8051处理器

武汉大学国家网络安全学院
丁玉龙 涂航

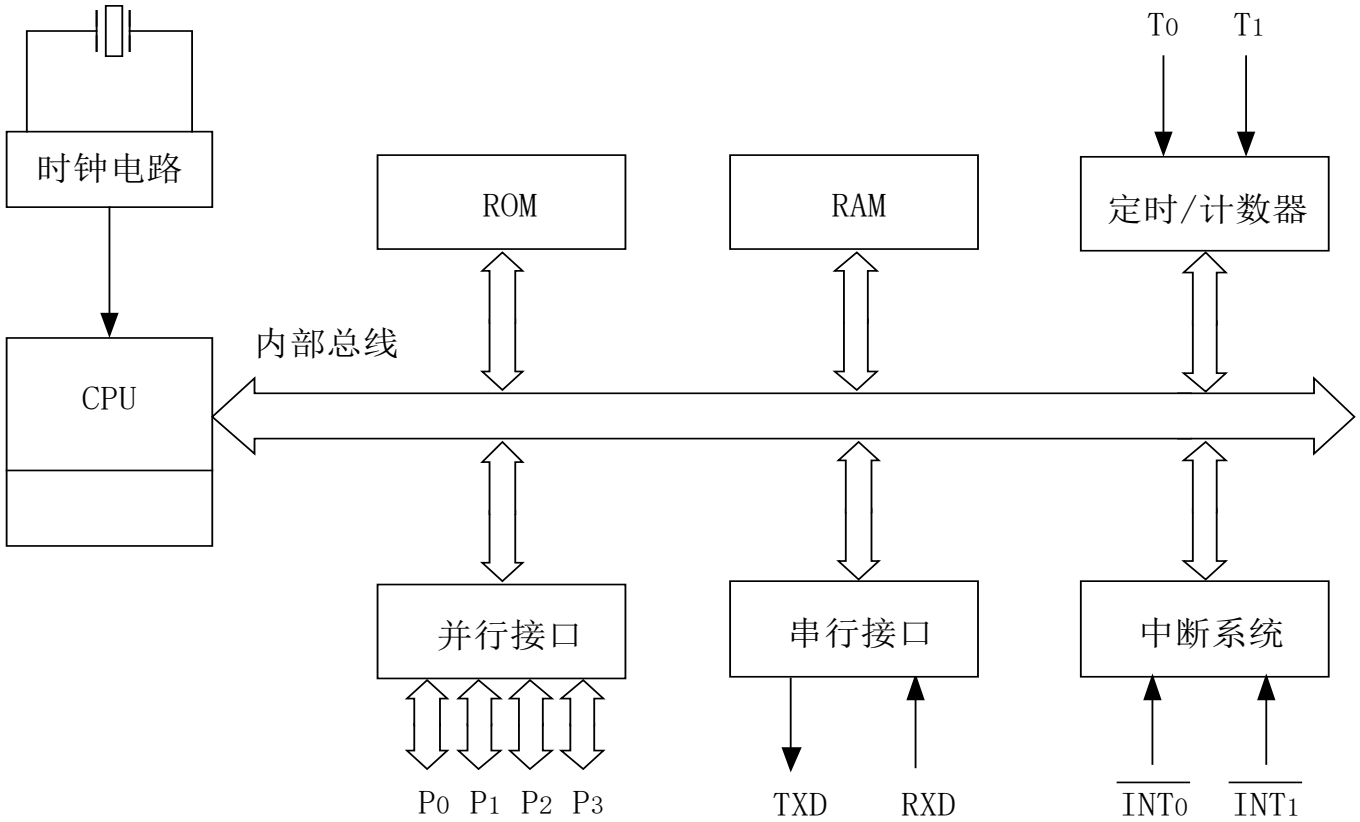
2024

内容提要

1	80C51 逻辑结构
2	80C51 单片机的信号引脚
3	80C51 时钟电路、工作时序、
4	80C51 工作方式
5	80C51 存储器结构与地址空间
6	80C51 总线、接口与扩展

80C51逻辑结构

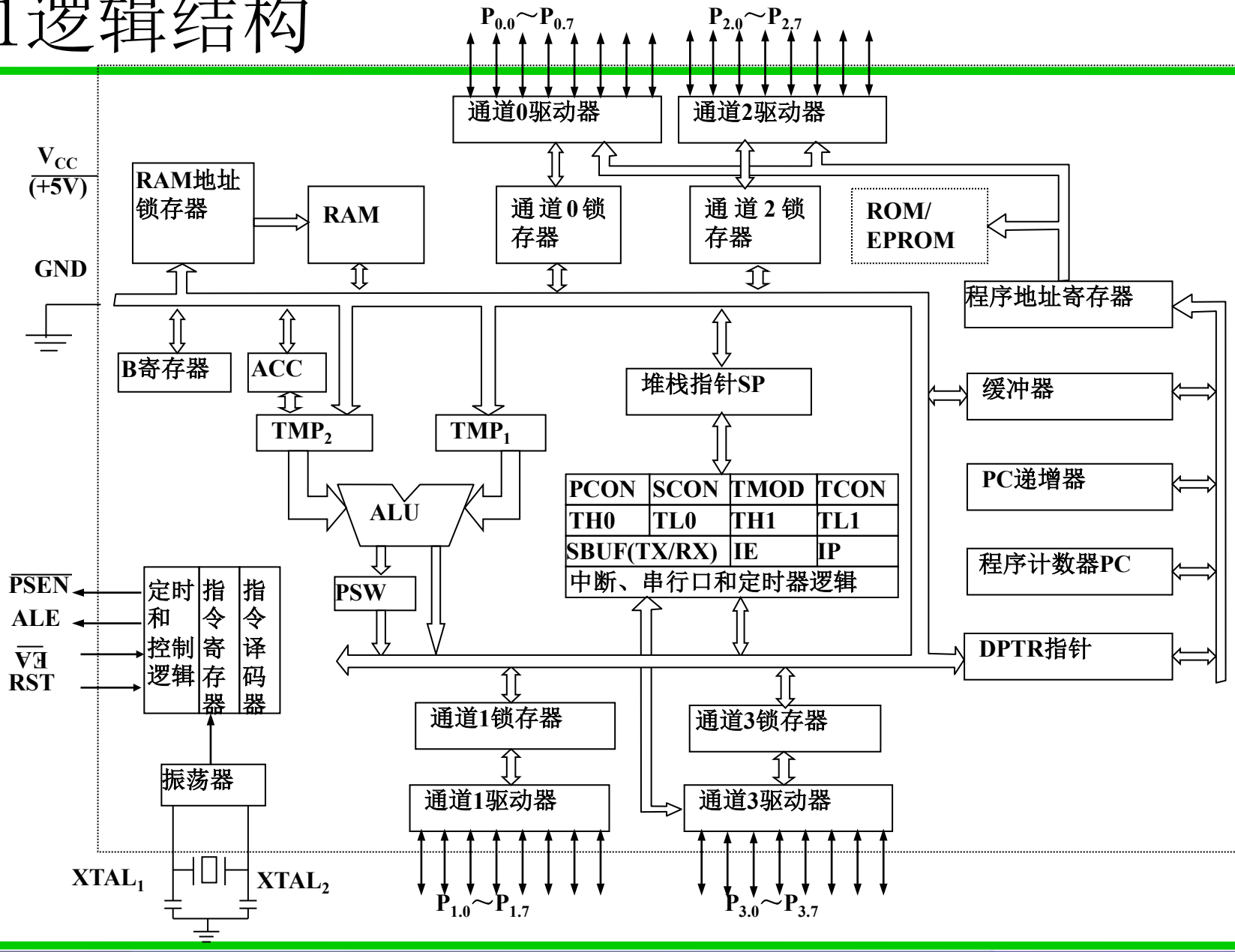
- 基本组成：中央处理器CPU +存储器+输入/输出 。
- 80C51基本结构框图



80C51逻辑结构（续）

- 80C51基本结构
  - （1）8位微处理器；
  - （2）数据存储器RAM（128B）和特殊功能寄存器SFR；
  - （3）内部程序存储器ROM（4KB）；
  - （4）2个16位定时/计数器T0和 T1；
  - （5）4个8位双向可编程GPIO，并行端口P0~P3；
  - （6）1个UART串行端口；
  - （7）中断控制系统；
  - （8）内部时钟电路；

80C51逻辑结构


P0.0～P0.7
P2.0～P2.7
通道0驱动器
通道2驱动器
VCC
(+5V)
GND
RAM地址锁存器
RAM
通道0锁存器
通道2锁存器
ROM/EPROM
程序地址寄存器
B寄存器
ACC
TMP2
TMP1
堆栈指针SP
缓冲器
PCON
SCON
TMOD
TCON
TH0
TL0
TH1
TL1
SBUF(TX/RX)
IE
IP
中断、串行口和定时器逻辑
ALU
PC递增器
PSW
程序计数器PC
PSEN
ALE
EA
RST
定时和控制逻辑
指令寄存器
指令译码器
DPTR指针
通道1锁存器
通道3锁存器
振荡器
通道1驱动器
通道3驱动器
XTAL1
XTAL2
P1.0～P1.7
P3.0～P3.7

80C51逻辑结构（续）

- 80C51内部结构
  - 1）CPU主要包括控制器、运算器和工作寄存器及时序电路
    - （1）控制器电路：识别指令，并根据指令性质控制计算机各组成部件进行工作的部件，与运算器一起构成中央处理器。在80C51中，控制器包括：
    - 程序计数器PC(Program Counter)
    - 程序地址寄存器
    - 指令寄存器IR
    - 指令译码器ID
    - 条件转移逻辑电路
    - 定时控制逻辑电路等

80C51逻辑结构（续）

- 执行指令是在控制电路的控制下进行的，执行一条指令的大致过程：

读出指令->指令寄存器->指令译码器(译码)->定时与控制逻辑电路（由控制定时逻辑电路产生各种定时信和控制信号，然后送往系统各部件去进行相应的操作）

1 80C51逻辑结构（续）

- 80C51内部结构
  - 1）CPU ---（1）控制器电路（续）
    - 程序计数器PC。存放的是下条指令的地址。
      - 其基本的工作过程是：读指令时，程序计数器PC将其中的数作为所取指令的地址输出给程序存储器，然后程序存储器按此地址输出指令字节，同时程序计数器PC本身自动加1，指向下一条指令地址。
      - 程序计数器PC变化的轨迹决定程序的流程。
      - 在执行条件转移或无条件转移指令时，程序计数器将被置入转移的目的地址，程序的流向发生变化。
      - 在执行调用指令或响应中断时，将子程序的入口地址或者中断向量地址送入PC，程序流向发生变化

80C51逻辑结构（续）

- 80C51内部结构
  - 1）CPU ---（1）控制器电路（续）
    - 数据指针 DPTR，一个16位的特殊功能寄存器，主要功能是作为片外数据存储器或I/O寻址用的地址寄存器（间接寻址），也可以作为两个8位寄存器处理，其高8位用DPH表示，低8位用DPL表示
      - 访问片外数据存储器或I/O的指令为：

```
MOVX   A，@DPTR      ；读
MOVX   @DPTR，A      ；写
```

      - DPTR寄存器也可以作为访问程序存储器时的基址寄存器。这时寻址程序存储器中的表格、常数等单元，不是寻址指令

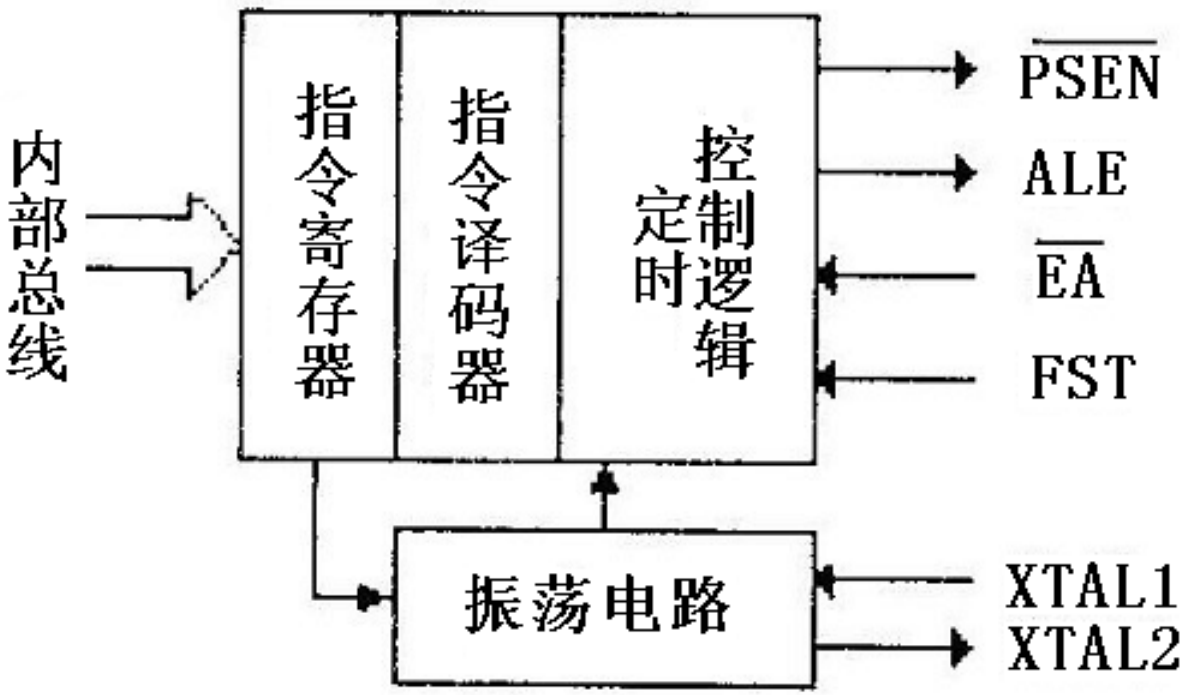
```
MOVC   A，@A＋DPTR
JMP    @A＋DPTR
```

80C51逻辑结构（续）

- 80C51内部结构
  - 1）CPU ---（1）控制器电路（续）
    - 指令寄存器IR、指令译码器及定时控制逻辑
      - 指令寄存器IR是用来存放指令操作码的专用寄存器。执行程序时，首先进行程序存储器的读操作，也就是根据**程序计数器**给出的地址从程序存储器中**取指令**，送指令寄存器**IR**，IR的输出送**指令译码器**；然后由指令译码器对该指令进行译码，译码结果送**定时控制逻辑电路**
      - 定时控制逻辑电路则根据指令的性质发出一系列定时控制信号，控制计算机的各组成部件进行相应的工作
      - 条件转移逻辑电路主要用来控制程序的分支转移。在80C51中，转移条件也可分为两部分，一部分是内部条件,即程序状态标志位（PSW）和累加器的零状态；另一部分是外部条件，即F0和所有~~位寻址~~空间的状态

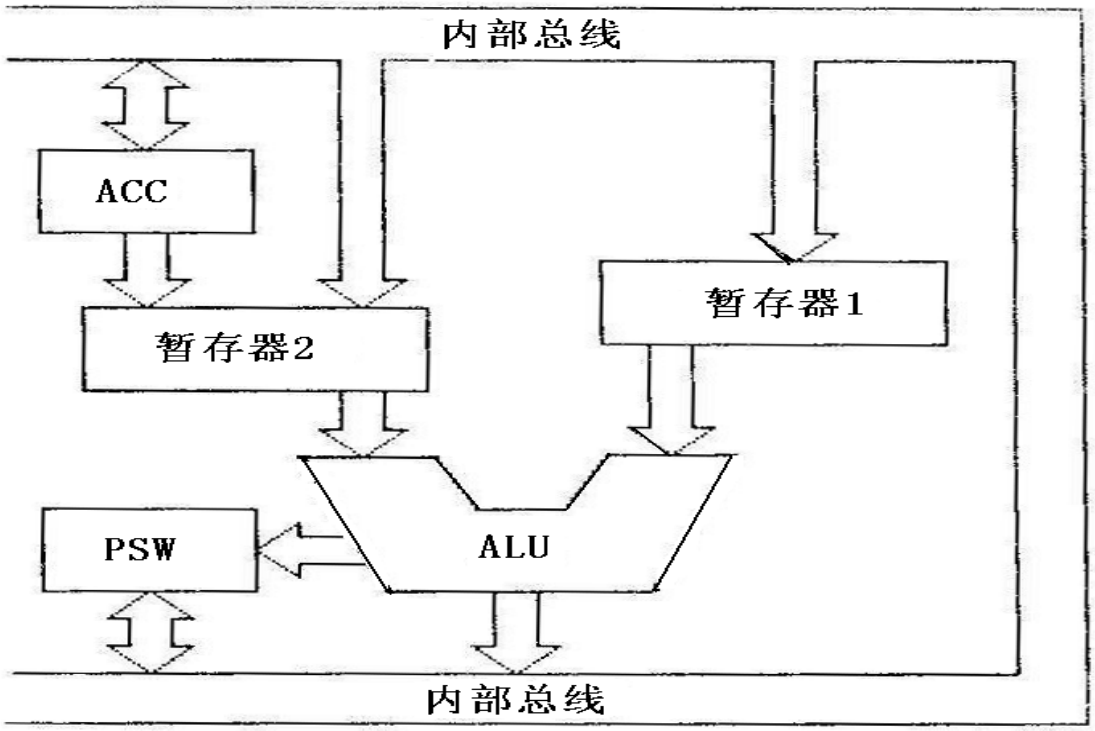
80C51逻辑结构（续）

- 80C51内部结构
  - ◆ 1）CPU ---（1）控制器电路（续）
    - ● 指令寄存器IR、指令译码器及定时控制逻辑（续）



80C51逻辑结构（续）

- 80C51内部结构
  - 1）CPU ---（2）运算器电路 包括：**ALU**(Arithmetic Logic Unit)、ACC（Accumulator 累加器）、**B寄存器、程序状态字PSW**(Program Status Word)、**TEMP1和TEMP2**两个暂存器等



80C51逻辑结构（续）

- 80C51内部结构
  - 1）CPU ---（2）运算器电路（续）
    - **ALU有两个输入**
      - 通过暂存器1的输入：输入数据来自**寄存器、直接寻址单元（含I/O口）、内部RAM、寄存器B或是立即数**
      - 通过**暂存器 2或累加器 ACC的输入**：通过暂存器 2的运算的指令有

        ANL A, #data; AND data to A

        ORL A, #data

        XRL A, #data
    - **ALU有两个输出**
      - 数据经过运算后，其结果又通过内部总线送回到累加器中
      - 数据运算后产生的标志位输出至程序状态字 PSW

80C51逻辑结构（续）

- 80C51内部结构
- 1）CPU ---（2）运算器电路（续）
- 累加器A
- 累加器A是CPU中使用最频繁的一个八位专用寄存器，简称ACC或A寄存器。主要功能：存放操作数，是ALU单元的输入之一，也是ALU运算结果的暂存单元
- 由于累加器的“ 瓶颈”作用制约着单片机运算速度的提高，人们又推出寄存器阵列来代替累加器，赋予更多寄存器以累加器功能，形成了多累加器结构

80C51逻辑结构（续）

- 80C51内部结构
  - ◆ 1）CPU ---（2）运算器电路（续）
    - ● 程序状态字PSW

CY	AC	F0	RS1	RS0	OV	—	P

      - 按位定义的8位寄存器，其内容主要部分是ALU的输出。其中有些位是根据指令执行结果，由**硬件自动生成**，而有些位状态可用软件方法设定。
      - 除PSW.1（**保留位**）、**RS1和RS0(工作寄存器组选择控制位)**及**用户标志F0**之外，其他四位：**奇偶校验位P**、**溢出标志位OV**、**辅助进位标志位AC**及**进位标志位CY**都是ALU运算结果的直接输出
      - 条件转移指令就是根据PSW中的相关标志位的状态实现程序的转移。它是一个程序可访问的寄存器，而且可以按位访问。

80C51逻辑结构（续）

- 80C51内部结构
  - 1）CPU ---（2）运算器电路（续）
    - 程序状态字PSW（续）

CY	AC	F0	RS1	RS0	OV	—	P

      - P （PSW．0）—奇偶标志位
      - 每个指令周期都由硬件来置位或清除。
      - 用以表示累加器A中值为1的个数的奇偶性：若累加器值为1的位数是奇数，P置位；否则P清除。
      - **在串行通信中，常以传送奇偶校验位来检验传输数据的可靠性**。通常将P置入串行帧中的奇偶校验位

80C51逻辑结构（续）

- 80C51内部结构
  - 1）CPU ---（2）运算器电路（续）
    - 程序状态字PSW（续）

CY	AC	F0	RS1	RS0	OV	—	P

      - OV （PSW．2）—溢出标志位
      - 当执行运算指令时，由硬件置位或清除，以指示运算是否产生溢出，OV置位表示运算结果超出了目的寄存器A所能表示的范围
      - 当位7向C进位(借位）时OV标志置位，表示带符号数运算时运算结果是错误的；否则，清除OV标志，运算结果正确

80C51逻辑结构（续）

- 80C51内部结构
  - ◆ 1）CPU ---（2）运算器电路（续）
    - ● 程序状态字PSW（续）

CY	AC	F0	RS1	RS0	OV	—	P

      - **OV （PSW．2）—溢出标志位**
      - 对**MUL乘法**，当A、B两个乘数的积超过255时OV置位；否则，OV＝0。因此，若OV＝0时，只需从A寄存器中取积；若OV＝1时，则需从B、A寄存器对中取积
      - **对DIV除法**，若除数为0时，OV=1；否则，OV=0

80C51逻辑结构（续）

- 80C51内部结构
  - ◆ 1）CPU ---（2）运算器电路（续）
    - ● 程序状态字PSW（续）

CY	AC	F0	RS1	RS0	OV	—	P

      - RS1、RS0 （PSW.4、PSW.3）—工作寄存器组选择位

        用于设定当前工作寄存器的组号

RS1	RS0	组号	R0～R7地址
0	0	0组	00H～07H
0	1	1组	08H～0FH
1	0	2组	10H～17H
1	1	3组	18H～1FH

80C51逻辑结构（续）

- 80C51内部结构
  - ◆ 1）CPU ---（2）运算器电路（续）
    - ● 程序状态字PSW（续）

CY	AC	F0	RS1	RS0	OV	—	P

- AC （PSW．6）—辅助进位标志位

  当进行加法或减法运算时，若低4位向高4位数发生进位或借位时AC将被硬件置位；否则，被清除。

  在十进制调整指令DA中要用到AC标志位状态。

- CY （PSW．7）—进位标志位

  在进行算术运算时，可以被硬件置位或清除，以表示运算结果中高位是否有进位或借位。在布尔处理机中CY被认为是位累加器

- F0 （PSW．5）—用户标志位/软件标志位

  开机时该位为“0”。用户可根据需要，通过位操作指令置“1”或者清“0”

80C51逻辑结构（续）

- 80C51内部结构
  - ◆ 2）**程序存储器**
    - 根据内部是否带有程序存储器而形成三种型号：

      内部没有程序存储器的称80C31

      内部带ROM的称80C51

      内部以EPROM代替ROM的称87C51

      内部以FLASH代替ROM的称89C51

    (1) 片内只读存储器：片内掩膜ROM，程序必须在制作单片机时写入

    (2) 片内可编程的ROM：可直接由用户进行编程

    - 紫外线可擦除型ROM－必须脱机固化，不能在线改写。
    - 电可擦除型ROM——称为Flash单片机（如89C51）

    (3) 片外只读存储器

80C51逻辑结构（续）

- 80C51内部结构
  - 3）**数据存储器 RAM**
    - 在单片机中，寄存器的运行速度高于数据存储器 RAM
    - 当内部RAM容量不够时，可通过串行或并行总线外扩数据存储器
  - 4）**并行I/O口**
    - 单片机往往提供了许多功能强、使用灵活的并行输入/输出引脚，用于检测与控制。有些I/O引脚还具有多种功能，比如可以作为数据总线的数据线、地址总线的地址线、控制总线的控制线等。
    - 80C51有四个8位的I/O口（P0、P1、P2、P3），以实现数据的并行输入输出

80C51逻辑结构（续）

- 80C51内部结构
  - 5）**串行I/O口**
  - 6）**定时器/计数器**
    - 在实际应用中，往往需要精确的定时，或者需对外部事件进行计数。为了减少软件开销和提高实时控制能力，故均设置定时器/计数器电路。80C51共有二个16位的定时器/计数器，80C52则有三个16位的定时器/计数器。
    - 定时器/计数器是嵌入式芯片的核心部件。（定时、计数、捕获、PWM等都是通过定时器/计数器部件实现的）

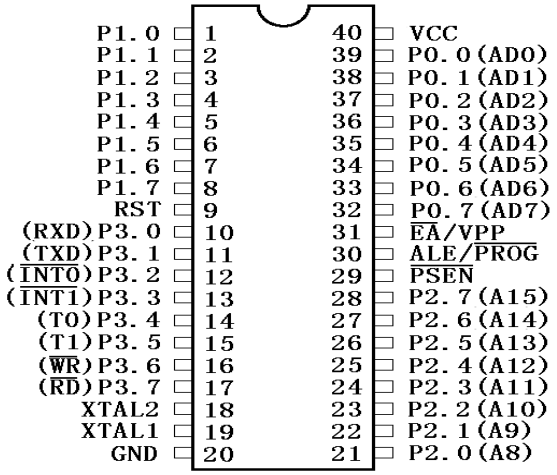
80C51逻辑结构（续）

- 80C51内部结构
  - **7）中断系统**
    - 80C51具有**内、外五个中断源**，即外中断两个，定时/计数中断2个，串行中断1个。全部中断分为高级和低级二个中断优先级
  - **8）振荡器电路及元件**
    - 外接振荡元件一般选用晶体振荡器（替代品：陶瓷振荡器），或用价廉的RC振荡器，也可用外部时钟源，作为振荡元件。也有的将振荡元件也集成在芯片内部，叫内部振荡器（精度不高，1-5%的误差）

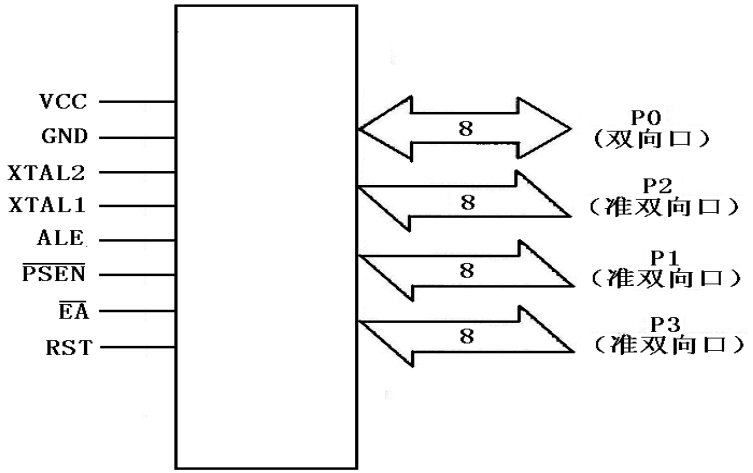
80C51信号引脚

- 80C51的封装
  - 40引脚双列直插（DIP, Dual In-line Package）
  - 44引脚（PLCC, plastic leaded chip carrier）
  - 44引脚（PQFP/TQFP, plastic quad flat pack / Thin Quad Flat Package）封装形式

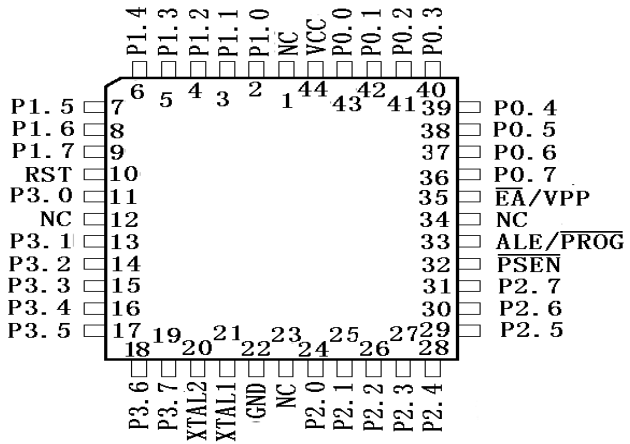
80C51信号引脚（续）



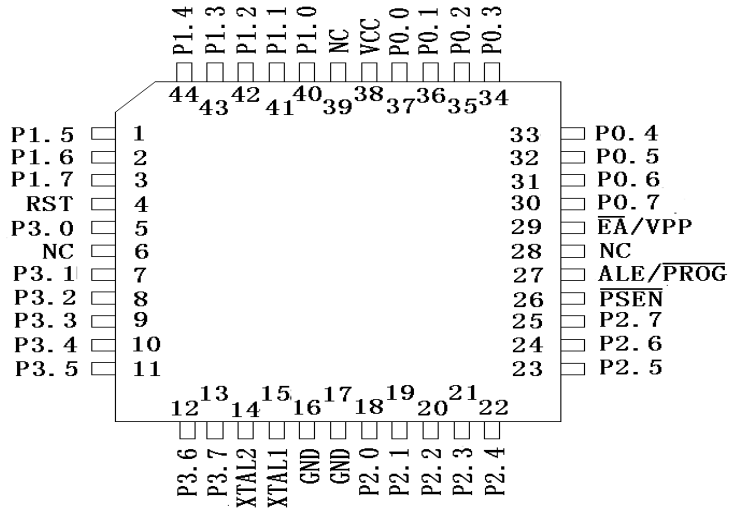
（a）40引脚双列直插（DIP）封装图



(b)逻辑图符号



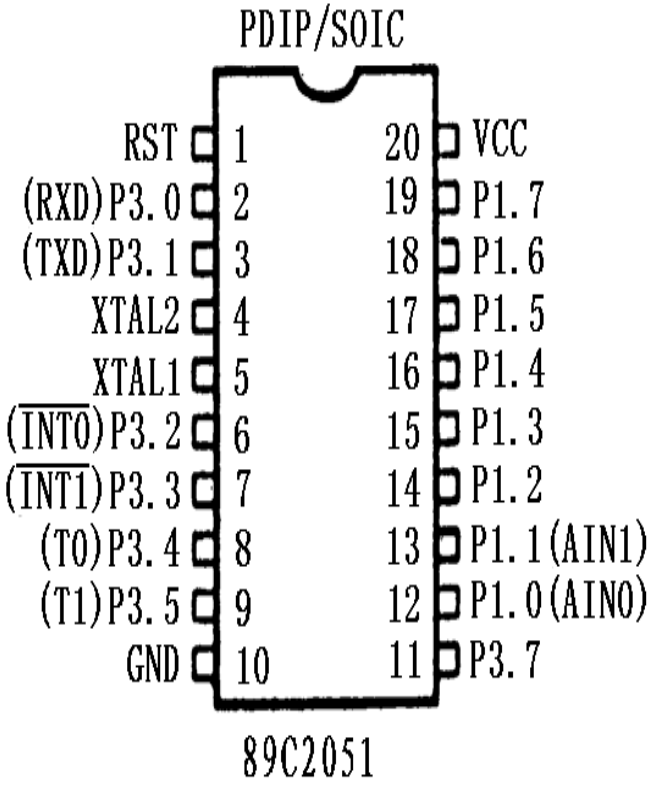
(c)44引脚（PLCC）封装图

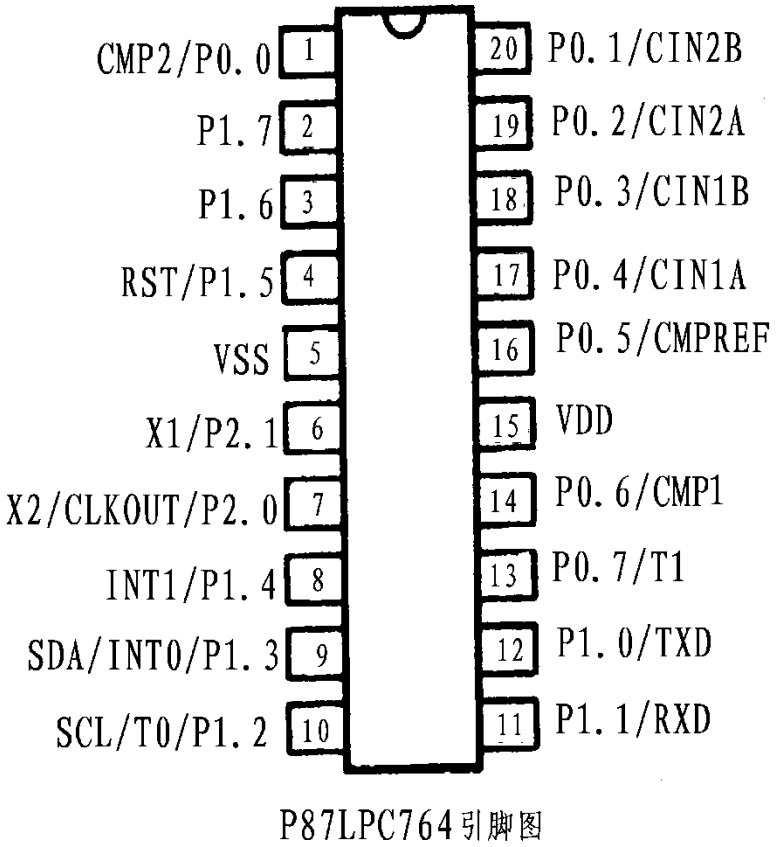


(d)44引脚(PQFP/TQFP)封装图

80C51信号引脚（续）

- 在某些场合，不需通过并行总线扩展芯片，常采用20引脚双列直插(DIP)/14引脚的单片机，如ATMEL公司的1051/2051/4051单片机等，或PHILIPS公司的P87LPC764单片机





80C51信号引脚（续）

AT89C51和AT89C2051主要性能表

AT89C51	AT89C2051
4KB可编程Flash存储器（可擦写1000次）	2KB可编程Flash存储器（可擦写1000次）
三级程序存储器保密	两级程序存储器保密
工作频率:0Hz-24MHz	工作频率:0Hz-24MHz
128字节内部RAM	128字节内部RAM
2个16位定时/计数器	2个16位定时/计数器
一个串行通讯口	一个串行通讯口
5个中断源	5个中断源
32条I/O引线	15条I/O引线
片内时钟振荡器	片内时钟振荡器 ，1个片内模拟比较器(AIN0-同相输入，AIN1-反相输入)

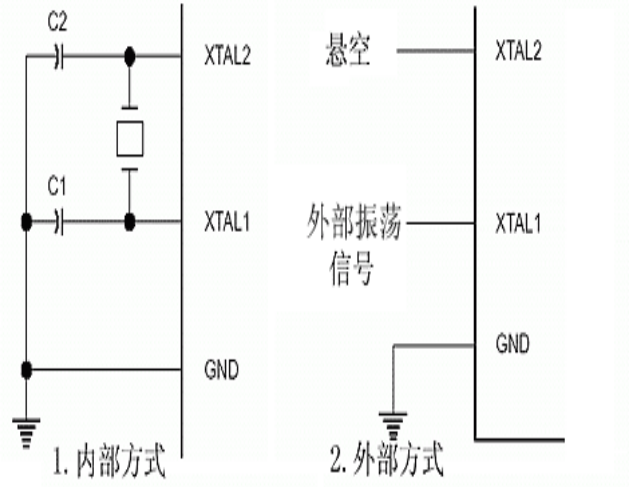
80C51信号引脚（续）

- 1）电源和晶振：
  - Vcc——电源　　• Vss——地线

  电源有三类：TYPE A:5V TYPE B:3.3V TYPE C:1.8V

  电源波动范围：国标DC电源误差范围± 10%，少量芯片只达到± 5%

  宽电源芯片：同时支持TYPEA/B等
  - XTAL1——片内振荡器的反相放大器输入端
  - XTAL2——片内振荡器的反相放大器输出端。
  - ◆ 使用外部振荡器时，外部信号应直接加到XTAL1，而XTAL2悬空。根据频率微调电容取15-30P左右。



80C51信号引脚（续）

- 2）I/O 共4个口，32根I/O线
  - ·P0——8位、漏极开路的双向I/O口，能驱动 8个 LSTTL
    - 使用片外寻址时，作低八位地址和数据总线分时复用
  - ·P1——8位、准双向I/O 口，可驱动 4个 LSTTL负载
    - 在编程/校验期间，用做输入低位字节地址
  - ·P2——8位、准双向I/O口，可以驱动4个LSTTL负载
    - 当使用片外存储器（ROM及RAM）时，输出高8位地址
    - 在编程/校验期间，接收高位字节地址

80C51信号引脚（续）

- 2）I/O 共4个口，32根I/O线（续）
  - ·P3—8位准双向I/O口，有内部上拉电路，4个LSTTL负载
    - P3有第二功能。使用这些功能时，其输出锁存器应由程序置1。
    - P3口总是按需要优先选择第二功能，剩下不用的才作口线使用

I/O口	第二功能	注 释
$P_{3.0}$	RXD	串行口数据接收端
$P_{3.1}$	TXD	串行口数据发送端
$P_{3.2}$	/INT_0	外部中断请求0
$P_{3.3}$	/INT_1	外部中断请求1
$P_{3.4}$	T_0	定时/计数器0外部输入
$P_{3.5}$	T_1	定时/计数器1外部输入
$P_{3.6}$	/WR	外部RAM写信号
$P_{3.7}$	/RD	外部RAM读信号

80C51信号引脚（续）

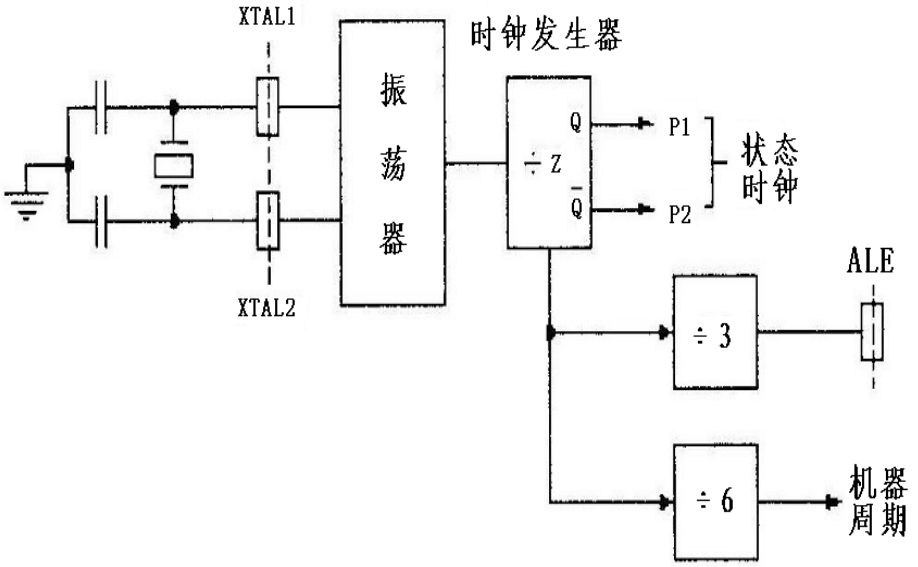
- 3）控制线：共4根
  - •RST（VPD：备用电源引入端，当电源发生故障，电源降到下限值时，备用电源经此端向内部RAM提供电压，以保护内部RAM中的数据不丢失）——复位输入信号，高电平有效。在振荡器工作时，在RST上作用两个机器周期以上的高电平，将器件复位。
  - • /EA（Vpp：编程电压,具体电压值视芯片而定）——片外程序存储器访问允许信号，低电平有效。/EA=1，选择片内程序存储器；/EA=0，则程序存储器全部在片外而不管片内是否有程序存储器。

80C51信号引脚（续）

- 3）控制线：共4根（续）
  - ·ALE（PROG：编程脉冲）——地址锁存允许信号，输出
    - 在访问片外存储器或I/O时，用于锁存低八位地址，以实现低八位地址与数据的隔离。
    - ALE可以驱动8个LS TTL负载
    - 对片内程序存储器编程时，该引脚用于输入编程脉冲PROG
  - ·/PSEN——片外程序存储器读选通信号，低电平有效
    - 在从片外程序存储器取指期间，在每个机器周期中，当其有效时，程序存储器的内容被送上 P0口（数据总线）
    - 它可以驱动 8个LSTTL负载

80C51时钟电路

- 时钟电路用于产生工作所需要的时钟信号
- 在80C51内带有时钟电路，在片外通过XTAL1和XTAL2引脚接入定时控制元件（晶体振荡器和电容），即构成一个稳定的自激振荡器
- 在80C51芯片内部有一个高增益反相放大器，而在芯片的外部，XTAL1和XTAL2之间跨接晶体振荡器和微调电容
- 时钟电路组成：振荡器及定时控制元件、时钟发生器、地址锁存允许信号 ALE



80C51时钟电路（续）

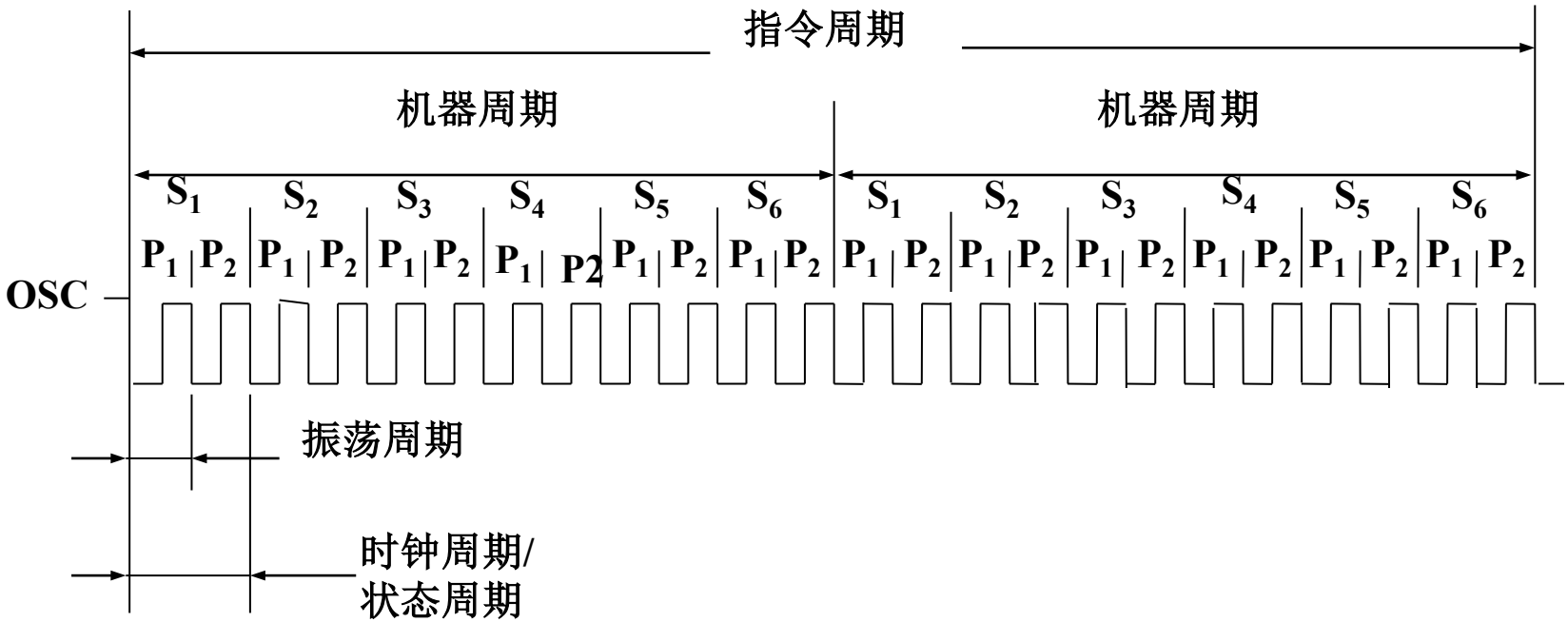
- **振荡器及定时控制元件**
  - 振荡器的工作由PD位（特殊功能寄存器PCON中的一位）控制。当 PD置1时，振荡器停止工作，系统进入低功耗工作状态
  - 振荡器的工作频率在1.2～12 MHz之间
  - 在多机系统中，为了使各芯片之间时钟信号的同步，应当引入唯一的公用外部脉冲信号作为各芯片的振荡脉冲
  - 当由外部输入时钟信号时，外部信号接入XTAL1，XTAL2悬空不用。对外部信号的占空比没有要求，高/低电平持续时间应不小于 20 ns

80C51时钟电路（续）

- **内部时钟发生器**
  - 内部时钟发生器实质上是一个2分频的触发器。其输入由振荡器引入的，输出为两个节拍的时钟信号。输出的前半周期，节拍1（P1）信号有效；后半周期，节拍2（P2）信号有效。每个输出周期为一个计算机CPU的状态周期，即时钟发生器的输出为状态时钟。每个状态周期内包括一个P1节拍和一个P2节拍，形成CPU内的基本定时时钟
- **ALE信号**
  - 状态时钟经过3分频之后，产生ALE引脚上的信号输出

时序定时单位

- 单片机执行指令是在时序电路的控制下一步一步进行的。80C51的时序定时单位共有4个：振荡周期/节拍、时钟周期/状态、机器周期和指令周期



时序定时单位(续)

- 1） **振荡周期**/节拍P
- 2） **时钟周期**/状态周期/状态S
  - 时钟周期是振荡周期的两倍，又称状态周期或状态S。一个状态S有两个节拍，其前半周期对应节拍叫P1，后半周期对应节拍叫P2
- 3） **机器周期**
  - 通常将完成一个基本操作所需的时间称为机器周期
  - 规定一个机器周期的宽度为6个状态，表示为S1～S6。一个机器周期共有12个振荡脉冲周期，机器周期就是振荡脉冲的12分频
  - 机器周期是处理器的最小时间单位

时序定时单位(续)

- 4）指令周期
  - 执行一条指令所需要的时间称为指令周期。**80C51的指令周期根据指令的不同，可包含有一、二、三、四个机器周期**

例如，设外接晶振为12MHz时，四个周期的具体值为：

振荡周期＝1/12MHz＝1/12μs＝0.0833μs

时钟周期＝1/6 μs＝0.167 μs

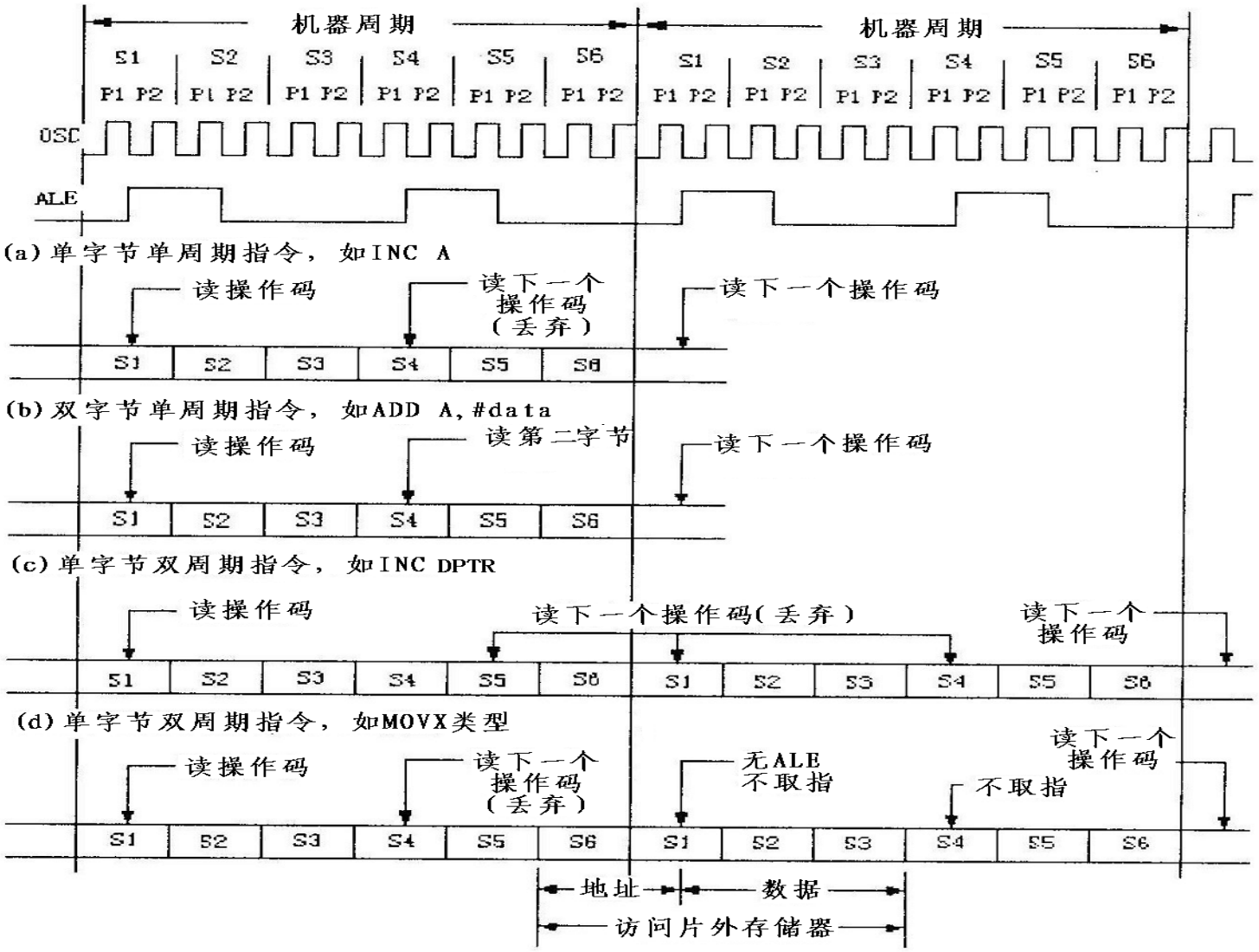
机器周期＝1μs

指令周期＝1～4μs

指令时序

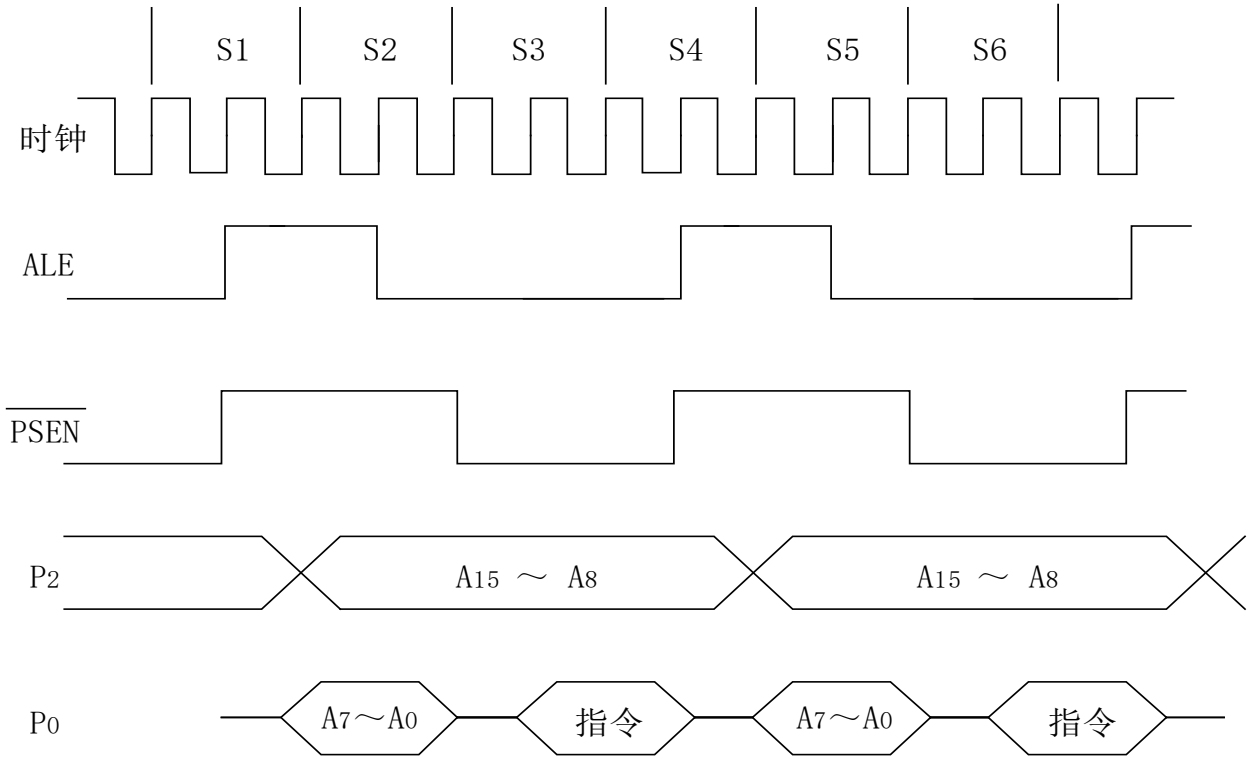
- 80C51指令按其长度分：单字节、双字节和三字节指令
  - 单字节或双字节指令可能是单机器周期或双机器周期的
  - 三字节指令是双机器周期的
  - 乘除指令是四个机器周期的

指令时序(续)


机器周期
机器周期
S1 S2 S3 S4 S5 S6
P1 P2
OSC
ALE
(a) 单字节单周期指令，如INC A
读操作码
读下一个操作码(丢弃)
读下一个操作码
(b) 双字节单周期指令，如ADD A,#data
读操作码
读第二字节
读下一个操作码
(c) 单字节双周期指令，如INC DPTR
读操作码
读下一个操作码(丢弃)
读下一个操作码
(d) 单字节双周期指令，如MOVX类型
读操作码
读下一个操作码(丢弃)
无ALE不取指
不取指
读下一个操作码
地址
数据
访问片外存储器

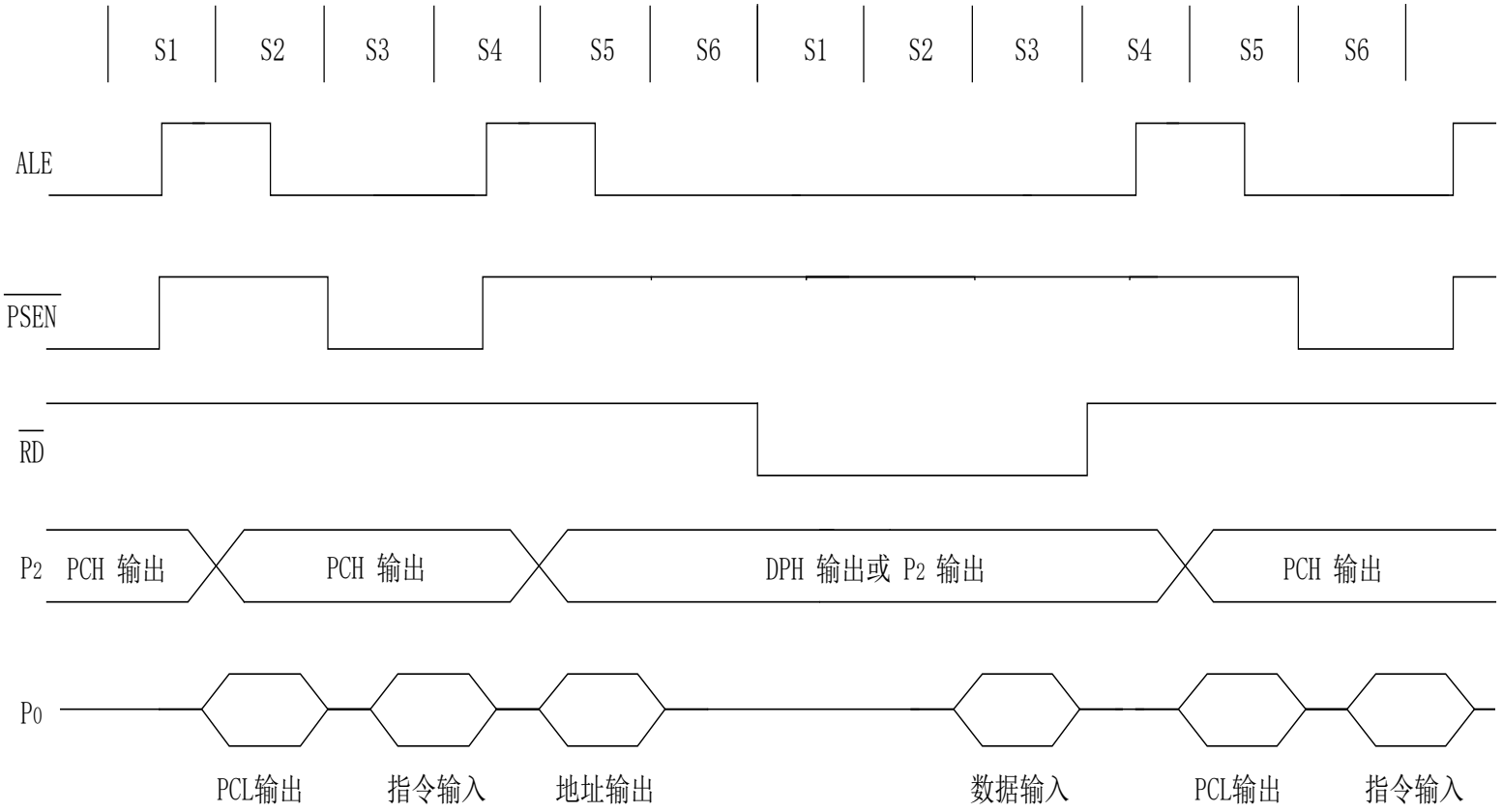
访问外部ROM和RAM的时序

- 对外部程序存贮器的访问使用/PSEN作读选通信号
- 1） 访问外部ROM的时序
  - 当从外部程序存贮器读取指令时，需要使用16位地址，且高8位地址从从P2口输出，并且在整个机器周期内保持不变



访问外部ROM和RAM的时序

- 2）访问外部RAM的时序



80C51工作方式

- 80C51单片机工作方式
  - 复位
  - 程序执行
  - 低功耗
  - 编程和校验

80C51复位

- 1）复位操作
  - 复位是单片机的初始化操作，主要功能是把PC初始化为0000H，使单片机从0000H单元开始执行程序。当由于程序运行出错或操作错误使系统处于死锁状态时，为摆脱困境，可以按复位键以重新启动，也可以通过WDT看门狗定时器来强迫复位。
  - 除PC之外，复位操作还对其它一些特殊功能寄存器有影响
  - 复位操作还对个别引脚信号有影响。例如在复位期间，ALE和/PSEN信号变为无效状态，即 ALE=0， /PSEN =1

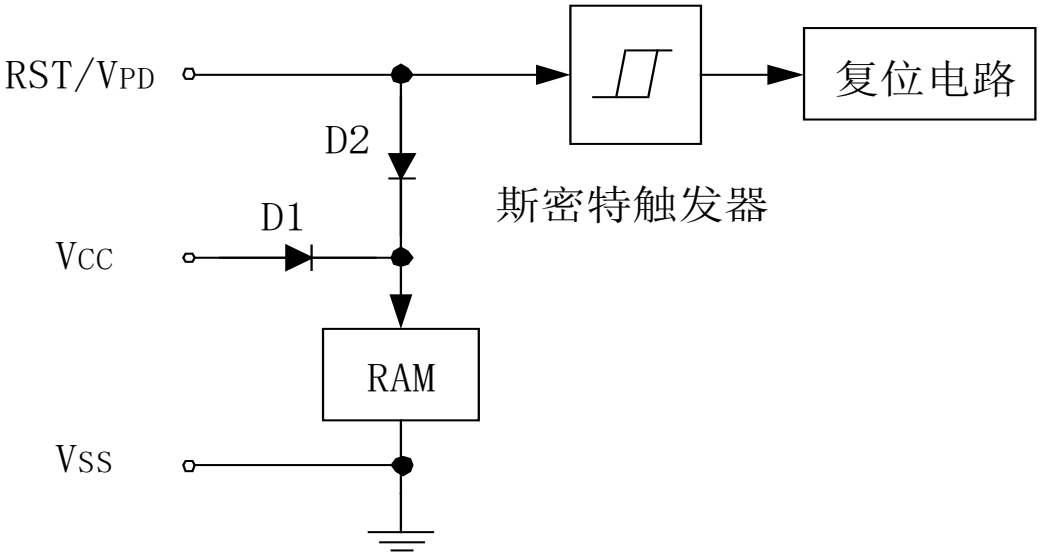
80C51复位(续)

- 1) 复位操作（续）

特殊功能寄存器	初始状态	特殊功能寄存器	初始状态
ACC/A	00H	TMOD	00H
B	00H	TCON	00H
PSW	00H	TH0	00H
SP	07H	TL0	00H
DPL	00H	TH1	00H
DPH	00H	TL1	00H
P0～P3	FFH	SBUF	xxxxxxxxB
IP	xx0000000B	SCON	00H
IE	0x000000B	PCON	0xxx0000B

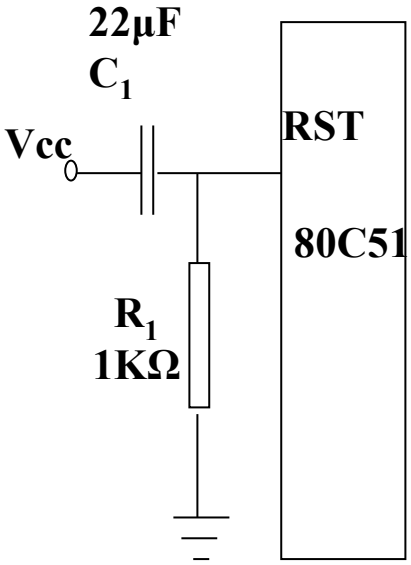
80C51复位(续)

- 2）复位信号
  - RST引脚是复位信号的输入端。复位信号是高电平有效，其有效时间应持续24个振荡周期(即2个机器周期）以上。若使用频率为6MHz的晶振，则复位信号应持续4μs以上
  - 整个复位电路包括芯片内、外两部分。外部电路产生的复位信号送施密特触发器，再由片内复位操作。
  - 有上电自动复位、按键复位两种方式

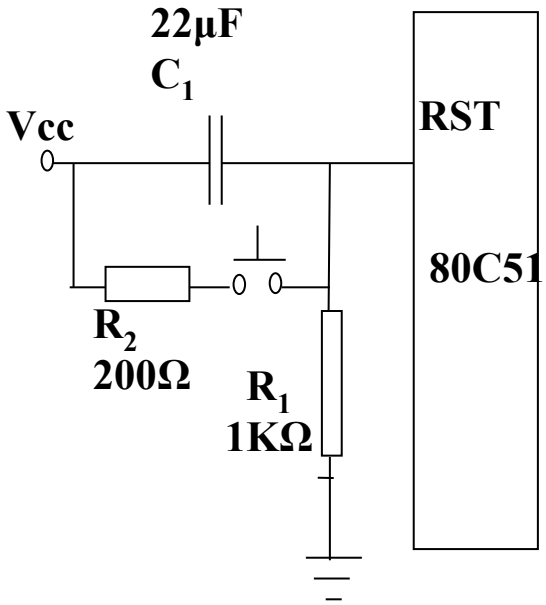


80C51复位(续)

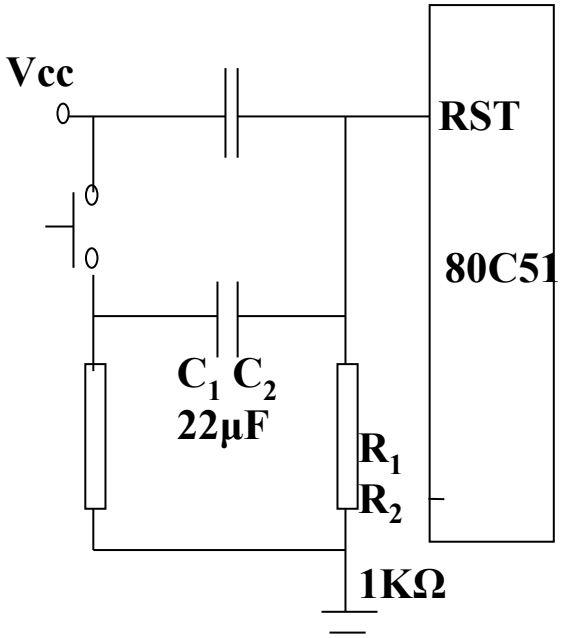
- 2）复位信号(续)



（a）上电复位电路



（b）按键电平复位电路



（c）按键脉冲复位电路

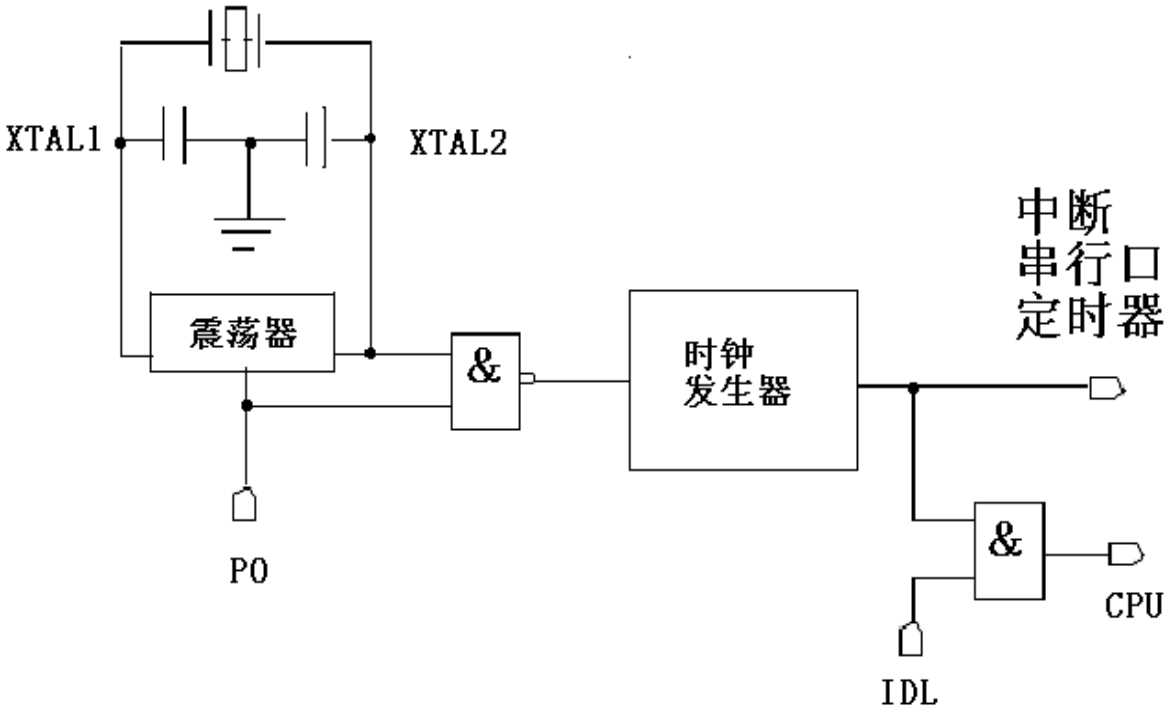
80C51 程序执行

- 程序执行方式是单片机的基本工作方式
  - 由于复位后PC＝0000H，因此程序执行总是从0000H开始的。一般在0000H开始的单元中存放一条无条件转移指令，以便跳转到实际主程序的入口去执行
  - 比如：

```
ORG     0000H
SJMP    MAIN; 转主程序
```

80C51低功耗工作方式

- 80C51有两种低功耗方式，由电源控制寄存器（PCON）的有关位来控制
  - 待机/空闲(IDLE)方式
  - 掉电(POWER DOWN)保护方式

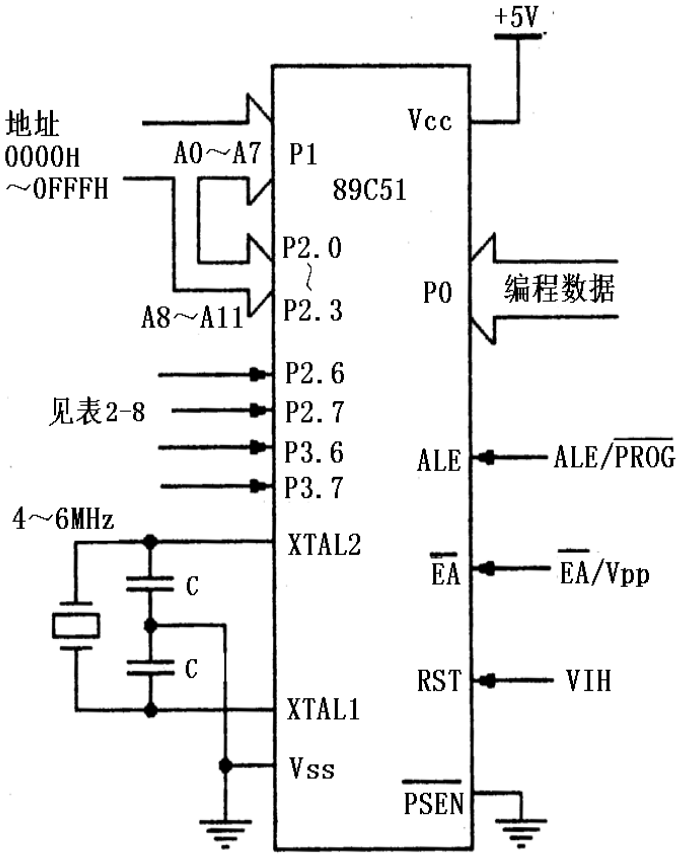


80C51 编程工作方式(烧录)

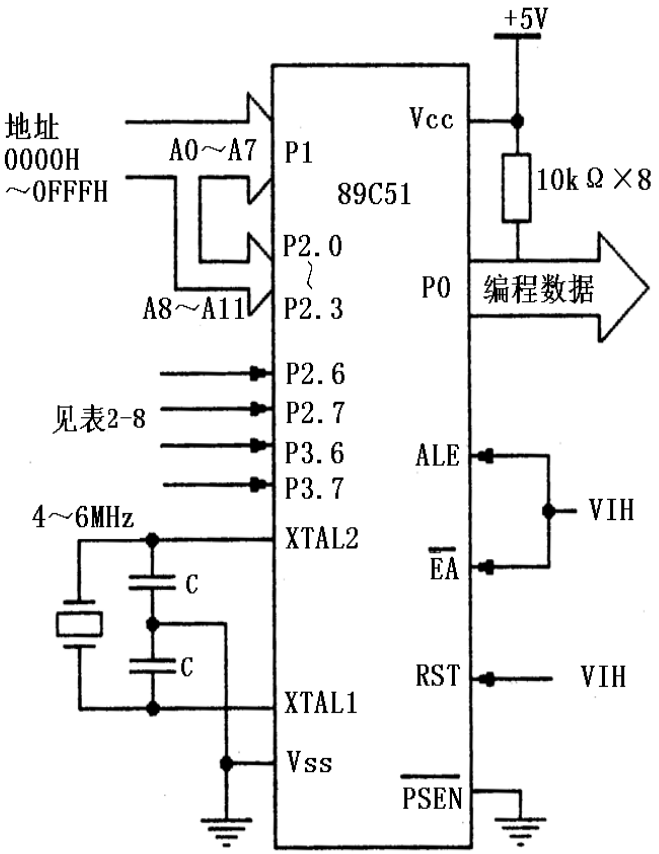
- 对于片内具有EPROM型程序存储器的87C51(87C52）和片内具有闪速存储器的89C51（89C52）、78E51（78E52）等单片机可以通过编程来修改程序存储器中的程序
  - **查询数据**
  - **准备好/忙(RDY/BSY) 信号**
  - **编程校验**
  - **芯片擦除**

80C51 编程工作方式(续)

- 1) 闪速存储器编程(续)



(a) 编　程



(b) 校　验

80C51 编程工作方式(续)

- 1) 闪速存储器编程(续)
  - 读特征字节
    - 89C51有三个特征字节，地址为030H、031H和032H，分别用来指示该器件的生产厂商、型号和编程电压
    - 比如：

(030H)=1EH	表示ATMER公司生产
(031H)=51H	表示型号为89C51
=61H	表示型号为89LV51
(032H)=FFH	表示编程电压为12V
=05H	表示编程电压为5V

80C51 编程工作方式(续)

- 1) 闪速存储器编程(续)
  - 程序锁定位的功能和编程
    - 80C51片内有三个锁定位。

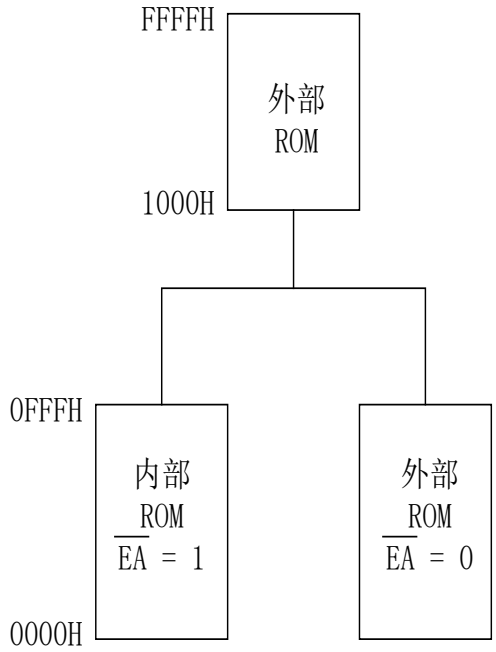
序号	锁定位编程状况			保护作用
	LB1	LB2	LB3	
1	未编	未编	未编	锁定作用，若密码阵列已编程，则校验时将得密码
2	已编	未编	未编	禁止片外程序存储器中的MOVC指令从片内程序中读取代码字；EA 值在复位时被采样并锁入内部，禁止 EPROM 进一步编程
3	已编	已编	未编	同 2，但校验也被禁止
4	已编	已编	已编	同 3，并禁止执行片外程序

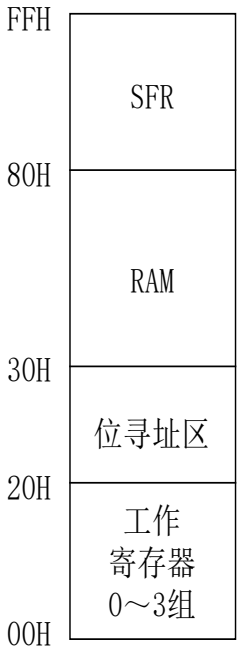
80C51 布尔(位)处理器

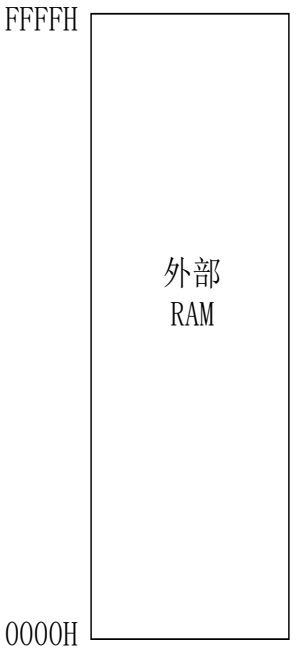
- 在80C51中，与字节处理器相对应，还特别设置了一个结构完整、功能极强的布尔（位）处理器
  - 位累加器：借用进位标志位CY/C。在布尔运算中CY是数据源之一，又是运算结果的存放处，位数据传送的中心。根据CY的状态实现程序条件转移：JC rel、JNC rel、JBC rel
  - 位寻址的RAM：内部RAM位寻址区中的0～127位(20H～2FH)；
  - 位寻址的寄存器：特殊功能寄存器（SFR）中的可以位寻址的位
  - 位寻址的I/O口：并行I/O口中的可以位寻址的位(如P1.0)。
  - 位操作指令：位操作指令可实现对位的置位、清0、取反、位状态判跳、传送、位逻辑运算、位输入/输出等操作

80C51存储器结构与地址空间

- 80C51采用哈佛结构
  - 物理上4个存储器空间
    - 程序存储器：　　片内程序存储器，片外程序存储器
    - 数据存储器：　　片内数据存储器，片外数据存储器







80C51存储器结构与地址空间(续)

- 逻辑上有3个存储器地址空间（三种基本寻址空间）
  - 片内、片外统一的 64 KB程序存储器地址空间；
  - 片内256B（80C52为384B）数据存储器地址空间；
  - 片外64 KB的数据存储器地址空间。
- 在访问这3个不同的逻辑空间时，应选用不同形式的指令(分别用MOVC、MOV、MOVX指令来区分三个不同的逻辑空间)

80C51程序存储器

- 用于存放程序和常数
- 采用16位的地址总线，可直接扩展的地址空间为64KB
- CPU访问片内和片外存储器，可由/EA引脚所接的电平来确定
  - /EA接高电平时，程序从片内程序存储器0000H开始执行；当PC值超出片内ROM容量时，会自动转向片外程序存储器空间执行
  - /EA接低时，系统执行片外程序存储器0000H开始存放的程序
  - 对于片内无ROM的80C31/80C32单片机，应将/EA引脚固定接低，以使系统执行片外程序存储器程序

80C51程序存储器(续)

- 程序存储器的某些单元被保留用于特定的程序入口地址
  - 0003H～002BH：6个中断源的中断服务程序入口地址
  - 以下7个特定地址被保留用于中断入口地址，这种中断模式叫**独立向量模式**：

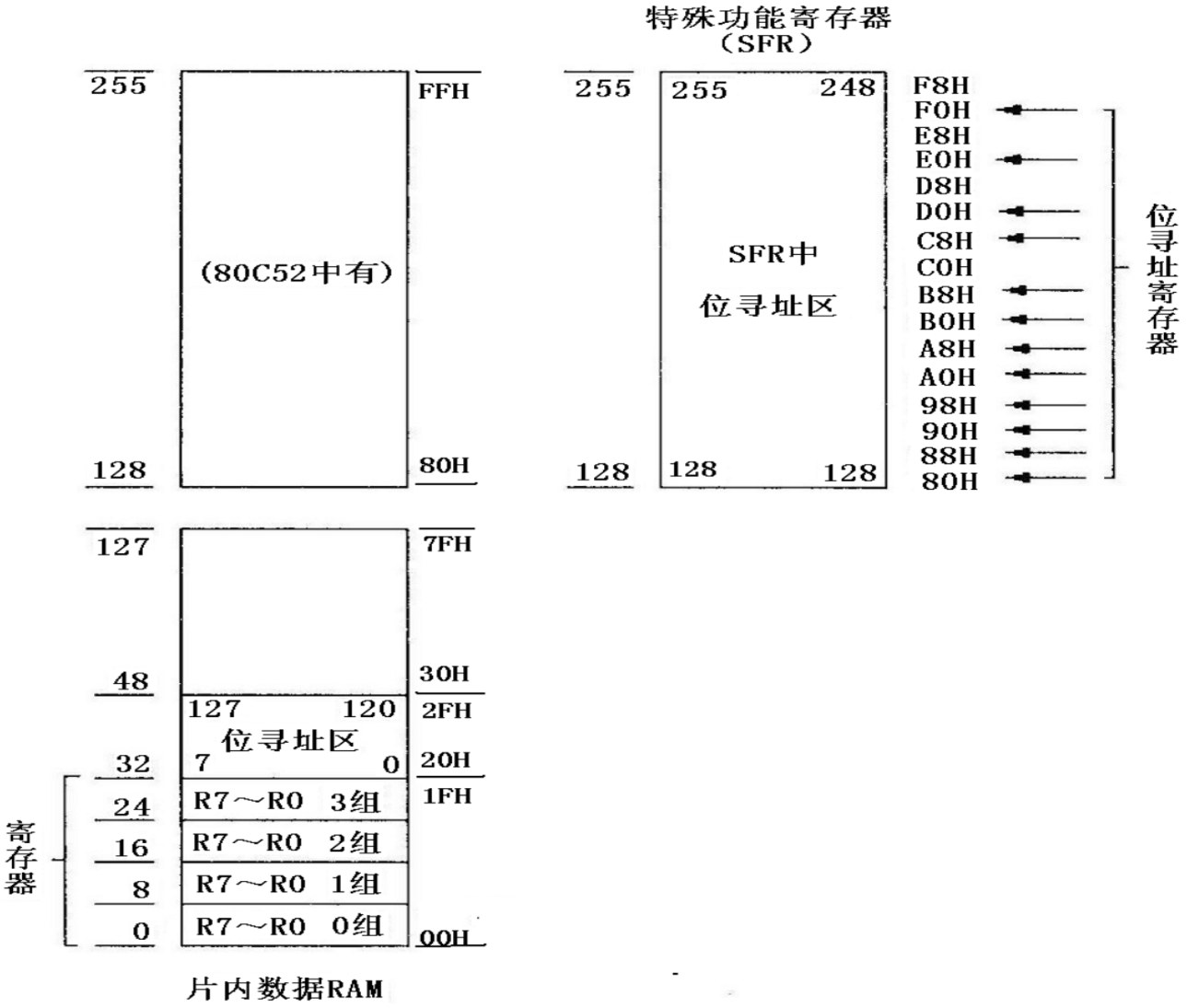
复位	0000H~0002H（3个单元）
外部中断0	0003H~000AH（8个单元）
计时器T0溢出	000BH~0012H （8个单元）
外部中断1	0013H~001AH （8个单元）
计时器T1溢出	001BH~0022H （8个单元）
串行口中断	0023H~002AH （8个单元）
*计时器 T2/T2EX	002BH~0032H （8个单元，80C52）

  - 在程序设计时，通常在这些中断入口处设置无条件转移指令，使之转向对应的中断服务程序段处执行

80C51片内数据存储器

- 片内数据存储器（IRAM）地址只有8位，最大寻址范围为256个字节
  - 片内数据RAM区
    - 对80C51，为地址空间的低128B。
    - 对80C52，为地址空间的0～256B。
  - 特殊功能寄存器SFR区
    - 对80C51，为地址空间的高128B
    - 对80C52，高128B的RAM区和SFR区的地址空间是重叠的。究竟访问哪一个区是通过不同的寻址方式来加以区别的，访问高128B RAM区时，选用间接寻址方式；访问SFR区，选用直接寻址方式

80C51片内数据存储器(续)



80C51片内数据存储器(续)

- 片内数据RAM区
  - 工作寄存器区
    - 用寄存器直接寻址区域，指令数量最多，均为单周期指令，速度最快
    - 片内数据 RAM区的 0～31（00H～1FH），共 32个单元，是 4个通用工作寄存器组，每个组包含8个8位寄存器，编号为 R0～R7
    - 在某一时刻，只能选用一组寄存器。通过程序状态字（PSW）中的RS0、RS1二位的设置来实现的。

RS1	RS0	组号	寄存器R0～R7地址
0	0	0组	00H～07H
0	1	1组	08H～0FH
1	0	2组	10H～17H
1	1	3组	18H～1FH

80C51片内数据存储器(续)

- 片内数据RAM区(续)
  - 位寻址区
    - 片内数据RAM区的32－47（20H－2FH）的16个字节单元，共128位，是可位寻址的RAM区。既可进行字节寻址，又可位寻址
    - 这16个位寻址单元，再加上可位寻址的特殊功能寄存器一起构成了布尔（位）处理器的数据存储器空间

字节地址	位地址							
	D_7	D_6	D_5	D_4	D_3	D_2	D_1	D_0
2FH	7FH	7EH	7DH	7CH	7BH	7AH	79H	78H
2EH	77H	76H	75H	74H	73H	72H	71H	70H
2DH	6FH	6EH	6DH	6CH	6BH	6AH	69H	68H
2CH	67H	66H	65H	64H	63H	62H	61H	60H
2BH	5FH	5EH	5DH	5CH	5BH	5AH	59H	58H
2AH	57H	56H	55H	54H	53H	52H	51H	50H
29H	4FH	4EH	4DH	4CH	4BH	4AH	49H	48H
28H	47H	46H	45H	44H	43H	42H	41H	40H
27H	3FH	3EH	3DH	3CH	3BH	3AH	39H	38H
26H	37H	36H	35H	34H	33H	32H	31H	30H
25H	2FH	2EH	2DH	2CH	2BH	2AH	29H	28H
24H	27H	26H	25H	24H	23H	22H	21H	20H
23H	1FH	1EH	1DH	1CH	1BH	1AH	19H	18H
22H	17H	16H	15H	14H	13H	12H	11H	10H
21H	0FH	0EH	0DH	0CH	0BH	0AH	09H	08H
20H	07H	06H	05H	04H	03H	02H	01H	00H

80C51片内数据存储器(续)

- 片内数据RAM区(续)
  - 字节寻址
    - 片内数据RAM区（30H～7FH），共80个字节，可直接寻址
    - 对于 80C52，还有高128B的数据RAM区，只能采用间接寻址
  - 堆栈及堆栈指针SP
    - 堆栈是在片内数据RAM区中，数据先进后出/后进先出的区域。
    - 堆栈有二种形式，一是向上生成，二是向下生成。80C51堆栈向上生成:进栈操作:先SP+1,后写入数据;出栈操作:先读出数据,后SP+1
    - 系统复位后SP内容为07H。堆栈深度不能超过片内RAM空间
    - 堆栈是为子程序调用和中断操作而设立。其具体功能有两个：保护断点和现场。
    - 子程序调用和中断都允许多级嵌套

80C51片内数据存储器(续)

- 片内数据RAM区(续)
  - 特殊功能寄存器SFR区(Special Function Registers)
    - 用以存放相应功能部件的控制命令、状态或数据的区域
    - 80C51设有128B片内数据RAM的特殊功能寄存器空间区。
    - 对于80C51共定义了21个特殊功能寄存器。在80C52中，增加了5个特殊功能寄存器，共计26个
    - 在特殊功能寄存器中，字节地址中低位地址为0H或8H的特殊功能寄存器(80C51有11个，80C52还增加了T2CON)，除可字节寻址外，还可位寻址

80C51片内数据存储器(续)

- 片内数据RAM区(续) --- SFR区(续)

序号	标识符	名　　称	字节地址	位 地 址
1	ACC	累加器	E0H	E0H～E7H
2	B	B 寄存器	F0H	F0H～F7H
3	PSW	程序状态字	D0H	D0H～D7H
4	SP	堆栈指针	81H	
5	DPTR	数据指针(DPH、DPL)	83H、82H	
6	P0	P0 口	80H	80H～87H
7	P1	P1 口	90H	90H～97H
8	P2	P2 口	A0H	A0H～A7H
9	P3	P3 口	B0H	B0H～B7H
10	IP	中断优先级控制寄存器	B8H	B8H～BFH
11	IE	中断允许控制寄存器	A8H	A8H～AFH
12	TOMD	定时器/计数器方式控制寄存器	89H	
13	TCON	定时器/计数器控制寄存器	88H	88H～8FH
14	T2CON	定时器/计数器 2 控制寄存器	C8H	C8～CFH
15	TH0	定时器/计数器 0(高位字节)	8CH	
16	TL0	定时器/计数器 0(低位字节)	8AH	
17	TH1	定时器/计数器 1(高位字节)	8DH	
18	TL1	定时器/计数器 1(低位字节)	8BH	
19	TH2	定时器/计数器 2(高位字节)	CDH	
20	TL2	定时器/计数器 2(低位字节)	CCH	
21	RLDH	定时器/计数器 2 自动重装载（高位字节）	CBH	
22	RLDL	定时器/计数器 2 自动重装载（低位字节）	CAH	
23	SCON	串行口控制寄存器	98H	98H～9FH
24	SBUF	串行数据缓冲器	99H	
25	PCON	电源控制及波特率选择寄存器	97H	

80C51片内数据存储器(续)

- 片内数据RAM区(续) --- SFR区(续)

SFR		位地址							
名称	字节地址	7	6	5	4	3	2	1	0
B	F0H	F7H	F6H	F5H	F4H	F3H	F2H	F1H	F0H
ACC	E0H	E7H	E6H	E5H	E4H	E3H	E2H	E1H	E0H
PSW	D0H	CY	AC	F0	RS1	RS0	OV	-	P
		D7H	D6H	D5H	D4H	D3H	D2H	D1H	D0H
T2CON	C0H	TF2	EXF2	RCLK	TCLK	EXEN2	TR2	C/$\overline{T}$	CP/RL2
		CFH	CEH	CDH	CCH	CBH	CAH	C9H	C8H
IP	B8H	-	-	PT2	PS	PT1	PX1	PT0	PX0
		BFH	BEH	BDH	BCH	BBH	BAH	B9H	B8H
P3	B0H	B7H	B6H	B5H	B4H	B3H	B2H	B1H	B0H
IE	A8H	EA	-	ET2	ES	ET1	EX1	ET0	EX0
		AFH	AEH	ADH	ACH	ABH	AAH	A9H	A8H
P2	A0H	A7H	A6H	A5H	A4H	A3H	A2H	A1H	A0H
SCON	98H	SM0	SM1	SM2	REN	TB8	RB8	TI	RI
		9FH	9EH	9DH	9CH	9BH	9AH	99H	98H
P1	90H	97H	96H	95H	94H	93H	92H	91H	90H
TCON	88H	TF1	TR1	TF0	TR0	IE1	IT1	IE0	IT0
		8FH	8EH	8DH	8CH	8BH	8AH	89H	88H
P0	80H	87H	86H	85H	84H	83H	82H	81H	80H

80C51片外数据存储器

- 片外数据存储器是在外部存放数据的区域，这一区域只能用寄存器间接寻址的方法访问，所用的寄存器为DPTR、R1或R0。指令助记符为MOVX
  - 用R0、R1寻址时，R0、R1为8位寄存器，最大寻址范围为256B在80C51中，有一个专门的数据存储器的地址指示器——数据指针DPTR，用于访问片外数据存储器（ERAM）。DPTR也是16位的寄存器，80C51具有64 KB的数据存储器扩展能力

80C51系统总线

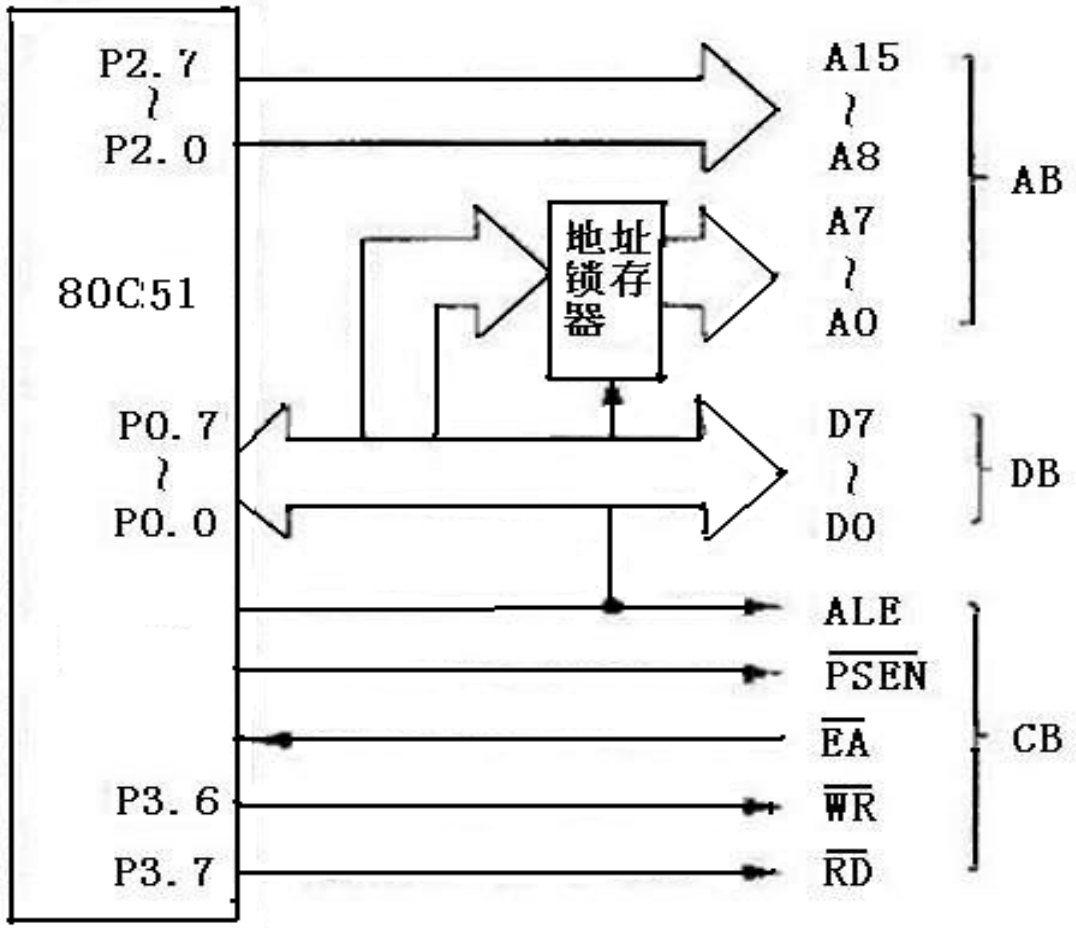
- 所谓总线，就是连接计算机各部件的一组公用信号线。使用并行总线结构的80C51系列单片机，按其功能通常把系统总线分为三组，即地址总线、数据总线和控制总线。具有总线的外部芯片都通过这三组总线进行扩展
- **地址总线（Address Bus，简写为AB）**
  - 地址总线上传送的是地址信号，用于存储单元和I/O端口的选择。地址总线是单向的，地址信号只能由单片机向外发出
  - 地址总线的数目决定着可直接访问的存储单元的数目。如n位地址可访问2n个存储单元，即通常所说的寻址范围为2^n 地址单元
  - 80C51单片机存储器最多可扩展64KB，即2^16KB，地址总线有16条

80C51系统总线(续)

- **数据总线（Data Bus，简写为DB）**
  - 数据总线用于与存储器或I/O端口之间传送数据
  - 数据总线的位数与处理数据的字长一致。数据总线是双向的
- **控制总线（Control Bus，简写为CB）**
  - 控制总线实际上就是一组控制信号线。对于一条具体的控制信号来说，其传送方向是单向的，但是由不同方向的控制信号组合的控制总线则表示为双向
  - 由于采用总线结构形式，因此大大减少了系统中传输线的数目，提高了系统的可靠性，增加了系统的灵活性。此外，总线结构也使扩展易于实现，各功能部件只要符合总线规范，就可以很方便地接入系统，实现扩展

80C51系统总线(续)

- 80C51没有专用的地址线和数据线,采用I/O口线的复用技术

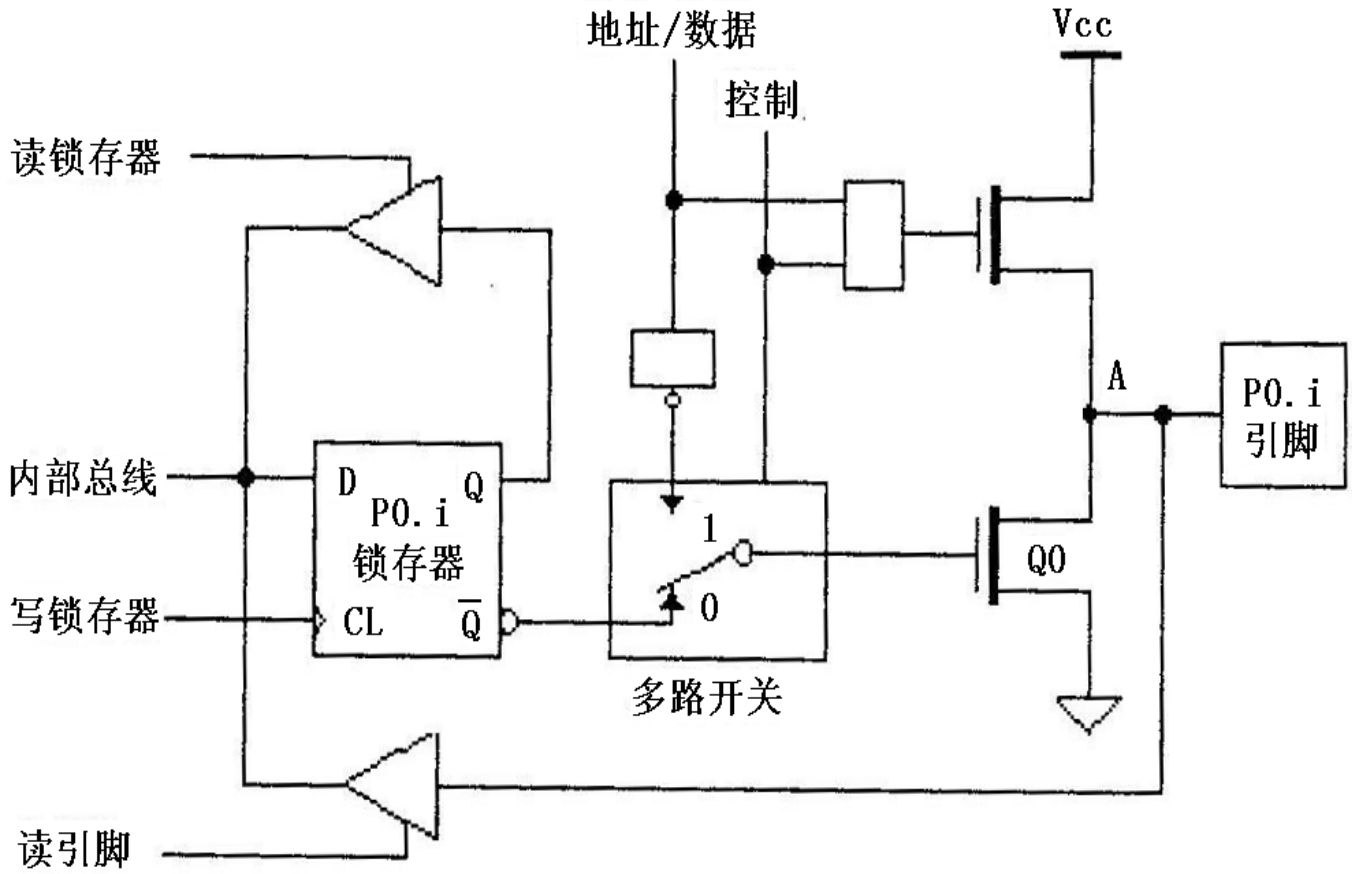


并行输入/输出端口

- 80C51单片机有4个双向并行的8位I/O口P0～P3
  - P0口为三态双向口,可驱动8个LSTTL电路
  - P1、P2、P3口为准双向口(作为输入时,要把口线拉成高电平,故称为准双向口),其负载能力为4个LSTTL电路
  - 8051在对端口P0一P3的输入操作上，有如下约定：凡属于读-修改-写方式的指令，从锁存器读入信号，其它指令则从端口引脚线上读入信号
- P0口
  - 可以字节访问也可位访问，其字节地址为80H，位地址为80H～87H

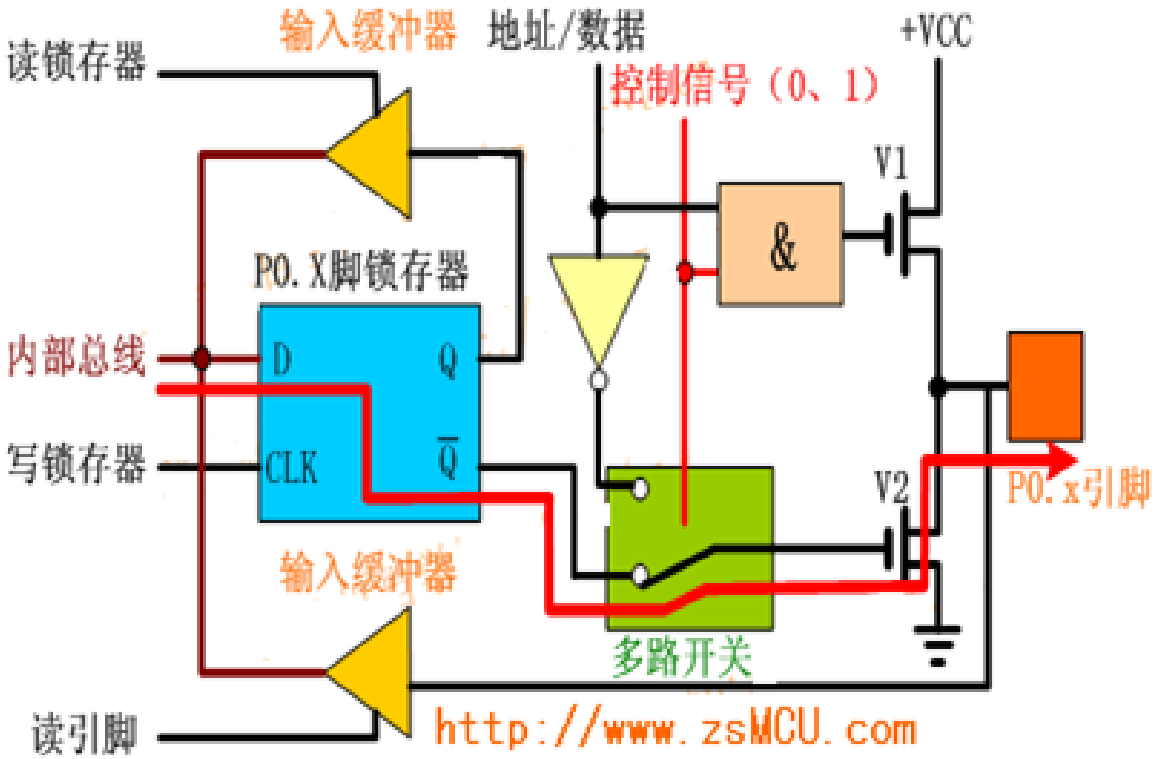
并行输入/输出端口(续)

- P0口(续)



并行输入/输出端口(续)

- P0口(续)
  - 做I/O端口使用 --- OUTPUT



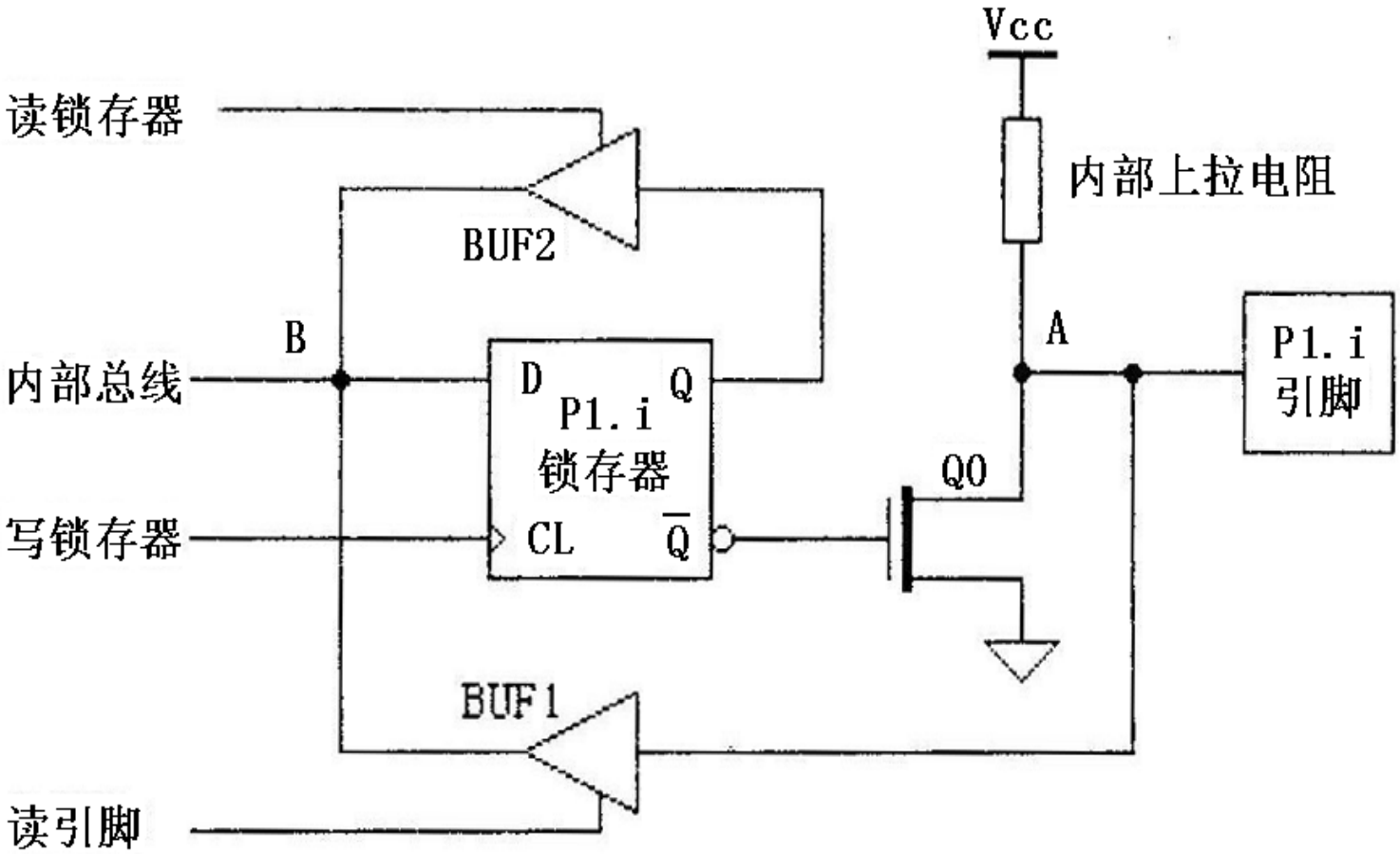
P0口由内部数据总线向引脚输出时的流程图

并行输入/输出端口(续)

- P1口
  - P1口是一个标准的准双向口
  - P1口 包含输出锁存器、输入缓冲器BUF1、BUF2（读锁存器）以及由 FET场效应管 Q0与上拉电阻组成的输入 / 输出驱动器
  - P1口是一个8位口，可以字节访问也可按位访问，其字节访问地址为90H，位访问地址为90H～97H

并行输入/输出端口(续)

- P1口(续)



并行输入/输出端口(续)

- P1口(续)
  - 特点
    - 输出锁存，输出时没有条件
    - 输入缓冲，输入时有条件；即当P1口作为输入口使用时，即先将其锁存器写入‘1’，使FET截止，然后才能输入，具有这种操作特点的输入/输出端口，称为准双向I/O口。8051单片机的P1、P2、P3都是准双向口
    - 工作过程中无高阻状态，也就是该口不是输入态就是输出态

并行输入/输出端口(续)

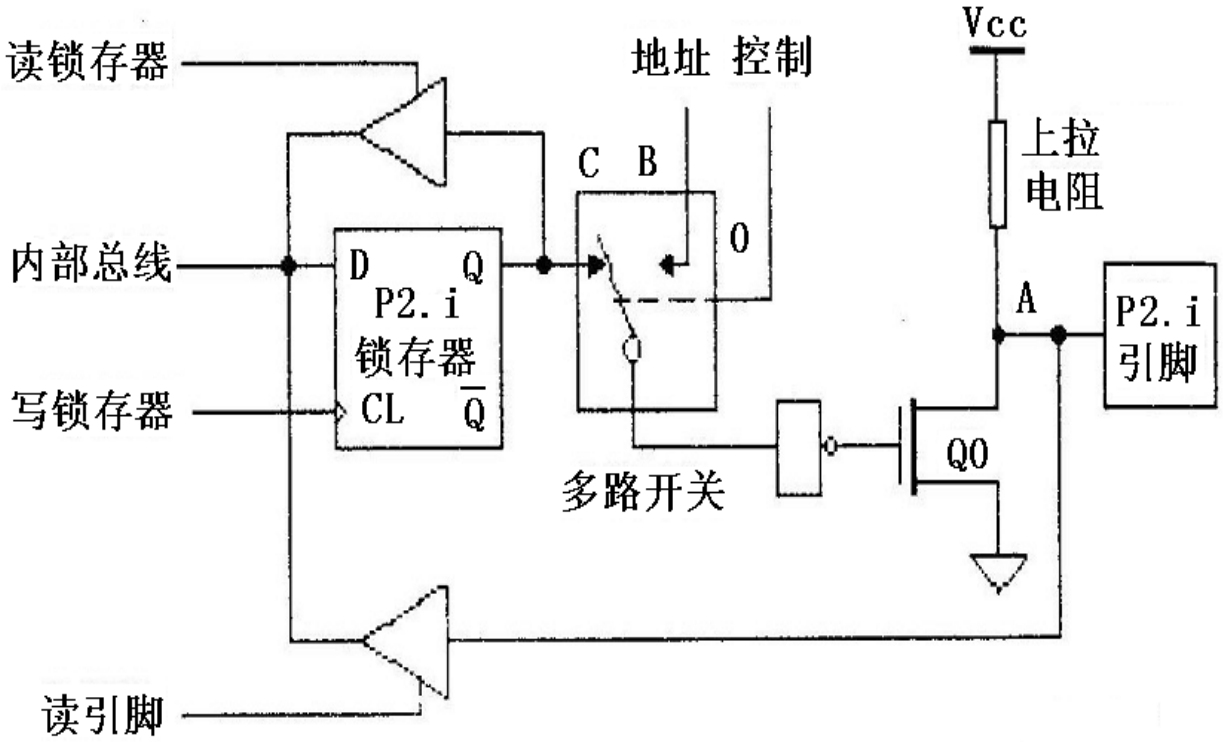
- P1口(续)
  - P1口的多功能线
    - 在80C52中，P1.0和P1.1口线是多功能的，即除作一般双向I/O口线之外，这两根口线还具有下列功能：

      P1.0—定时器/计数器2的外部输入端T2；

      P1.1—定时器/计数器2的外部控制端T2EX

并行输入/输出端口(续)

- P2口
  - P2口是准双向口。 P2口是一个多功能的8位口，可以字节访问也可位访问，其字节访问地址为A0H，位访问地址为A0H～A7H

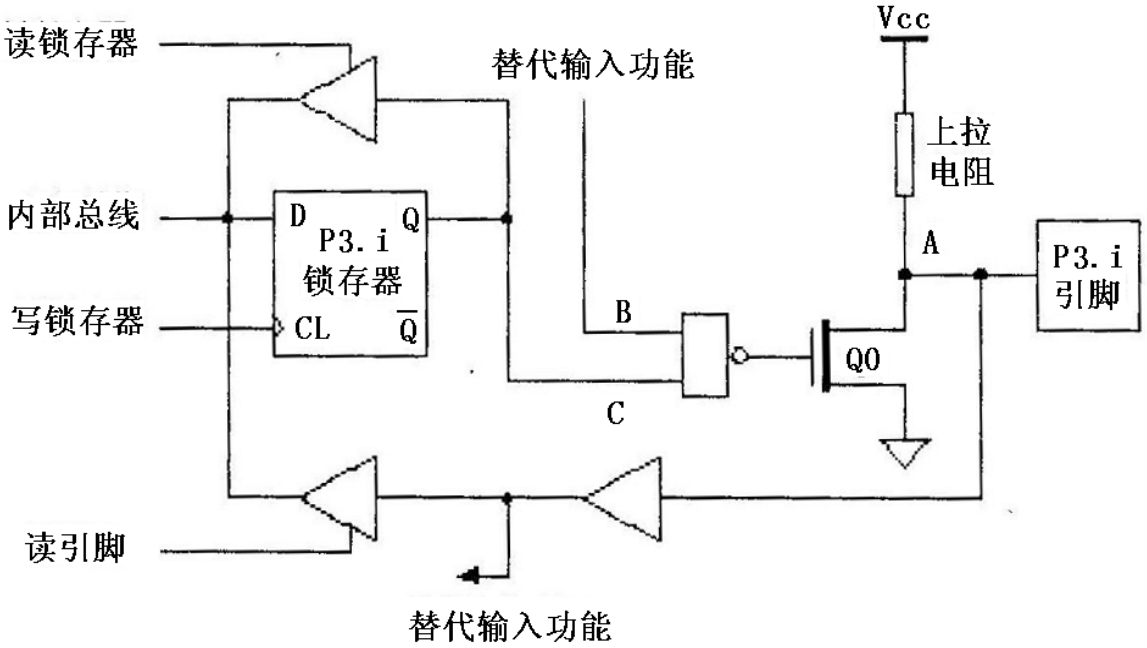


并行输入/输出端口(续)

- P2口(续)
  - P2口的功能
    - 作I／O口使用时，P2口为一准双向口
    - 作地址输出时，P2口可以输出程序存储器或片外数据存储器的高8位地址，与P0输出的低地址一起构成16位地址线

并行输入/输出端口(续)

- P3口
  - P3口是一个多功能的8位口，可以字节访问也可位访问，其字节访问地址为B0H，位访问地址为B0H～B7H
  - 有两个输入缓冲器，第二输入功能取自第一个缓冲器的输出端；I/O口的通用输入信号取自第二个缓冲器的输出端



并行输入/输出端口(续)

- P3口(续)
  - P3口是一个多功能口
    - 可作I/O口使用，为准双向口。 既可以字节操作，也可以位操作；既可以8位口操作，也可以逐位定义口线为输入线或输出线；既可以读引脚，也可以读锁存器，实现“读一修改一输出”操作
    - 可以作为第二(替代)功能的输入、输出

第二输入功能：

P3.0 —— RXD，串行输入口

P3.2——/INT0，外部中断0的请求

P3.3——/INT1，外部中断1的请求

P3.4 —— T0，定时器/计数器0外部计数脉冲输入

P3.5 —— T0，定时器/计数器0外部计数脉冲输入

第二输出功能：

P3.1 ——TXD，串行输出口。

P3.6 ——/WR，外部数据存储器写选通，输出

P3.7 ——/RD，外部数据存储器读选通，输出

80C51存储器扩展

- 扩展ROM的地址与芯片内是否有程序存储器有关，如果没有片内程序存储器，扩展ROM的地址从0000H开始，如果有片内程序器，则扩展ROM的地址从1000H开始
- 扩展RAM的地址，不管容量大小，都是从0000H开始

- 如何使用系统提供的地址线，通过适当连接，使系统中的一个存储单元只唯一地对应一个地址，存储器编址分两个层次
  - 存储芯片的选择，实质就是如何产生芯片的“片选”信号
  - 芯片内部存储单元的编址，是由芯片自身的译码电路完成的，只需把存储器芯片的地址引脚与相应的系统地址线直接连接即可

80C51存储器扩展(续)

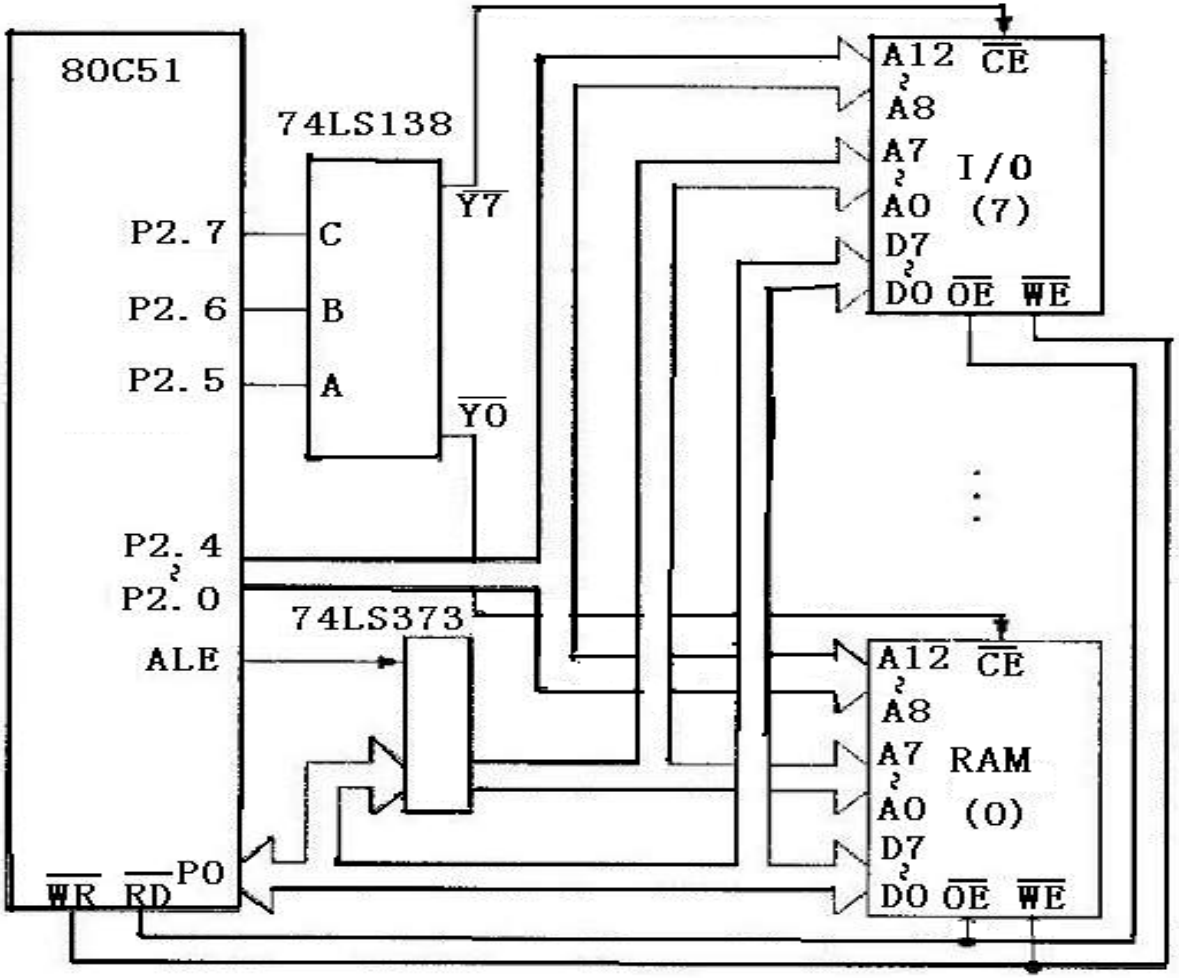
- “片选” 保证每次读或写时，只选中某一片存储器芯片或I/O接口芯片
- 通常把单片机系统地址笼统地分为低位地址和高位地址，芯片内部存储单元地址译码使用低位地址，剩下的高位地址才作为芯片选择使用实际上
- 除了研究地址线的连接外，还讨论各存储器芯片在整个存储空间中所占据的地址范围
- 常用的芯片选择方法（寻址方法）
  - 线选法：利用单片机系统的位地址信号（如P2.7）作为某一片存储器芯片或I/O接口芯片的“片选” 控制线，用于扩展芯片较少的场合
  - 译码法：用译码器对高位地址线进行译码，译码器的输出作为“片选”控制线。常用译码器有3/8译码器74LS138、双2/4译码器74LS139、4/16译码器74LS154等。它们的CMOS型芯片分别是74HC139、74HC138、74HC154

80C51存储器扩展(续)

- 常用的芯片选择方法 --- 译码法(续)
  - 74LS139片中有两个2-4译码器
    - /G-使能端，低电平有效。
    - A、B-选择端，即译码输入，控制译码输出的有效性。
    - /Y0、/Y1、/Y2、/Y3-译码输出信号，低电平有效。
    - 74LS139对两个输入信号译码后得到4个输出状态
  - 74LS138译码器
    - G1、/G2A、/G2B：使能端。当G1=1、/G2A=/G2B=0时，芯片使能
    - C、B、A：译码器输入，高电平有效
    - /Y0~/Y7：译码器输出，低电平有效。正常情况下，只有一根输出是低电平，其余输出都是高电平。当译码器输出作为单片机应用系统中外扩芯片的片选控制线时，保证每次读或写时只选中一个芯片

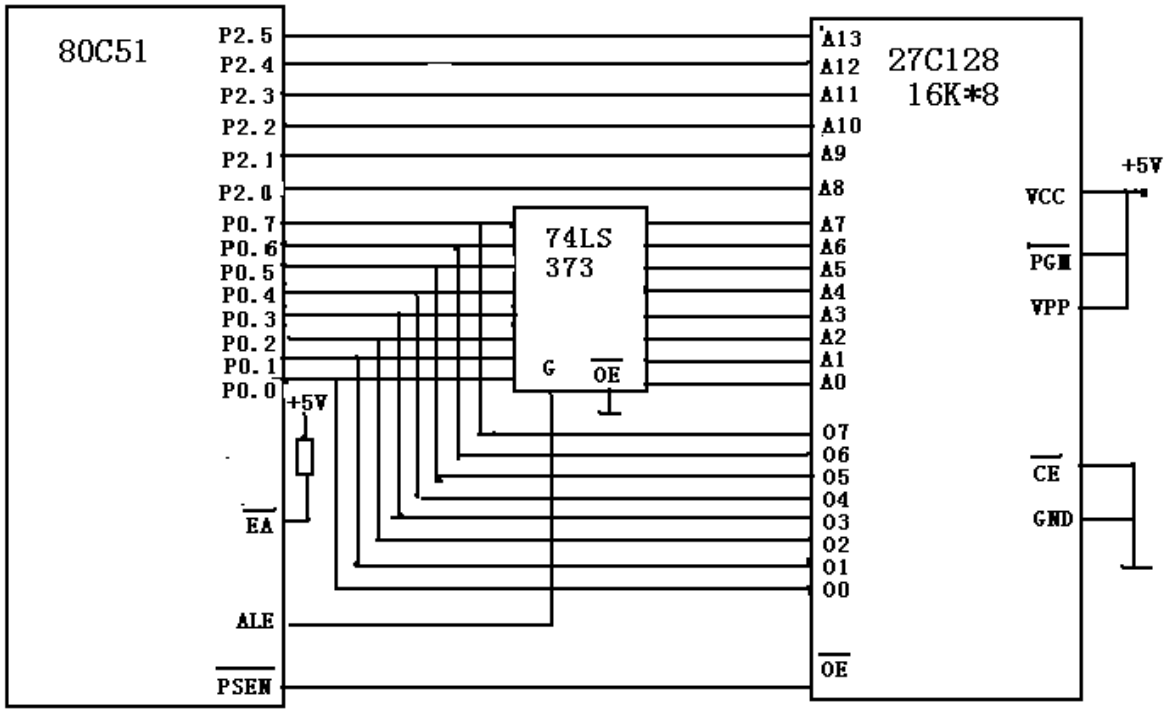
80C51存储器扩展(续)

- 常用的芯片选择方法 --- 译码法(续)



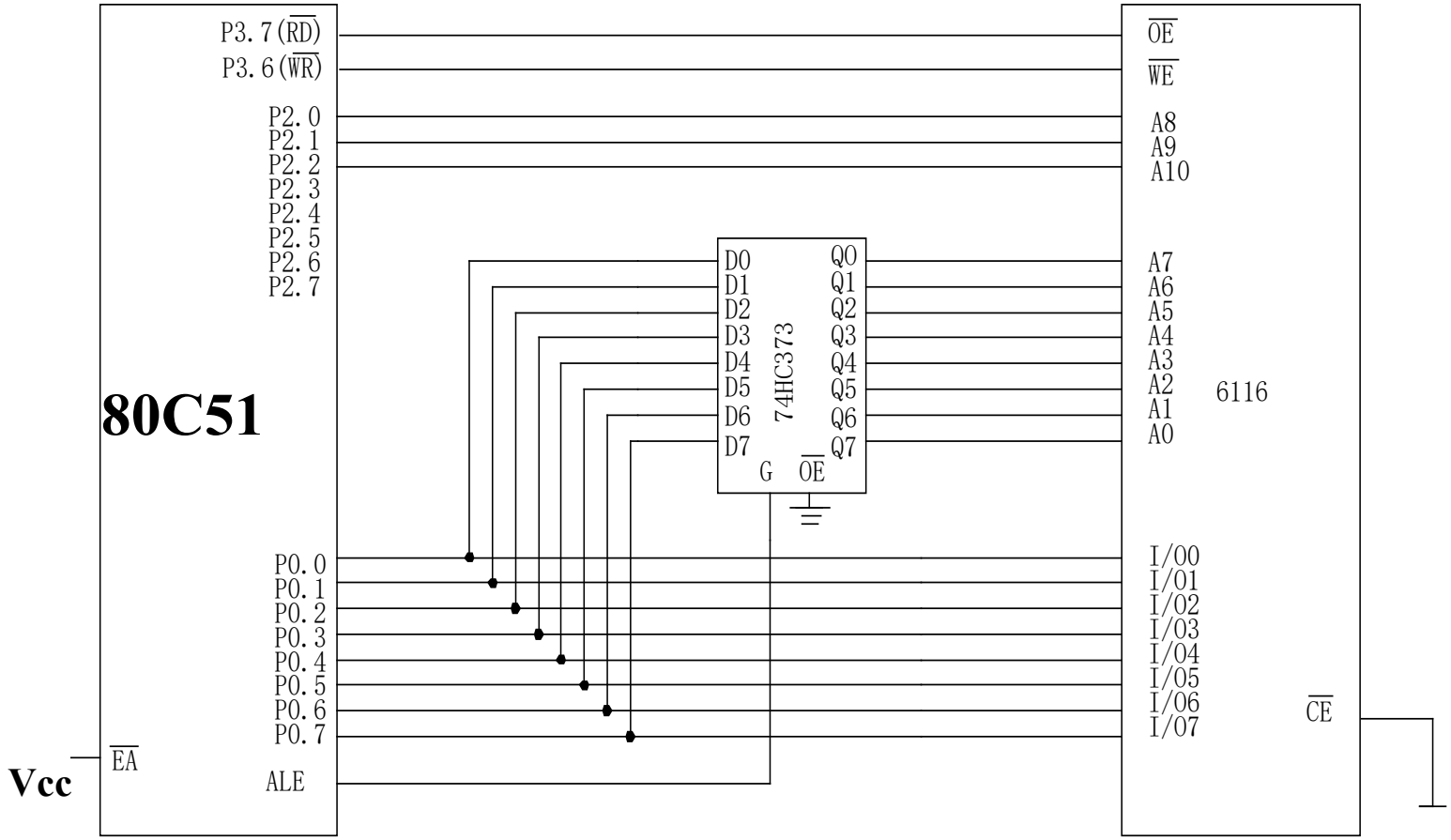
80C51存储器扩展(续)

- ROM扩展(续) --- 程序存储器扩展举例
  - 扩展16K *8位片外程序存储器
    - 在电路中/EA是接高电平的。27128A是16KB容量的EPROM，所以用到了14根地址线A0～A13。系统中只扩展了一片程序存储器，所以27128A的片选端可直接接地，一直有效



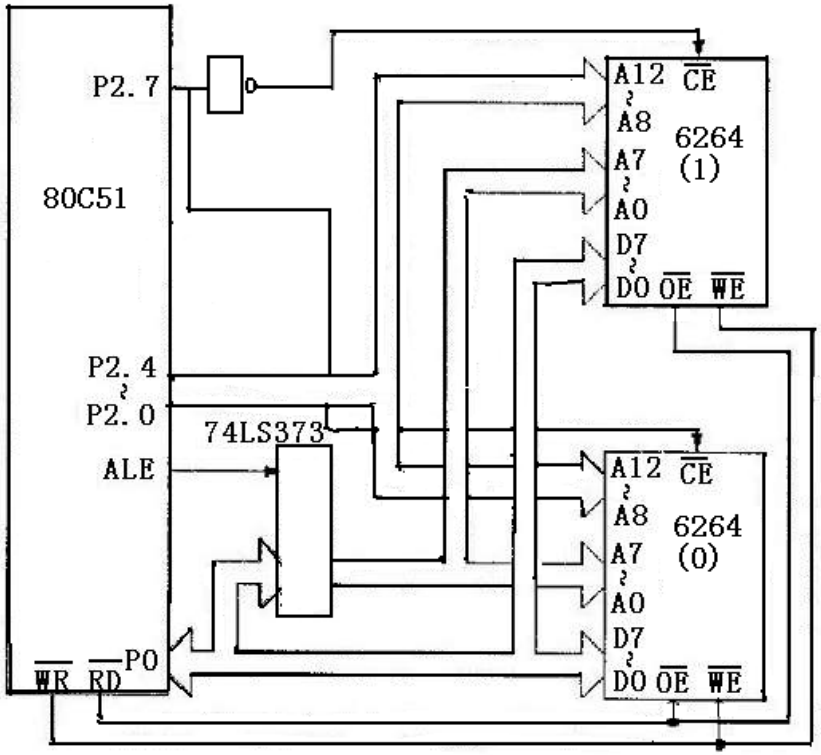
80C51存储器扩展(续) --- RAM扩展(续)

- RAM扩展举例(续)
  - 单片数据存储器扩展(续)



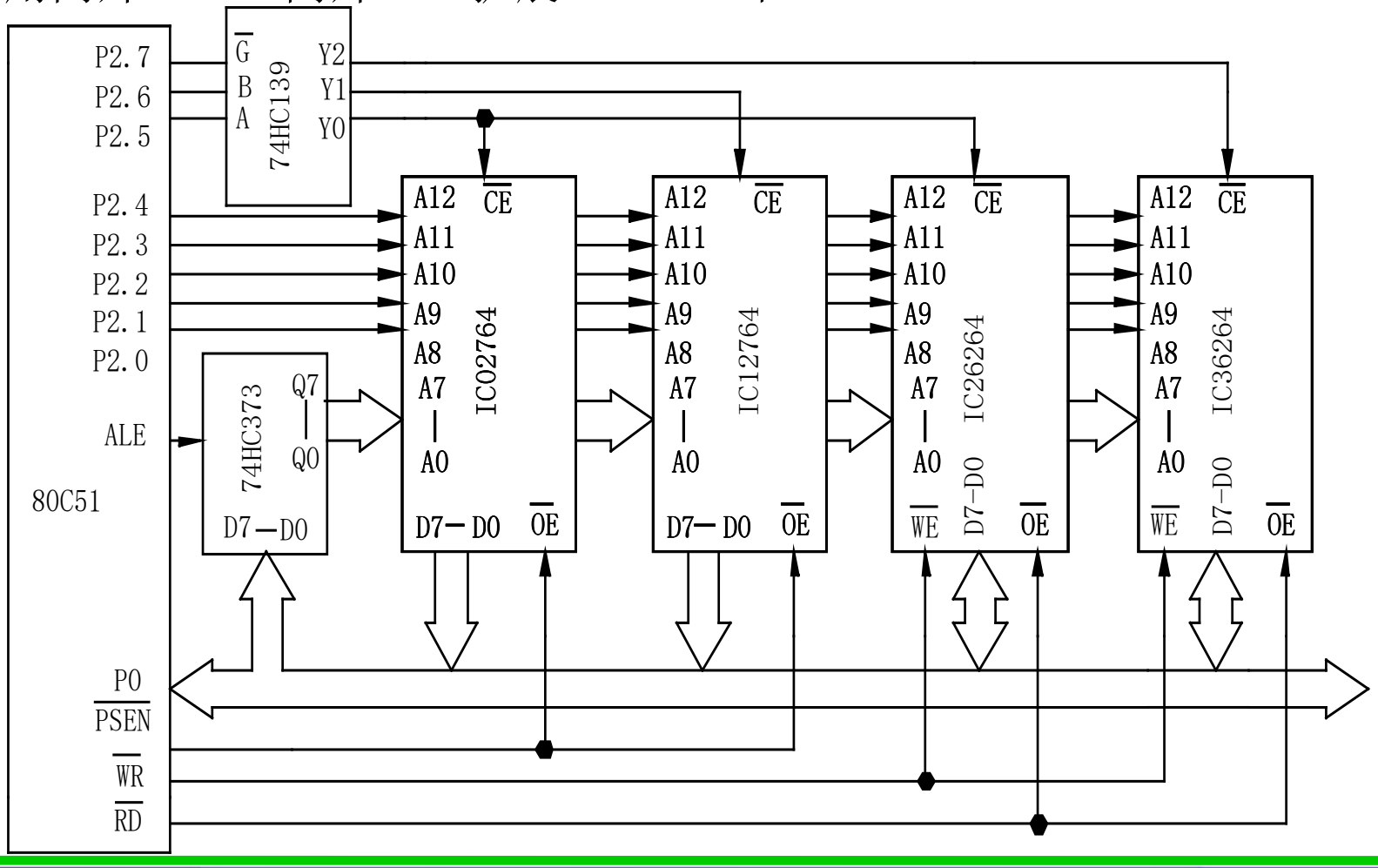
80C51存储器扩展(续) --- RAM扩展(续)

- RAM扩展举例(续)
  - 线选法多片存储器扩展
    - 如图所示的是用两片6264扩展16K*8位片外数据存储器的电路。
    - 在图中，采用线选法寻址。用一根口线P2.7来寻址：当 P2. 7=0时，访问片(0)，地址范围为6000H～7FFFH；当P2.7=1时，访问片(1)，地址范围为E000H～FFFFH



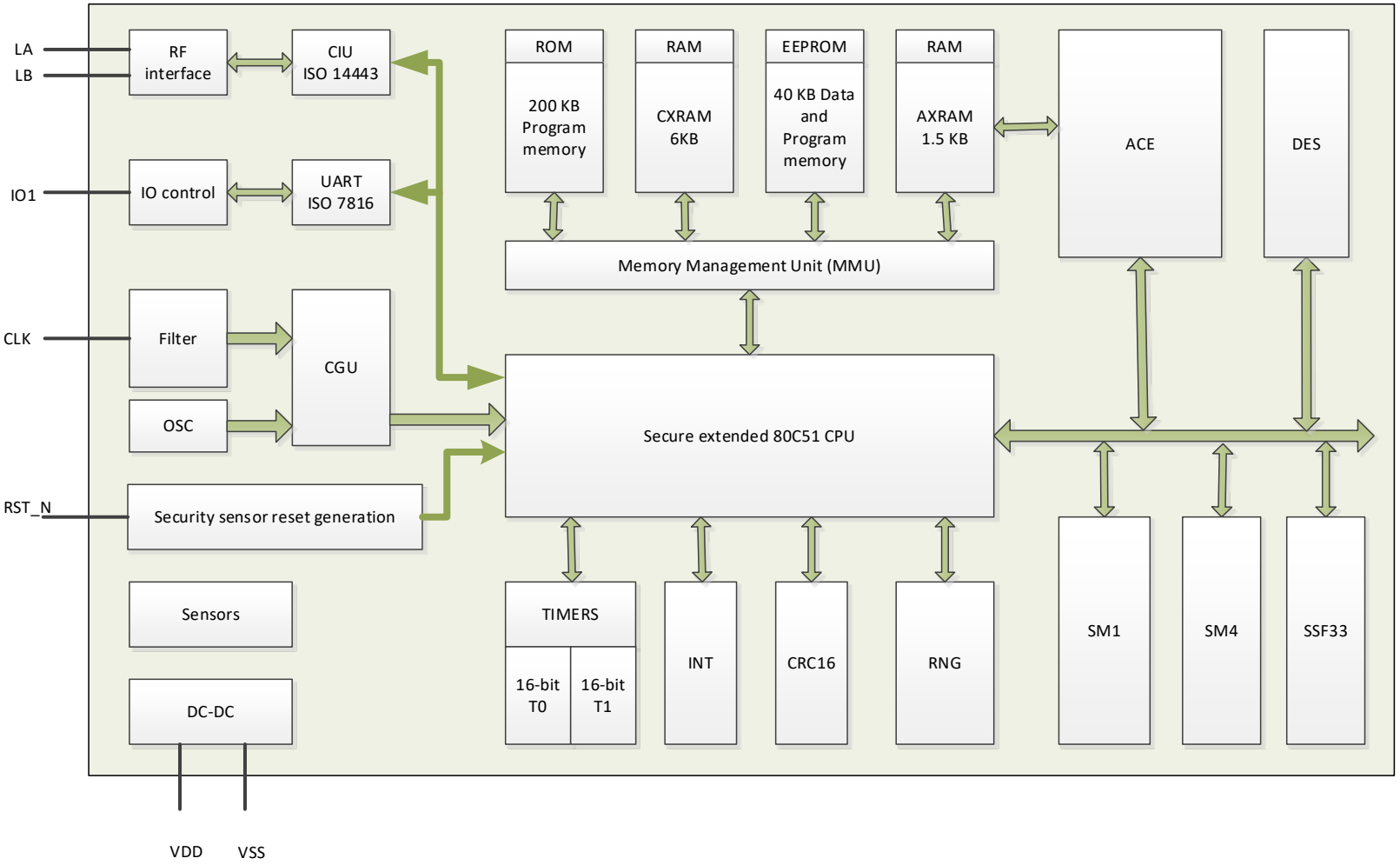
80C51存储器扩展(续) --- 综合扩展

- 同时扩展程序存储器和数据存储器
  - 用两片6264、两片2764扩展16KB RAM和16KB EPROM

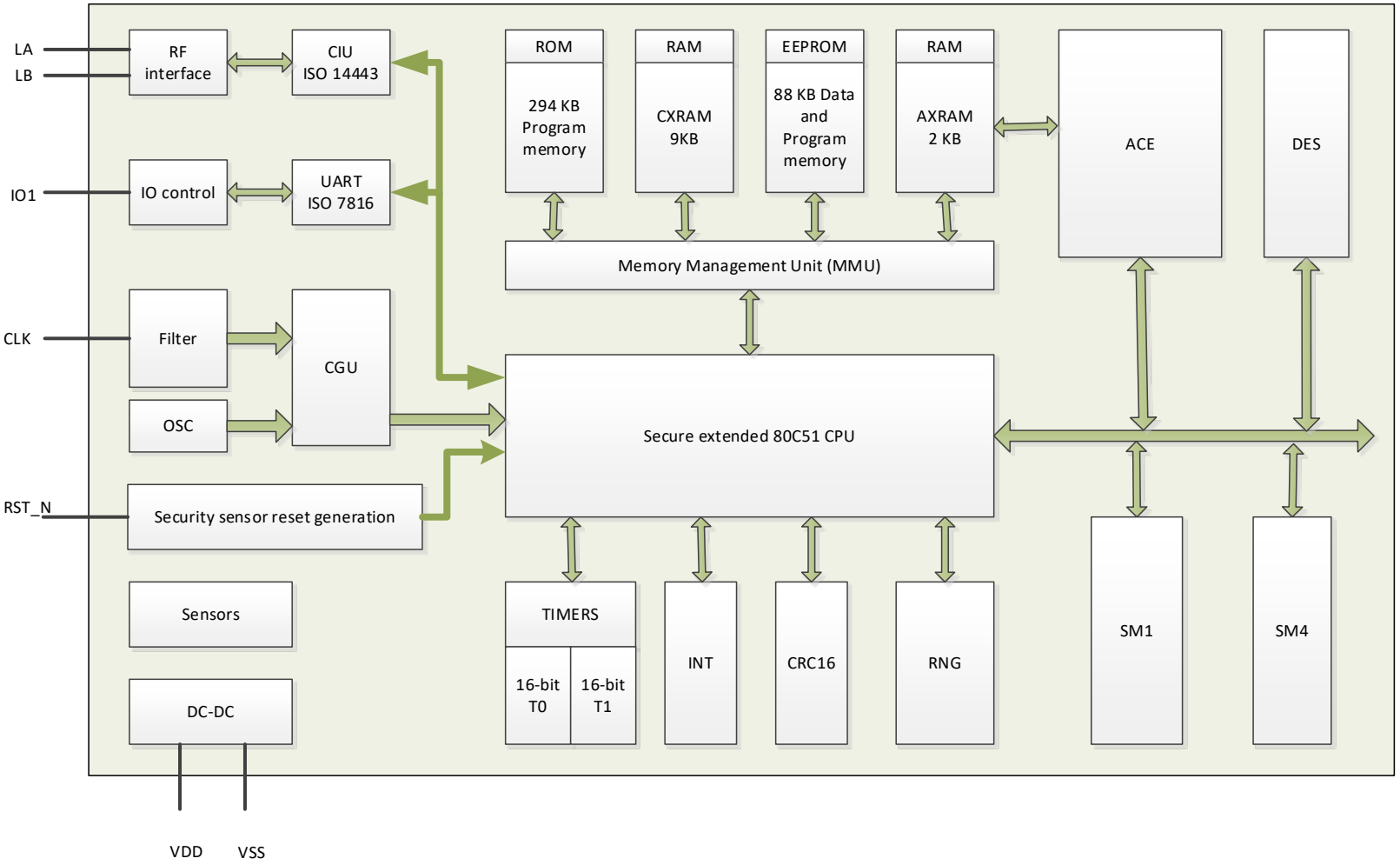


基于8051处理器的CVF安全芯片

芯片组成-CVF1040D



芯片组成-CVF1088D



技术指标-整体技术指标

- 使用台积电 CMOS 14-1P5M和ROM掩膜工艺；
- CVF1040D容量为200KB ROM、40KB EEPROM、7.5KB RAM；
- **CVF1088D容量为294KB ROM、88KB EEPROM、11KB RAM；**
- **扩展80C51的低功耗安全处理架构，最高**时钟频率72MHz；
- 采用32位高性能、低功耗算法加速协处理器，**最高时钟频率72MHz**；
- 支持32个外部中断源，4级中断优先级；
- **支持硬件补丁机制；**
- **同时支持接触界面和可选触的非接界面。**

技术指标-电气特性和通讯接口

- 支持低功耗模式：自动打盹模式、休眠模式、IDLE模式
- 供电电压：1.62V-5.5V， 内核电压：1.8V
- 典型功耗：12mW， 支持低功耗模式，最低功耗小于30uA
- 典型工作电流：12mA @ 36MHz
- 最大工作电流：32mA @ 36MHz
- 工作温度：-25℃ ~ +85℃
- ESD保护：4000V以上
- 支持ISO/IEC 7816接口，接口时钟频率为1-12MHz
- 支持ISO/IEC 14443 Type A/B射频协议，波特率106K/212K/424K/848Kbps，正常工作场强范围1.5A/m~7.5A/m

技术指标-安全性功能指标

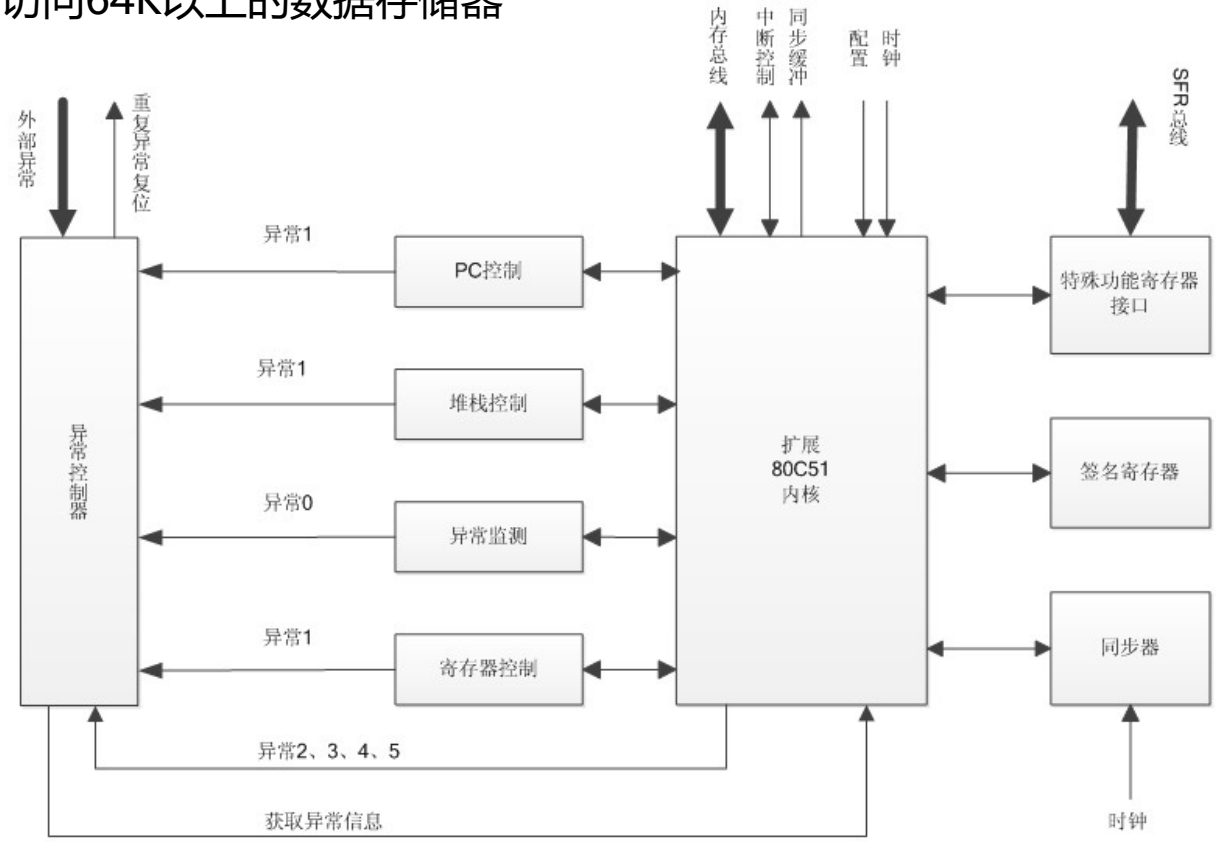
- SM2算法、RSA2048算法、SM3算法使用软硬协同实现：
- 硬件采用高级加密引擎ACE，ACE支持大数（2048比特）模乘、模幂、乘法运算协处理；
- 软件由安全算法库完成，并由安全算法库提供用户接口；
- SM2密码算法模块：支持签名和验证、密钥生成；
- RSA2048密码算法模块：支持签名和验证、密钥生成。
- SM1、SM4和SSF33密码算法支持ECB模式，加解密由硬件完成，通过安全算法库提供用户接口。
- 真随机数发生器遵循国密局《随机性检测规范》技术要求。

安全特性

- 安全检测与防护单元：高低电压检测、高低频率检测、高低温检测、光照检测、电源毛刺检测
- 超级用户模式、系统模式、用户模式三级安全机制，采用独立寄存器组
- 独立的电源模块、内部时钟模块和内部复位逻辑
- 主动防护层检测
- 安全存储分区和存储区访问控制
- 存储区加密、校验
- 总线加扰、CPU时钟加扰
- 异常中断日志存储
- 运行时数据签名
- 安全固件输入参数检查
- 过程检查、 随机延时
- 关键路径检查、处理分支消除
- 密钥导入随机化、 RAM随机化

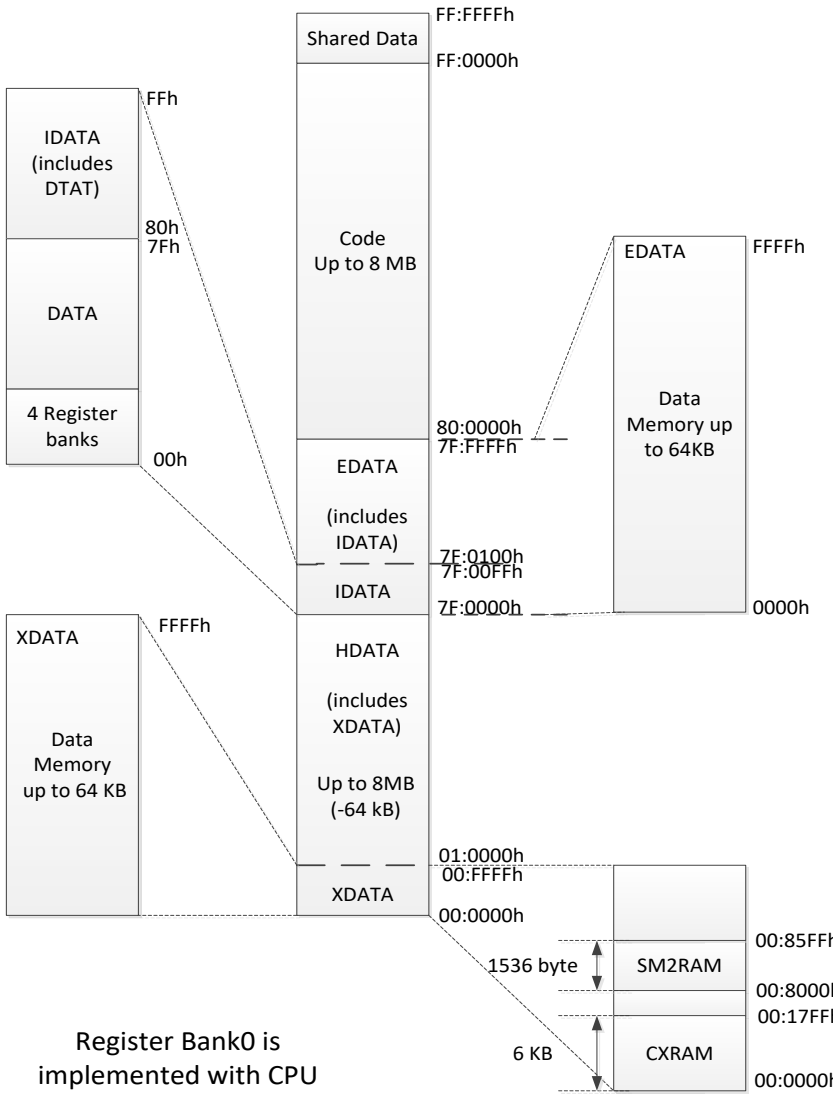
CPU

- **增加新的寻址模型，支持对所有除SFR外数据和代码区的单指令访问**
- **增加两个独立可选的堆栈模式，压栈地址可扩展到24位，支持栈空间可扩展**
- 新增24位数据指针，以方便访问64K以上的数据存储器
- **程序指针扩展到24位**



- 三种工作模式
  - 超级系统模式
  - 系统模式
  - 用户模式

存储器映射



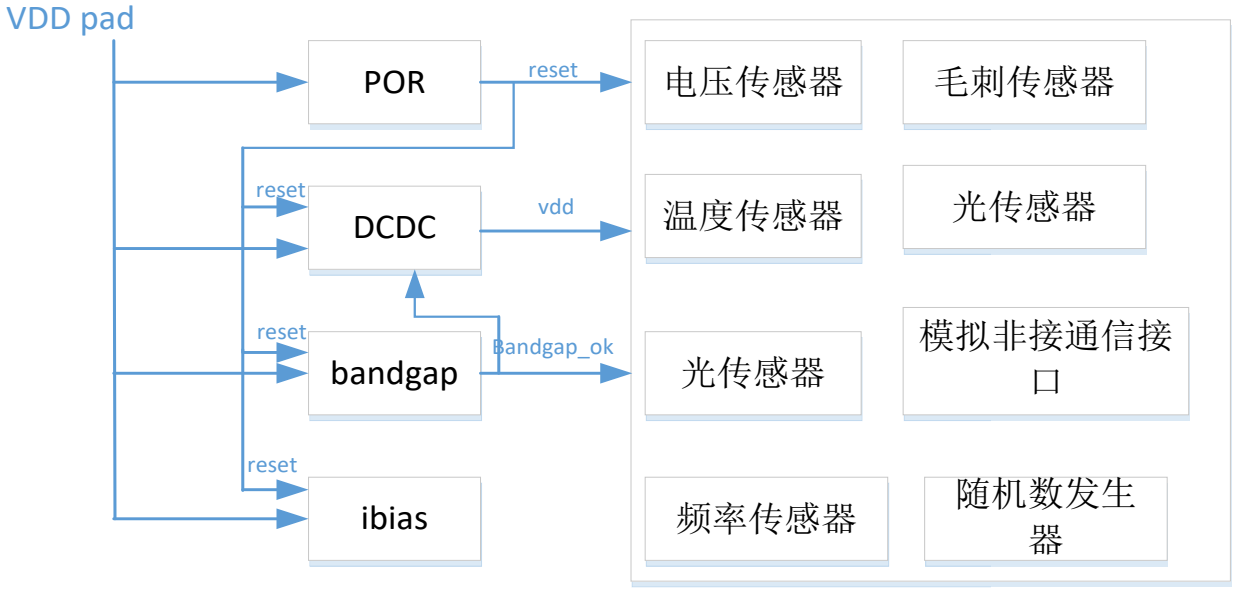
- 存储器采用统一编址
- RAM Shell通过MMU建立起RAM与CPU之间的连接，包括RAM本身以及RAM接口两部分
- 两种不同的RAM块，CXRAM只能通过MMU访问；AXRAM可被MMU和ACE访问，其中ACE拥有优先权
- AXRAM内含32位数据总线的SRAM硬核，再加上一些控制逻辑、数据加解密、地址加密逻辑
- CXRAM内含16位数据总线的SRAM硬核，再加上一些控制逻辑、数据加解密、地址加密逻辑

启动流程

- 芯片启动的顺序是模拟电路、数字电路、引导程序、芯片操作系统。
- 引导程序（BOOT程序）并决定进入芯片操作系统进入系统模式还是进入测试模式。
- 如果芯片进入系统模式，所有的防攻击措施全部生效，而在测试模式下，部分功能和sensor是可配置的，以便于调试。

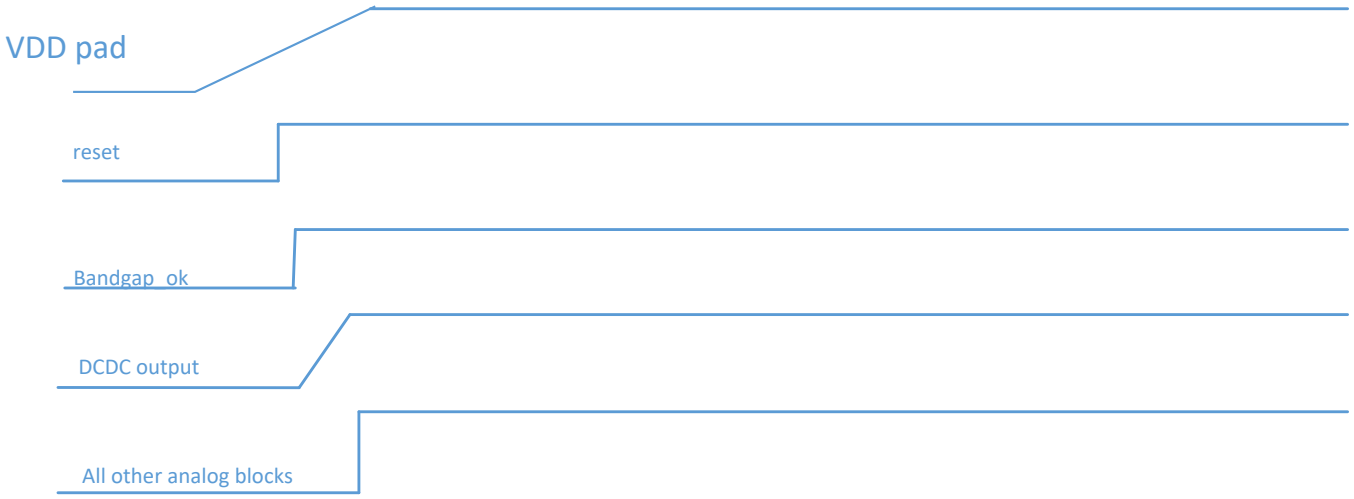
启动流程

- 模拟电路的启动流程
  - 在芯片上电的几乎同时，DCDC（）、POR（上电复位）、IBIAS（）、bandgap（带隙基准）即启动，POR模块在1.2V开始工作，即外部供电电压高于1.2V芯片即可复位。
  - Bandgap利用与温度成正比的电压与与温度成反比的电压之和，二者温度系数相互抵消，实现与温度无关的电压基准。
    - 为芯片提供一套精确的参考电压和参考电流，为所有的易受温度影响需独立供电的模拟部件供电，供电电压范围是1.1V~2.2V。输出稳定之后，产生”bandgap OK”信号。



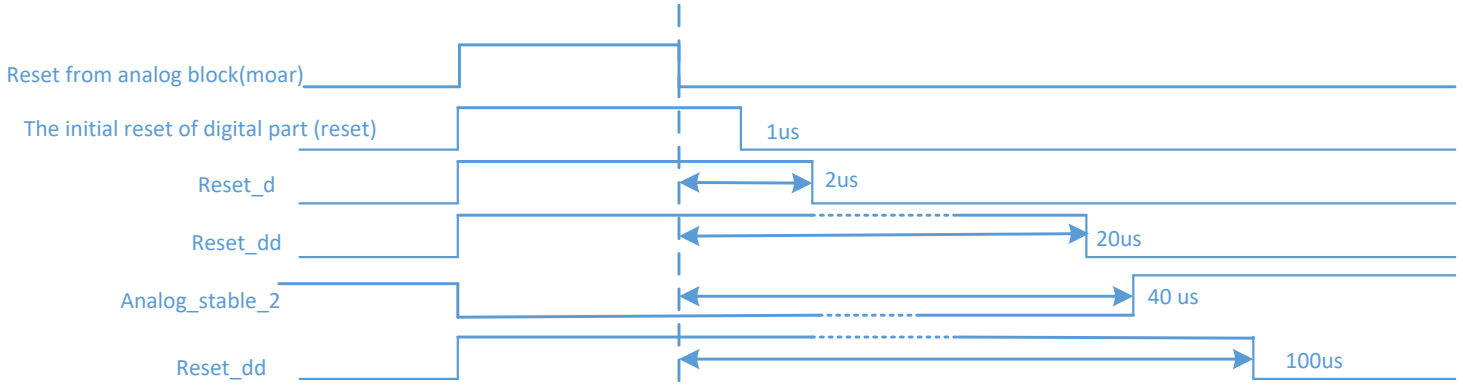
启动流程

- 模拟电路的启动流程
  - 一旦POR正常，DCDC立即启动，当接收到” bandgap OK”信号，DCDC的内部bandgap电压将来自于外部bandgap。
  - IBIAS模块的作用是通过一个反馈环产生一个基准电流，并将这个电流通过不同比例的电流镜输出至其他模块作为偏置电流。
  - 以上启动并达到稳定输出的时间小于50微秒。
  - 当bandgap输出稳定后，RC振荡器启动工作，在等待一定时间后产生稳定的内部时钟，之后所有的传感器和RNG启动，之后数字电路启动。



启动流程

- 数字电路的启动流程
  - 模拟电路启动并稳定之后数字电路激活，所有的数字模块不能同时启动，必须按时序启动。只要复位条件有效，复位逻辑始终保持在复位状态。复位条件失效，复位逻辑就会被禁止，时间为127us。
  - 复位源可被”~reset_delay”禁止，芯片若要进入测试模式必须在100us以内，以保证BootOS中没有复位发生。
  - 100us以后，所有的传感器皆可触发复位，在此之前，所有的复位源都是禁止的，不会产生复位。
  - 数字部分获得复位信号以后，大多数模块被激活。一些模块被reset_d激活，一些被reset_dd激活。而有一些模块还需等待analog_stable_2信号置位，例如频率传感器模块。



启动流程

- BOOT的流程
  - 硬件配置：
    - 1. CRC模块检查；
    - 2. RDS模块检查；
    - 3. RNG模块检查；
    - 4. EEPROM加密和RAM加密的初始化；
    - 5. 通过CRC检查EEPROM中的安全配置区首页内容的完整性；
    - 6. 通过RDS检查所有的EEPROM数据是否完整；
    - 7. 将EEPROM中的硬件配置写入RAM，然后从RAM写入SFR，检查一致性；
    - 8. 选择接口（接触式或非接触式）；
    - 9. 清除各种CPU模式所共享的寄存器。
  - 选择是进入测试模式还是系统模式。
    - 通过测试引脚输出测试多路复用器的输出信息。