中毒。病毒自带Root功能，会先对手机进行Root操作，获取系统最高权限，再执行恶意代码。

超级手机病毒“幽灵推”已遍布全球，左图以不同颜色表示各地区病毒发现热度。

62

嵌入式系统攻击分类

01 根据攻击对象分类

利用嵌入式自身的安全缺陷，或者利用其外部不受信任的环境，嵌入式系统面临诸多攻击威胁，根据攻击对象不同，可将其分为隐私数据攻击、可用性攻击、代码完整性攻击等。

隐私数据攻击	可用性攻击	代码完整性攻击
这种攻击的目的是获取嵌入式系统内存储、传递或操作的敏感信息数据；防范这类攻击的主要手段是对敏感信息数据进行加密保护，但实现加密保护需要密钥，密钥的创建、存储、使用和销毁等，需要引入能够信任的密钥管理机制以保障其安全性。此外，还可通过访问控制对敏感信息数据进行保护。	这类攻击挪用系统资源，扰乱系统的正常工作，使系统不能执行相应正常操作。可以通过在嵌入式系统中，添加可靠的资源分配管理组件，来防范这类攻击。	这种攻击的目的是获取嵌入式这种攻击试图修改嵌入式系统相关数据或代码。防范这类攻击的重点是保证嵌入式系统自身代码的完整性，可以在运行前通过对嵌入式系统相关代码进行安全度量，检测代码是否被篡改。

63

嵌入式系统攻击分类

02 根据发起攻击的代理工具或手段分类

软件攻击	硬件攻击	缓存溢出攻击
如病毒，木马，蠕虫等通过软件代理对终端系统结构的薄弱环节发起的攻击。这类攻击是耗费代价较小，是较为常见的一种攻击。	如硬件分解、电磁干扰、使用探针对嵌入式芯片内部的交互信息进行窃听等。这类攻击需要较为昂贵的基础设施要求，较难实现。	向缓存中传送超出容量的数据，并伴以一段恶意执行代码及用来覆盖调用程序返回地址的地址数据，造成缓存溢出。当功能返回时，开始执行恶意代码。

64

软件增强

01 使用嵌入式安全操作系统

- 安全操作系统通过参照监视器监视系统的运行，防止违反安全策略的动作产生，当前嵌入式安全操作系统一般都具备身份认证、自主访问控制和安全审计等功能。第四代防火墙的设计以这种安全操作系统为基础。

65

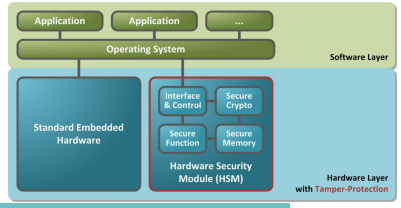
硬件增强

01 增添加密运算模块

- 使用应用程序特定的集成电路（ASIC）在硬件上实现给定的加密算法，只需要很少的成本且可批量生产。

66

硬件增强



02 添加专用安全存储模块

◆ 参考PC端可信计算思想，在嵌入式系统中添加一个专用的安全硬件模块，并将敏感数据保护在一个安全设计十分牢靠的物理设备中，可采用以下几种先进技术。

防篡改技术　物理安全技术　硅工艺技术

67

架构设计增强

01 引入TrustZone架构

✓ 从体系架构角度出发，引入TrustZone架构增强嵌入式系统安全。TrustZone提供硬件隔离，在尽量不影响原有处理器设计的情况下保护安全内存、加密块、键盘和显示器等外设。

68