

目录

嵌入式系统概论	3
1 嵌入式系统简介	4
1.1 嵌入式系统的定义	5
三要素	6
特征	7
与常见计算机系统的区别	8
1.2 嵌入式系统的组成	9
嵌入式微处理器	10
电磁兼容性	11
嵌入式微处理器的体系结构	12
嵌入式微处理器指令系统	13
外围硬件设备	16
ROM/Flash/OTP/E2PROM	17
嵌入式操作系统	18
应用软件	19
1.3 嵌入式系统的应用与发展	20
结论	29
2 嵌入式微处理器	30
2.1 嵌入式微处理器分类	31
嵌入式微处理器 EMPU	32
嵌入式微控制器 MCU	33
嵌入式DSP处理器	34
嵌入式片上系统 SoC	35
2.2 ARM嵌入式微处理器	36
应用领域	37
特点	38
ARM的几种系列	40
ARM微处理器内核的选择	44
2.3 嵌入式CPU架构	45
DSP、MCU和MPU	45
2.3.1 冯诺依曼结构	46
2.3.2 哈佛结构	47
2.3.3 改进的哈佛结构	50

2.3.4 处理器结构小结	51
3 嵌入式操作系统	53
4 嵌入式系统安全简介	54
嵌入式系统安全事件频发	54
嵌入式系统攻击分类	63
根据攻击对象分类	63
根据发起攻击的代理工具或手段分类	64
软件增强	65
硬件增强	66
架构设计增强	68

目录

80C51单片机	4
1 80C51 逻辑结构	5
微型计算机的基本组成	6
80C51单片机基本结构	7
80C51逻辑结构及信号引脚	8
80C51单片机内部结构	9
1) CPU	9
控制器	9
运算器	15
2) 程序存储器	24
三种型号	24
3) 数据存储器 RAM	25
4) 并行I/O口	25
5) 串行I/O口	26
6) 定时器/计数器	26
7) 中断系统	27
8) 振荡器电路及元件	27
2 80C51信号引脚	28
80C51的封装	28
AT89C51和AT89C2051主要性能表	31
1) 电源和晶振	32
2) I/O 共4个口，32根I/O线	33
3) 控制线：共4根	35
3 80C51时钟电路、工作时序、工作方式	37
时钟电路作用及组成	37
振荡器及定时控制元件	38
内部时钟发生器	39
ALE信号	39
时序定时单位	40
1) 振荡周期/节拍P	41
2) 时钟周期/状态周期/状态S	41
3) 机器周期	41

4) 指令周期	42
指令时序	43
单字节、双字节和三字节指令	43
1) 单机器周期指令	43
2) 双机器周期指令	44
访问外部ROM和RAM的时序	47
80C51工作方式	49
80C51复位	50
80C51 程序执行	55
80C51低功耗工作方式	56
80C51 编程工作方式(烧录)	57
1) 闪速存储器编程	58
80C51 布尔(位)处理器	65
4 80C51存储器结构与地址空间	66
4个存储器空间	66
三种基本寻址空间	67
80C51程序存储器	68
80C51片内数据存储器	70
片内数据RAM区	72
工作寄存器区	72
位寻址区	73
字节寻址区	74
堆栈区	74
特殊功能寄存器SFR区	75
80C51片外数据存储器	78
5、80C51 总线、接口与扩展	79
80C51系统总线	79
地址总线	79
数据总线	80
控制总线	80
并行输入/输出端口	83
P0□	83
P1□	89
P2□	97

目录

PIC MCU	4
1 PIC16F_LF722A_723A高性能 RISC CPU	5
2 PIC16F_LF722A_723A特性	6
高精度内部振荡器	6
模拟特性	8
外设特性	9
引脚	9
Timer0	10
增强型 Timer1	10
Timer2	11
资源	13
封装	14
引脚说明	16
结构框图	17
存储器	18
程序存储器构成	18
程序存储器分页	19
数据存储器构成	20
寄存器	22
间接寻址、INDF 和FSR 寄存器	22
STATUS 寄存器	23
OPTION 寄存器	24
电源控制 (PCON) 寄存器	25
程序计数器PC	26
堆栈	27
片上复位电路的简化框图	28
复位	29
MCLR复位	32
上电复位 (POR)	33
上电延时定时器 (PWRT)	34
看门狗定时器 (WDT)	35
欠压复位 (BOR)	37
超时序列	39

中断	43
中断工作原理	45
中断响应延时	46
休眠期间的中断	47
外部中断INT	48
中断现场保护	49
INTCON：中断控制寄存器	50
PIE1 寄存器包含中断允许位	51
PIE2 寄存器包含中断允许位	52
PIR1 寄存器	53
PIR2 寄存器	54
低压差（LDO）稳压器	55
I/O 端口	56
PORT A	57
-PORT B	65
PORT C	73
PORT E	82
振荡器模块	84
频率选择位（IRCF）	85
振荡器控制	86
振荡器调节	86
振荡器起振定时器（OST）	87
外部时钟EC 模式	89
石英晶振工作原理（LP、XT 和HS 模式	90
器件配置	93
CONFIG1：配置字寄存器1	94
CONFIG2：配置字寄存器2	95
模数转换器	96
Timer0	97
带门控的 TIMER1	98
TIMER2	99
电容触摸传感	100
可寻址通用同步异步收发	101
同步串行端口（SSP）模	102

目录

ARM 架构	5
1、ARM 体系结构	6
1 ARM嵌入式微处理器	7
命名规则	7
ARM 变种	9
T变种(Thumb指令集)	9
M变种(长乘法指令)	10
E变种(增强型DSP指令)	11
J变种(Java加速器Jazelle)	12
SIMD*变种(ARM媒体功能扩展)	13
ARM架构变种对比	14
ARMv4T结构	15
ARMv6架构	15
ARMv7架构	16
ARM7的三级流水线	18
ARM9 五级流水线	19
AMBA(Advanced Microcontroller Bus Architecture)总线体系结构	20
ARM9 E-S内核	21
Thumb指令集	22
ARM工作模式	24
内部寄存器	28
通用寄存器	30
程序状态寄存器	34
Thumb寄存器	39
异常	41
异常的类型及向量地址	42
进入和退出异常	46
存储器组织结构	50
大端存储和小端存储	50
I/O端口和存储器统一编址	53
2、ARM 存储器	54
2.1 存储器概述	55

分类：主存储器和辅存储器	56
分类：内存、外存	57
主存储器的分类	58
ROM分类	60
ROM优缺点	61
Compact Flash,CF卡	63
Secure Digital Card, SD卡	64
RAM优缺点	66
存储系统的层次结构	68
SRAM和DRAM	70
NAND Flash	71
2.2 存储系统机制	73
存储器接口方式	74
SRAM型的全地址/数据总线接口	74
DRAM型动态存储器接口	74
串行存储器接口	74
高速缓存机制	75
存储管理单元MMU	77
分页虚拟存储管理	79
3、ARM 时钟及电源管理（以S3C2410为例）	80
3.1 S3C2410时钟结构	80
时钟控制	81
USB控制	81
电源控制	81
3.2 S3C2410电源管理模式	84
1.空闲模式(IDLE Mode)	85
2 .正常模式(NORMAL Mode)	85
3 .低速模式(SLOW Mode)	85
4 .休眠/掉电模式(POWER-OFF Mode)	85
时钟分配	86
电源管理模式转换	87
各种模式下时钟和电源状态	88
4种模式对比	89
3.3 常用单元电路设计	90

电源电路设计	90
晶振电路设计	93
4、ARM 定时技术	94
4.1 定时器工作原理	94
4.2 S3C2410看门狗定时器	96
看门狗概念	96
功能	98
组成	100
工作原理	100
初始化	101
工作原理	102
4.3 S3C2410 RTC部件（实时时钟）	103
定义、功能、应用	103
特点	104
振荡电路	105
可能会引起的显示错误	107
报警功能	108
时间片中断	109
4.4 S3C2410 Timer部件及PWM	110
功能、应用	110
主要特性	111
PWM(脉宽调制)概念	112
定时器结构	113
工作原理	115
定时器工作过程	115
初值自动重装、手动装载和双缓冲	116
PWM输出	117
死区发生器	118
DMA请求模式	119
计数时钟和输出计算	120
定时器最大、最小输出周期	121
5、ARM 中断	122
5.1 中断概述	122
微处理器与外设间数据传送方式简介	123
中断概念、功能、与查询的对比	126

优点	127
中断向量	128
中断响应的一般过程	129
中断方式控制的I/O操作步骤	130
5.2 S3C2410中断系统	131
S3C2410中断控制器	132
中断仲裁	132
S3C2410中断处理流程	133
ARM系统的中断处理	134
S3C2410的中断控制器	136
中断屏蔽寄存器	137
中断请求	138
仲裁器	139
5.3 IRQ和FIQ异常中断处理	140
FIQ异常中断	141
用户自定义中断向量表	143
6、ARM DMA	143
6.1 DMA 概述	144
概念、特点	145
DMA传送过程	146
6.2 S3C2410 DMA	147
S3C2410芯片的DMA系统	148
DMA请求源	149
DMA的工作过程	150

目录

嵌入式接口技术—通信	3
硬件-通信(相互通道)	5
UART 串行通信协议基础知识	6
串行通信的特点	6
1) 数据通信方式	7
单工通信	7
半双工通信	7
全双工通信	7
2) 串行通信方式	9
异步通信方式	9
同步串行通信方式	10
3) 串行通信协议	11
异步协议	11
同步协议	14
4) 信息的校验方式	15
5) 波特率	15
6) 信号的调制与解调	16
串行接口基本功能	19
异步串行通信接口基本结构	20
异步串行通信常见的错误	21
RS - 232C串行接口标准	22
接口信号功能	25
信号线的连接	27
RS-232-C接口标准的缺点	29
RS-485标准	30
电气特性	30
平衡发送和差分接收	32
通信距离	32
注意事项	33
串行通信协议应用注意事项	36
I2C 总线	37
概念、优点	38
I2C总线系统组成	39

I2C总线的状态和信号	41
I2C总线基本操作	45
启动和停止条件	47
I2C总线数据传输格式	48
标准模式I2C 总线规范的扩展	50
I2C应用注意事项	51
SPI 串行外设接口总线	53
概念、优点	53
SPI 总线系统的组成	54
SPI 总线时序、特性	55
用GPIO口线模拟SPI 操作	56
SPI 注意事项	57
1-WIRE(单总线)	58
处理流程	61
初始化	62
1-Wire ROM 功能命令	62
Read ROM 读取的8位家族码、唯一的48位序列码和8位CRC 码	62
Match ROM 64 位ROM 码	62
Search ROM [F0h]	63
Skip ROM [CCh]	64
Resume [A5h]	65
Overdrive Skip ROM [3Ch]	66
Overdrive Match ROM [69h]	67

目录

嵌入式接口技术-人机界面（HMI）	2
按键	4
独立式键盘	5
矩阵式键盘	6
AD键盘	7
常用按键种类	8
电容式触摸按键	9
摇杆	10
七段/米字/点阵数码管/灯带	11
数码管显示	12
数码管静态显示	13
数码管动态显示	14
LED驱动	15
多色LED控制	16
蜂鸣器buzzer	18
定义	18
分类	18
蜂鸣器驱动电路	19
蜂鸣器的选用	21
其他发声方式	22
编码器	20
编码器图片	22
增量式编码器	24
如何判断方向及计数	26
绝对式编码器	27
编码器接口举例	29
其他通信显示（I2C/SPI/UART）	30

目录

嵌入式接口技术-功率驱动	2
常用功率驱动器件	3
功率晶体管	4
场效应管	5
晶闸管	6
继电器	8
继电器作用	9
电磁继电器	10
磁保持继电器	14
固态继电器	16
固态继电器组成与分类	17
电磁铁/电磁阀	18
马达/电动阀	19
步进电机	20
BLDC马达	23
舵机	25

目录

1 嵌入式操作系统简介	4
MCU生态体系	4
1. 芯片硬件设计	5
2. 工具链	7
3. SDK	8
4. 高级开发工具	9
5. OS	10
6. 解决方案	11
7. 校园计划	12
8. 联盟	13
9. 兼容stm32	13
实时多任务操作系统与分时多任务操作系统	14
时钟节拍	16
实时操作系统中的重要概念	17
多处理器结构	18
智能手机操作系统	20
2 μ C/OS	21
前后台系统	22
μ C/OS-II	24
3 VxWorks	26
VxWorks概述	27
VxWorks基本特征	28
高实时性、高稳定性的微内核	28
丰富的外挂组件模块	30
可裁减性	31
对多种硬件平台的可移植性	32
友好、开放的集成开发环境	33
4 嵌入式Linux	34
Linux的版本	35
典型的嵌入式Linux	36
嵌入式Linux种类	37
RT-Linux	38

uClinux	43
嵌入式Linux的组成	46
Linux启动	48
嵌入式linux bootloader	50
嵌入式系统的存储	51
文件系统类型	51
日志文件系统	52
YAFFS文件系统	53
YAFFS和JFFS的相同点与不同点	54
X Window	55
面向嵌入式Linux 系统的图形用户界面	57
嵌入式Linux-Android	58

目录

芯片操作系统(COS)	4
COS的发展过程	5
COS的基本特点	6
COS的基本任务	7
COS要解决的三个问题	8
文件操作	8
鉴别与核实	7
安全体系	7
安全状态	9
安全属性	10
文件安全属性	11
命令安全属性	12
内部认证	13
外部认证	14
MAC/TAC校验	15
COS的四个模块	16
COS程序结构	18
COS文件系统	20
COS数据传输	29
物理层	30
异步传输的ATR	31
协议参数选择	36
T=0 异步半双工字符传输协议	43
T=1异步半双工分组传输协议	44
COS命令集	45
COS实现举例介绍	46
文件的逻辑结构	47
文件描述块(文件头16B)	51
文件体	68
与文件操作相关的命令	79
与生命周期维护相关的命令	81

目录

嵌入式软件设计	2
嵌入式软件架构与层次	4
代码优化	5
充分利用硬件	6
变量类型	7
算法优化	8
适当的使用宏提高程序的时间效率	9
内嵌汇编	10
提高循环语言的效率	11
提高 switch 语句的效率	12
其他语句	12
函数优化	14
变量	15
尽量避免使用标准库	16
采用数学方法优化程序	17
存储器分配	18
嵌入式代码优化是平衡艺术	19
代码可靠性	20
程序存储器	21
RAM	23
EEPROM/FLASH	24
输入	25
输出	26
通信	27
嵌入式软件可维护性	27

目录

旁路攻击 SCA 及防御	3
密码攻击	4
数学攻击	5
实体攻击	6
微探针技术	7
版图重构	8
实现攻击	9
主动式攻击（失效分析攻击）	11
干扰攻击	13
电涌攻击	15
电磁攻击	16
光攻击	19
热攻击	22
射线攻击	23
被动式攻击（旁路攻击SCA）	24
条件	28
攻击过程	28
机理	29
CMOS电路的瞬间物理功耗模型	30
旁路攻击原理	32
旁路攻击分类	33
时间攻击	34
故障攻击	35
功耗攻击	36
电磁攻击	37
声音攻击	38
可见光攻击	39
组合分析攻击	40
旁路攻击分析技术	41
对旁路攻击的防御技术	42
已有的抗攻击研究	43
算法级	43
电路级	44
软件算法抗攻击研究	45

对旁路攻击的硬件防御技术	46
反向调节技术	47
乱序技术	48
间接供应电源技术	49
并行处理器技术	50
异步电路技术	51
冗余编码技术	52
掩码技术	53
对旁路攻击的硬件防御方法	54
对旁路攻击的软件防御技术	56
数据冗余	57
控制冗余	58
执行冗余	59
对旁路攻击的软件防御实现方法	60

目录

工业控制系统信息安全	3
1 工控系统安全介绍	4
工业控制系统ICS的基本概念	5
可编程逻辑控制器(PLC)	6
监控和数据采集(SCADA)系统	7
分布式控制系统 (DCS)	8
工业控制系统特点	8
工业控制系统功能层次	10
2 工控系统安全威胁	12
Stuxnet震网病毒	13
工业控制系统安全事件-能源	19
工业控制系统安全事件-水处理	20
工业控制系统安全事件-交通	21
工业控制系统安全事件-制造	24
工业控制系统安全事件	25
工控系统的脆弱性	28
工控系统面临的威胁	34
安全标准与动态	37
工控安全动态	38
3 工控系统安全理念	40
工控系统安全-白名单	41
工控系统安全-层次化	42
工控系统安全-边缘化	43
工控系统安全-透明化	44
4 工控系统安全策略	45
工控系统安全解决方案思路	45
工控系统安全防护	47
工控系统安全加固	49
工控系统安全监控	51
工控系统安全解决方案整体框架	54
解决方案解决的主要问题	55
国外工控系统安全解决方案	56
主动隔离式解决方案	56

Tofino 工控系统信息安全解决方案	58
被动隔离式解决方案	61
Industrial De-fender 解决方案	62
主动隔离与被动隔离式解决方案比较	66
国内工控系统信息安全解决方案	67

目录

TrustZone技术	3
1、 TrustZone技术简介	4
1.1TrustZone技术背景	5
1.2TrustZone概述	7
什么是TrustZone？	7
为什么选择TrustZone技术？	8
2、 TrustZone技术安全实现与应用	9
2.1TrustZone技术的硬件架构	10
从硬件架构角度看	10
好处	12
监控模式	13
安全中断	15
从数据存储的角度看	17
硬件安全扩展	21
2.2TrustZone技术的软件架构	23
TrustZone安全启动顺序	24
2.3TrustZone技术实现机制与实现方式	25
TrustZone完整性安全策略	25
2.4TrustZone应用	26
3 基于ARM Trustzone的STPM	30
3.1.1 背景——移动终端面临的安全问题	31
3.1.2 方案	32
采用STPM的缺点	32
引入Trustzone	33
Trustzone实现	34
基于Trustzone的STPM	35
3.2.1 总体思路	36
01 物理TPM调用	36
02 Trustzone架构	37
03 整体架构	38
04 sTPM与TSS	39
系统整体架构	40

Tofino 工控系统信息安全解决方案	58
被动隔离式解决方案	61
Industrial De-fender 解决方案	62
主动隔离与被动隔离式解决方案比较	66
国内工控系统信息安全解决方案	67