**2015级嵌入式：**

**一、改错题(共5小题，每小题3分，共15分)**

1.实时操作系统内核的性能可以以每秒钟能做多少次任务切换来评价。

错。做任务切换所需要的时间取决于CPU有多少寄存器要入栈。实时内核的性能不应该以每秒钟能做多少次任务切换来评价。

2.在ARM中复位属于异常。

对。

3.在大端存储模式下存储32位数0x1234567到2000-2003四字节单元中，2000H单元的数值为0x12.

错。应为0x01H。

4. I2C总线是异步通信总线。

错。同步。

5.商业操作系统几乎都是不可剥夺型内核。

错。商业软件几乎没有不可剥夺型内核。

**二、简答题(共10小题，每小题5分，共50分。回答简明扼要。)**1.什么是嵌入式系统?嵌入式系统由哪几个部分组成?

答：

（1）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。

（2）组成：微处理器、外围支撑硬件、嵌入式实时操作系统（或调度器）、用户应用软件。

2简述NAND Flash和NOR Flash的特点。

答：NOR和NAND是现在市场上两种主要的非易失闪存技术。

NAND FLASH：以页为单位进行读和编程操作，以块为单位进行擦除操作。数据、地址采用同一总线。实现串行读取。随机读取速度慢且不能按字节随

机编程。芯片尺寸小、引脚少，是位成本最低的固态存储器。

NOR FLASH：PPT没有。

下面是网图：



3.电磁兼容性(EMC)包含哪两个方面的含义。

答：能在一定的干扰环境工作、不产生不可容忍干扰

4.嵌入式微处理器的体系结构由哪两类?各有何特点?

答：

（1）冯·诺依曼 (von neumann)/普林斯顿(Princeton)体系结构

①程序存储器和数据存储器共用一个存储空间，统一编址；

②采用统一的地址及数据总线，指令和数据的宽度相同；

③使用灵活（例如 代码远程更新OTA）。

（2）哈佛体系结构

①程序存储器和数据存储器是独立编址的两个存储空间；

②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）。

5.简述WDT看门狗的原理和作用。

答：

看门狗：是一种电路，具有监视并恢复程序正常运行的功能。它是一定时器电路。

**看门狗的工作原理**：设一系统程序完整运行一周期的时间是Tp，看门狗的定时周期为Ti，要求Ti>Tp。在程序运行一周期后，修改定时器的计数值，只要程序正常运行，定时器就不会溢出。若由于干扰等原因使系统不能在Tp时刻修改定时器的计数值，定时器将在Ti 时刻溢出，引发系统复位，使系统得以重新运行，从而起到监控作用。

**看门狗的作用**：当嵌入式系统运行时受到外部干扰或者系统错误，程序有时会出现“跑飞”，导致整个系统瘫痪。在对系统稳定性要求较高的场合，为了防止这一现象的发生，需要一种叫“看门狗”(Watchdog)的电路。看门狗的作用就是当系统“跑飞”而进入死循环时，恢复系统的运行。

6.很多嵌入式芯片没有除法指令，系统是如何实现除法和取模运算的?

答：

用位操作（移位和+/-）代替除法；取模运算用 & 代替取模（P632）

7.要提高嵌入式系统可靠性，对未使用的引脚该如何配置?（问的老师）

答:芯片手册有说明的按手册处理；

输出脚悬空处理；

GPIO可设置为输出低悬空处理；

输入脚有内部上拉或下拉的可配置下拉或上拉，否则必须通过电阻或直接接地或电源。

8.设计COS时，文件头和文件体为什么不能存放在存储器的相同页面?

答：

文件头不变，文件体可变，因此不能放在相同的页面，防止撕裂。

9.试举例说明什么是时间攻击。

答：

1996年美国科学家Paul首先发现针对密码芯片的时间攻击法。该方法通过对密码芯片运算过程中执行时间信息的采集，结合密码算法的内部实现，证实了算法指令和执行时间存在相关性，从而推测出密钥信息。在Paul的基础上，Dhem等人将时间攻击方法成功地应用于破解RSA密码算法。

10.Y是无符号整型变量，请从代码大小、执行时间、完成功能等角度分析比较if(Y>1)和if(Y>=2)的异同。  
答：

（1）代码大小: Y>1的代码长度多余Y>=2， 因为Y>1要先判断大于，再判断不等于，而Y>=2只要直接判断大于等于即可。

（2）执行时间: Y>1用时更长，因为Y>=2可以直接通过psw位来进行比

较。

（3）完成功能：显而易见......

总的来说，总过程就是：先进行减法，然后先判断是否“>=0”，若是，psw=1；若不是还要判断是否“=”0

一般>=和<直接判PSW中的C标志就可以了；若判断>则先判断C标志，还要判断Z标志。<=等价于>

**三、论述题(共2小题，每题10分，共20分)**

1.什么是旁路攻击?抵御旁路攻击的软件方法有哪些?

旁路攻击 SCA（side channel attack），是指加密系统能够以各种形式泄漏信息，比如温度、声波、能量耗散、执行时间、电磁泄漏和光信号等，通过提取加密电路中的泄漏物理量，分析泄漏物理量变化规律来从而分析出密钥。

抵御旁路攻击的软件方法：数据冗余(数据单元/备份)；控制冗余(前序/入

口检查)；执行冗余(随机顺序/等价实现/随机延时功耗)；特定算法；软件陷阱；

SLEEP躲避。

软件防御技术关键是代码分块的粒度粗细和等价实现的数量

2.请说明COS设计中完工操作的作用和实现方法。（PPT没有，要改写）

完工操作作用：

当交给芯片厂商的时候，COS不是完整的。处理完毕后，厂商有必要下载和配置芯片以得到完整的COS。每个芯片厂商获得的只是芯片的部分信息，这样便可以有效防止COS被厂商仿制。

实现方法：

在交给芯片厂商时，COS被放在ROM空间里，但相关的函数命令的入口却被放在EEPROM中，并且其中的跳转表为空。待厂商处理完毕，芯片拿回后，再通过命令将下载的数据完整地填充在EEPROM跳转表中，如此就可以通过查询跳转来实现芯片正常功能。

**四、设计题**

用C语言设计一个去极值平均滤波算法的函数。

说明： a)接口自己定义；

b)请注意代码质量；

c)添加注释。

答：假设数据在数组uchar Data[18]中，选择18是因为去掉最大、最小还有16个数，可以避免做除法。代码如下：

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

函数名: .uchar AVR (void)

描 述: 去极值平均滤波算法函数，数据在数组uchar Data[18]中

输入值: 无

输出值: 无

返回值: 去极值平均值

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

.uchar AVR (void)// 去极值平均滤波算法函数

{

uchar \*p; //使用指针比数组快

uchar Temp ; //定义缓冲区，可以避免频繁进行数组或指针运算，

uchar Min = 0xff; //数值滤波最小值,初始化=0xff

uchar Max = 0; //数值滤波最大值,初始化=0x00

uint Sum = 0; //累加和,初始化=0x0000

for (p=&Data; p<(&Data+18); p++) {//滤波计算,数据数组Data[18]去极值平均

Temp = \*p; //取数据

Sum += Temp; //计算数值累加和

if (Temp < Min ){ //比较，求最小值

Min = Temp;

}

else {

if (Temp >= Max ) { //比较，求最大值

Max = Temp;

}

}

}

Sum -= Max + Min; //累加和去除最大和最小值

return( Sum >> 4); //返回16次的平均值

}

滑动滤波参考：

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
函数名: .uchar AVR (void)  
描  述: 滑动平均滤波法，数据存放在uchar Data[16]，Data数组当作一个队列，Data[0]是队首，先出。  
输入值: 数组的首地址指针Data  
输出值: 无  
返回值: 滑动平均值  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/  
#define N 16  
.uchar  AVR (uchar \*data)// 滑动平均滤波函数  
{  
uchar  \*q; //循环求和的指针  
uchar  \*New\_value=&data; //新的值,使用指针更快  
uchar i=0; //计数器  
uint  Sum = 0; //累加和,初始化=0x0000  
for(;;){  
\*New\_value= get\_ad();  //获取新值  
i+=1; //计数器加1  
\*New\_value++; //指针后移，指向Data的下一个位置  
if(i>=N){ //如果队列满了，就重置  
p=&data;  
i=0;  
}  
  
for (q=&data; q<(&data+18); q++){ //滤波计算,数据数组Data[18]去极值平均  
Sum  += \*q;   //计算数值累加和  
}  
return( Sum >> 4); //返回滑动滤波的16次的平均值  
}

<https://blog.csdn.net/weixin_42019584/article/details/80142292>

**2016级嵌入式：**

**一、改错题(共5小题，每小题3分，共15分)**

1. ARM TrustZone技术是系统范围的安全方法

对

2.旁道攻击是一种针对密码系统实现上的物理攻击方式。但它既没有系统的攻击方式，也没有系统的解决方法。

对

3.在嵌入式系统设计中嵌入式操作系统是必需的。

错，不是必需的。

4. SPI总线对于不同的串行接口外围芯片，它们的时钟时序是不同的。

对

5. COS命令APDU包含一个必备的命令头。其中关于命令是否密文传输由INS说明。

错误，INS是指令类型，由CLA说明。（没明说，不太确定）

**二、简答题(共10小题，每小题5分，共50分。回答简明扼要）**

1.简述嵌入式系统的特点。

答：

面向特定应用、软/硬件可裁剪、低功耗、低成本、体积受限、实时性、较长的生命周期、本身不具备自主开发能力，需特定开发工具（仿真机、开发器）。

3.嵌入式系统由哪四个部分组成?

答：

嵌入式微处理器、外围支撑硬件、嵌入式实时操作系统（或调度器）以及用户应用软件四个部分组成。

4. 电磁兼容性包含的两个要素是什么?

答：

①能在一定的干扰环境下工作； 有很多量化的指标，抗雷击。。。 ②不产生不可容忍的干扰。

5.软实时系统和硬实时系统的区别是什么?

答：

软实时系统：各个任务运行得越快越好，并不要求限定某一任务必须在多长时间内完成。

硬实时系统：各任务不仅要执行无误而且要做到准时

6.为什么在设计串口异步通信电路时必须使用外部晶体振荡器?

答：

计算机的整个工作是在时钟信号的驱动下，按照严格的时序有规律地一个节拍一个节拍地执行各种操作。单片机内部设计有定时电路，只需外接振荡元件即可工作。

7. 简述WDT看门狗的原理及对嵌入式系统可靠性的作用。

答：

原理：

设一系统程序完整运行一周期的时间是Tp，看门狗的定时周期为Ti，要求Ti>Tp。在程序运行一周期后，修改定时器的计数值，只要程序正常运行，定时器就不会溢出。若由于干扰等原因使系统不能在Tp时刻修改定时器的计数值，定时器将在Ti 时刻溢出，引发系统复位，使系统得以重新运行，从而起到监控作用。

当嵌入式系统运行时受到外部干扰或者系统错误，程序有时会出现“跑飞”，导致整个系统瘫痪。在对系统稳定性要求较高的场合，为了防止这一现象的发生，需要一种叫“看门狗”(Watchdog)的电路。看门狗的作用就是当系统“跑飞”而进入死循环时，恢复系统的运行。

看门狗：是一种电路，具有监视并恢复程序 正常运行的功能。它是一定时器电路。

9.评估实时操作系统实时性能的三个重要时间是什么?

系统响应时间：系统发出处理要求到系统给出应答信号的时间。

任务切换时间：任务之间切换而使用的时间。

中断延迟：硬件接收到中断信号到操作系统作出响应，并转入中断服务程序的时间。

10.提高输入和输出信号可靠性的软件方法是什么?

答：（6.4 PPT24）

输入：

周期性重复配置，不同内容放在不同block

周期性输入与滤波（例如程序判断、算术平均、加权平均、去极值算术平均、低通/高通/带通滤波）

输入部件寿命管理（例如按键次数）

时间限制（超时处理）与延时（绝对时间与相对时间）

输出：

内存可靠性高于端口，利用端口数据备份周期性刷新内容与配置（注意：内容在前）

输出部件寿命管理（例如LED、马达、喇叭）

输出与反馈

时间限制（超时处理）与延时（绝对时间与相对时间）

**三、论述题(共2小题，每题10分，共20分**

1.什么是实现攻击?抵御实现攻击的软件方法有哪些?

实现攻击：加密算法的实现电路经常会泄漏一些有用信息，这些信息能够被用来分析加密算法的敏感数据或密钥，这即是实现攻击。实现攻击可分为主动式攻击（失效分析攻击）和被动式攻击（旁路攻击）

抵御实现攻击的软件方法：

（1）数据冗余；

（2）控制冗余；

（3）执行冗余；

（4）特定算法；

（5）软件陷阱；

（6）SLEEP躲避

1. 工业控制系统有何特点?实现工控系统安全理念有哪些?国际上两种不同的工控系统信息安全解决方案是什么?

工业控制系统特点：

（1）实时性要求高，强调实时I/O能力；

（2）可用性要求高，系统一旦上线，不能接受重新启动之类的响应，中断停机必须有计划（例检修）；

（3）工控硬件要求寿命长、可靠性高，防电磁干扰，防爆，防尘等要求非常严格；

（4）特有的工业控制协议通讯协议，不同厂商控制设备采用不同通信协议，很多协议不公开；

（5）工控系统上线生产后，一般不会调整；

（6）工控系统要求封闭性比较强

实现工控系统安全理念：白名单、层次化、边缘化、透明化

国际上两种不同的工控系统信息安全解决方案：

主动隔离式解决方案：即相同功能和安全要求的设备放在同一区域内，区域间通信靠专有管道执行，通过对管道的管理来阻挡非法通信，保护网络区域及其中的设备。其典型代表是加拿大 Byres Security 公司推出的 Tofino 工控系统信息安全解决方案。

被动检测式解决方案：被动检测式解决方案延续了IT系统的网络安全防护策略。由于IT系统具有结构、程序、通信多变的特点，所以除了身份认证、数据加密等技术以外，多采用病毒查杀、入侵检测等黑名单匹配的方式确定非法身份，通过多层次的部署来加强网络信息安全。其典型代表是美国Industrial De-fender公司的工控系统信息安全解决方案。

**2016级下学期：**

**一、判断题**

1.在小端存储模式下存储32位数1234567H到2000:200四字节单元中，200单元的数值为0x70.

错，67H  
2.uC0S-11操作系统是不可剥夺型内核。

错，商业cos几乎没有不可剥夺的内核  
3.SPI总线是异步通信总线。

错，同步通信  
4.YAFFS文件系统是为NOR FLASH量身定做的。

错，专为NAND Flash设计的  
5.C0S命令APDU包含一个必备的命令头。其中关于命令是否密文传输由P2说明。

错，CLA  
  
**二、简答题(共10小题，每小题5分。共50分。回答简明抓要.)**1.从应用的角度可将嵌入式微处理器分成哪几类?

答：

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）。

3.比较CISC与RISC指令系统之间的主要差异。

答：

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。

4.嵌入式系统硬件通常包含有哪些电路模块

答：

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。

外围硬件设备：以嵌入式微处理器为中心，包括电源、时钟、复位、输入输出及驱动、存储、等其他电路模块 。

6.嵌入式操作系统内核的主要工作是什么?

答：

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)。

多任务系统中，内核负责管理任务，或者说为任务分配CPU时间，并且负责任务之间的通讯。

内核的基本服务是任务切换。之所以使用实时内核可以大大简化应用系统的设计，是因为实时内核允许将应用分成若干个任务，由实时内核来管理它们。

调度（Scheduler、dispatcher）也是内核的主要职责之一，就是要决定该轮到哪个任务运行了。多数实时内核是基于优先级调度法的。每个任务根据其重要程度的不同被赋予一定的优先级。

10.请说明嵌入式芯片引脚配置为推挽输出和0D开漏输出的差别及对可靠性的影响。

答：

0C/OD不需要输出高电平，需要外部上拉电阻，可以通过控制外部上拉电阻电流来控制，电路不容易损坏，通常用于电路板之间的连接，而推挽输出通常用于板内。推挽输出的高低电平都有信号驱动，适合比较高的时钟频率（上课讲的）。