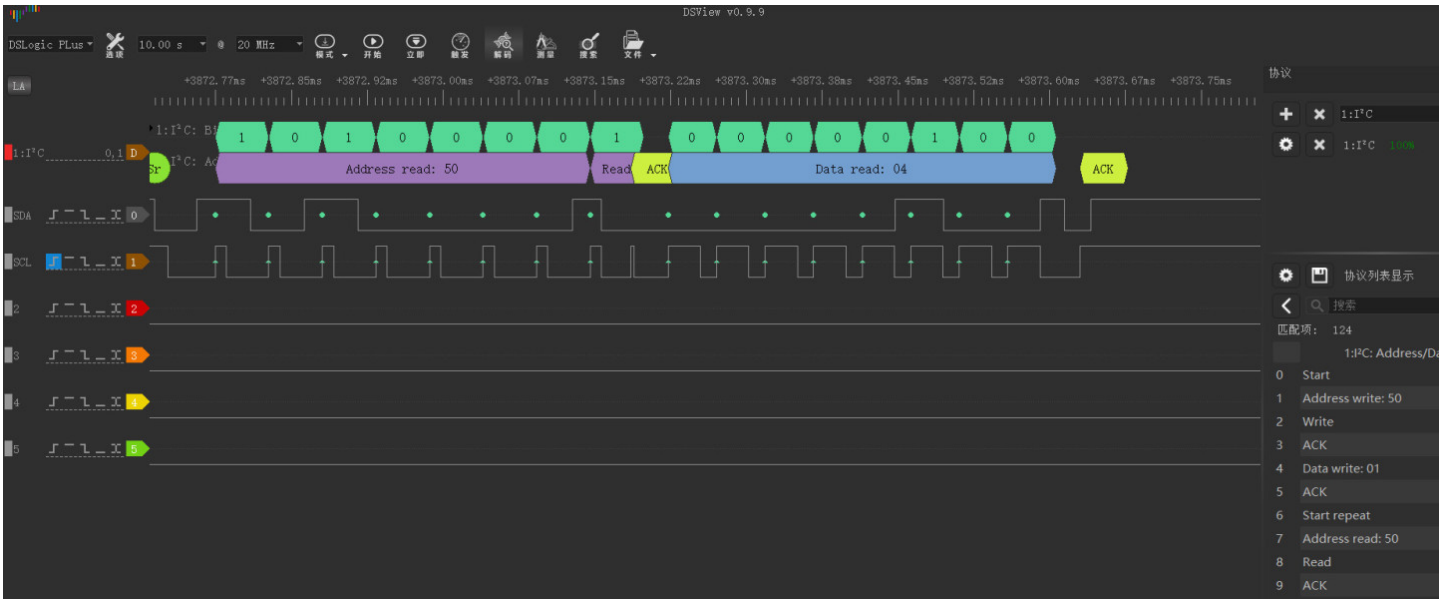


常见硬件通信协议介绍

伏宸安全...
专注物联网安全研究

关注他

61 人赞同了该文章

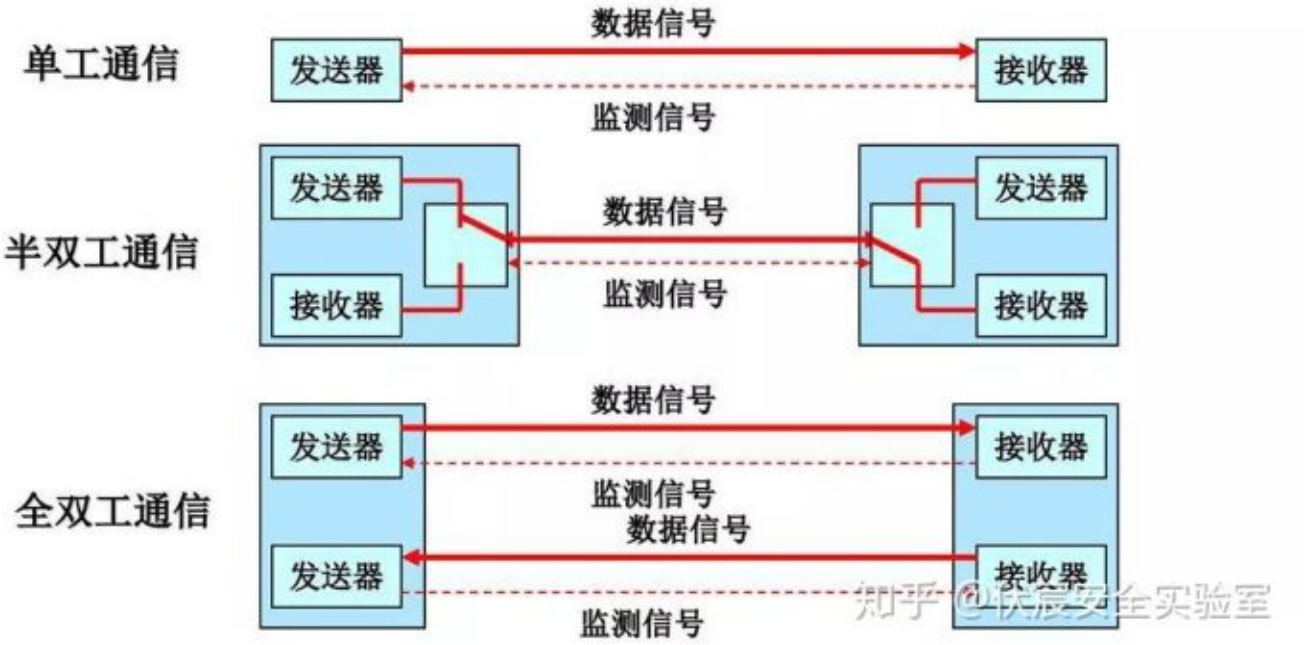
前言

完整的硬件产品是由多种模块组合实现产品功能的，微控制器 MCU 充当大脑，外围的存储单元、显示单元、发声单元、传感器单元、运动单元等等是其躯干和四肢，而不同类型的硬件单元需要有机的结合起来，就离不开相互之间的数据通信，电子工业经过了百余年的发展，衍生出了繁多的协议，其中既有行业公认的标准协议，也有企业自研的内部标准，这些协议通常可以分为并行通信协议和串行通信协议。

- 并行通信，在同一时刻发送多位数据（可以是多根线）。优点是发送速度快；缺点是传输距离短资源占用多。
- 串行通信，用一根线 在不同的时刻发送8位数据。优点是传输距离远 占用资源少；缺点是发送速度慢。

通信的方式可以分为：全双工、半双工、单工

- 单工通信 只能接受或者发送 收音机 遥控器，一般只有一根线
- 半双工通信 在同一时刻只能发送或者接收 对讲机，至少有两根线
- 全双工通信 在同一时刻 既能接收又能发送 电话，至少有两根线



根据是接收端和发送端时钟频率的异同又可分为同步通信和异步通信，本章将简单介绍主流的一些硬件通信协议。

SPI 协议

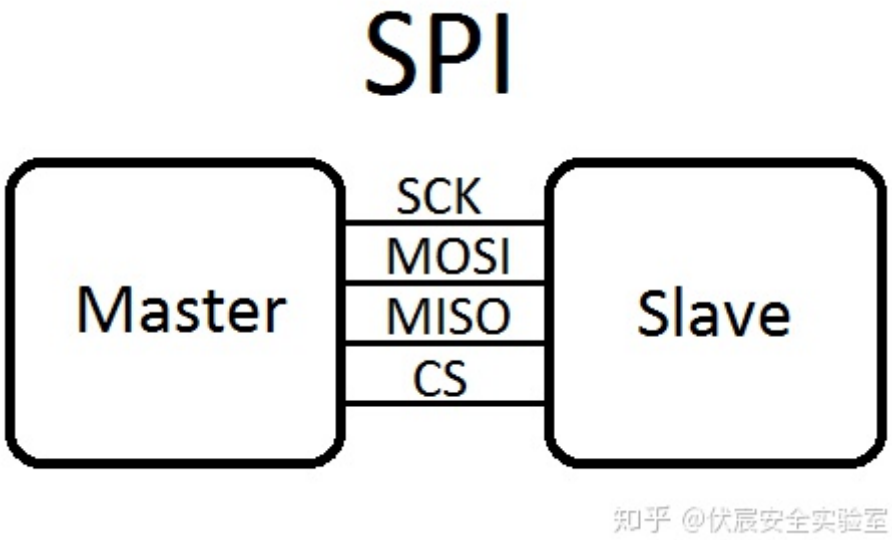
协议概括

SPI是串行外设接口（Serial Peripheral Interface）的缩写。SPI，是一种高速的，全双工，同步的通信总线，并且在芯片的管脚上只占用四根线，节约了芯片的管脚，同时为PCB的布局上节省空间，提供方便，正是出于这种简单易用的特性，如今主流的微控制器都集成有spi接口，如 stm32 家族。

通信原理

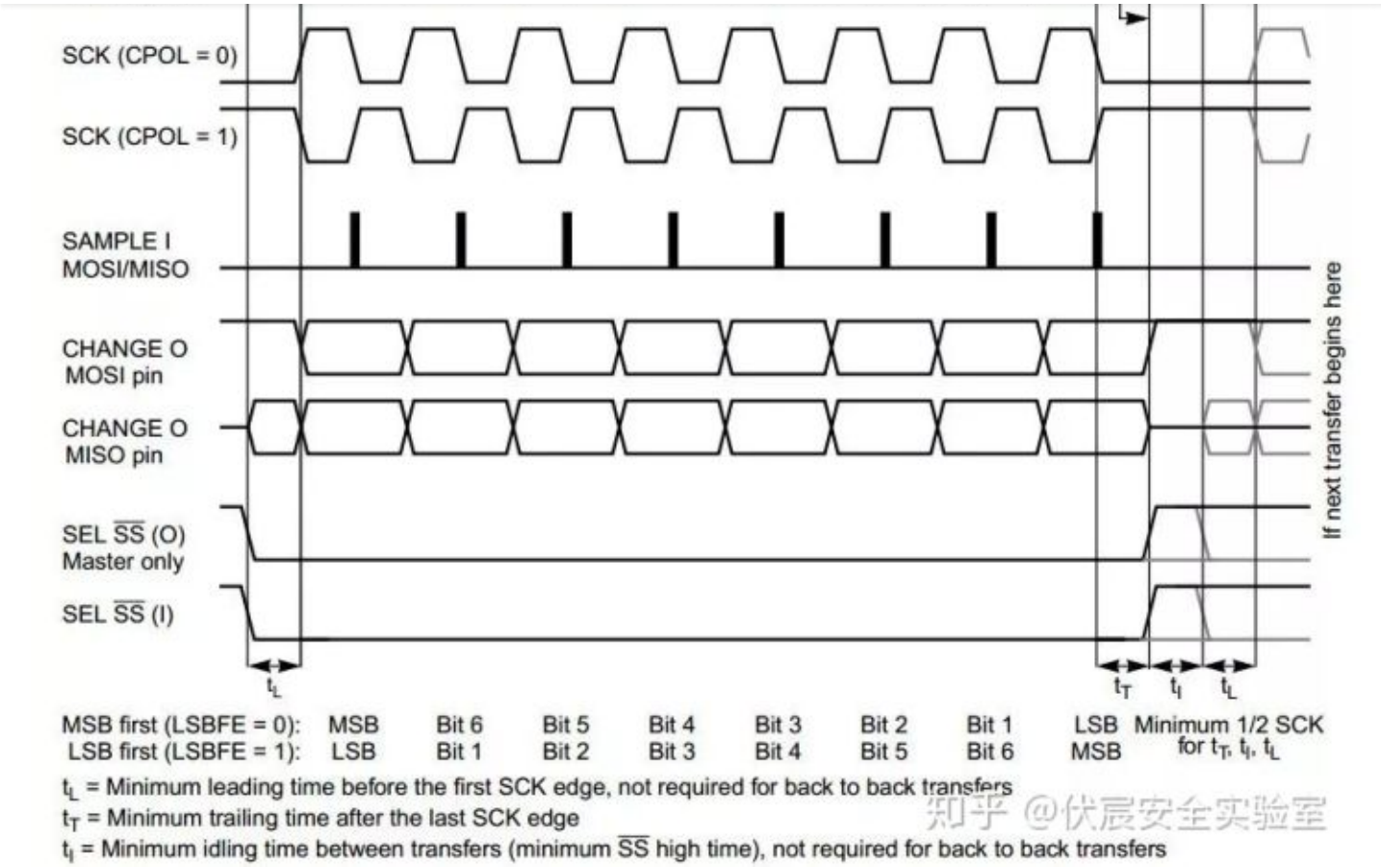
SDI（数据输入）、SDO（数据输出）、SCLK（时钟）、CS（片选）。

- SDI – SerialData In,串行数据输入；
- SDO – SerialDataOut,串行数据输出；
- SCLK – Serial Clock,时钟信号，由主设备产生；
- CS – Chip Select,从设备使能信号，由主设备控制。



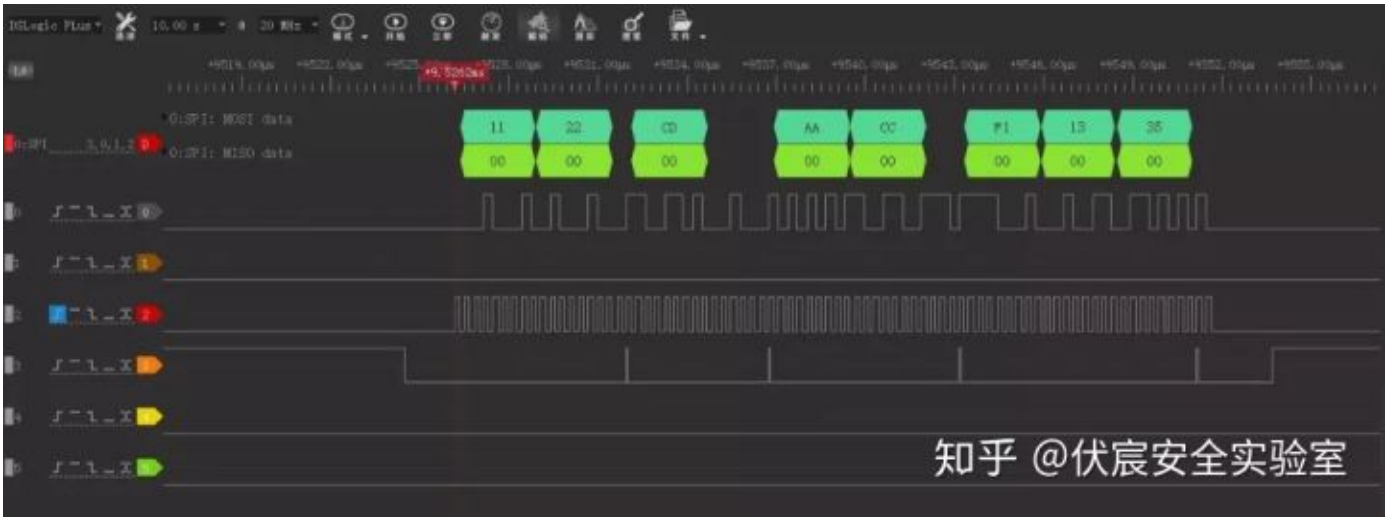
其中，CS是从芯片是否被主芯片选中的控制信号，也就是说只有片选信号为预先规定的使能信号时（高电位或低电位），主芯片对此从芯片的操作才有效。这就使在同一条总线上连接多个SPI设备成为可能。

接下来就负责通讯的3根线了。通讯是通过数据交换完成的，这里先要知道SPI是串行通讯协议，也就是说数据是一位一位的传输的。这就是SCLK时钟线存在的原因，由SCLK提供时钟脉冲，SDI，SDO则基于此脉冲完成数据传输。数据输出通过 SDO线，数据在时钟上升沿或下降沿时改变，在紧接着的下降沿或上升沿被读取。完成一位数据传输，输入也使用同样原理。因此，至少需要8次时钟信号的改变（上沿和下沿为一次），才能完成8位数据的传输。



SCLK信号线只由主设备控制，从设备不能控制信号线。同样，在一个基于SPI的设备中，至少有一个主控设备。这样传输的特点：这样的传输方式有一个优点，与普通的串行通讯不同，普通的串行通讯一次连续传送至少8位数据，而SPI允许数据一位一位的传送，甚至允许暂停，因为SCLK时钟线由主控设备控制，当没有时钟跳变时，从设备不采集或传送数据。也就是说，主设备通过对SCLK时钟线的控制可以完成对通讯的控制。

通过逻辑分析仪采集 spi 总线数据，可以看到四个通道的波形变化，判断信号的时钟周期、时钟相位和极性，并能够解码获取实际传输的数据和指令。



SPI是一个数据交换协议：因为SPI的数据输入和输出线独立，所以允许同时完成数据的输入和输出。不同的SPI设备的实现方式不尽相同，主要是数据改变和采集的时间不同，在时钟信号上沿或下沿采集有不同定义，具体请参考相关器件的文档。

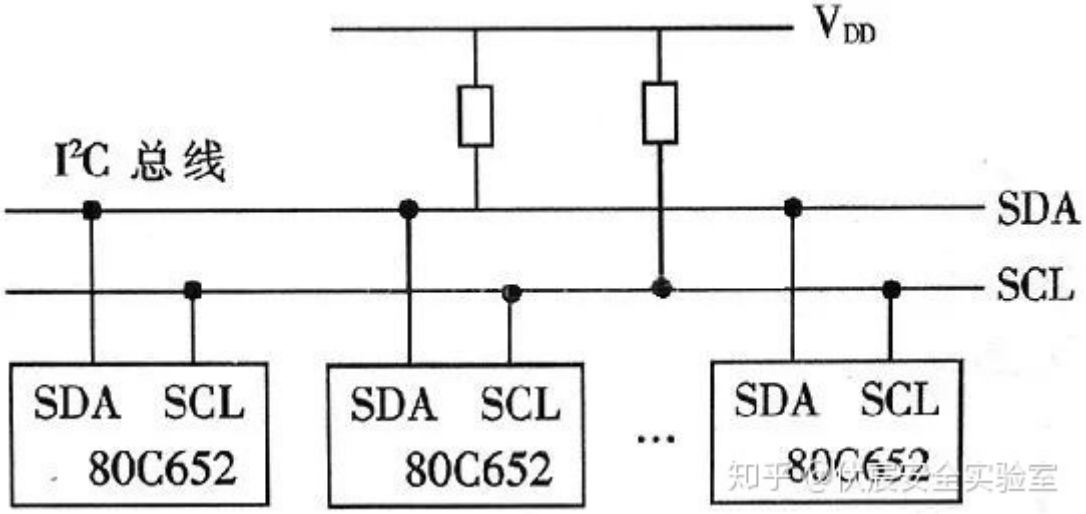
最后，SPI接口的一个缺点：没有指定的流控制，没有应答机制确认是否接收到数据。

I2C 协议

协议概括

I2C总线是由Philips公司开发的一种简单、双向二线制同步串行总线。它只需要两根线即可在连接于总线上的器件之间传送信息。

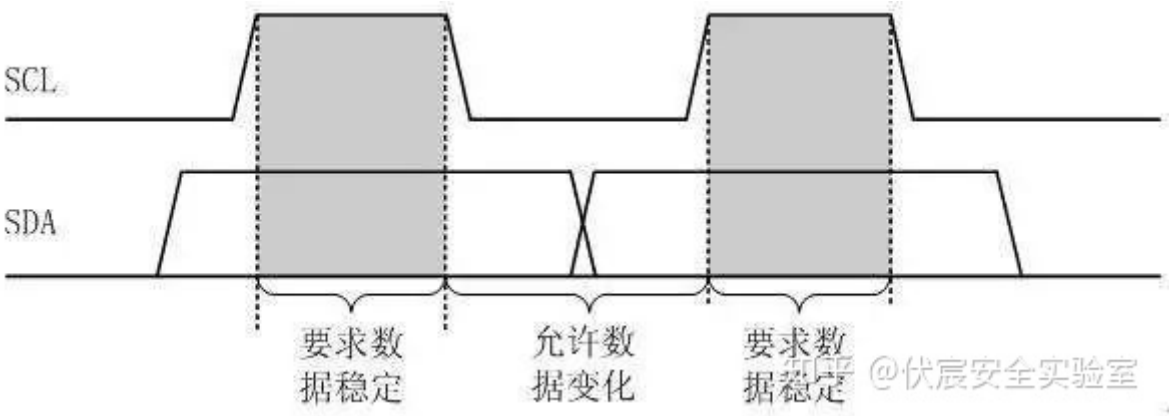
主器件用于启动总线传送数据，并产生时钟以开放传送的器件，此时任何被寻址的器件均被认为是从器件．在总线上主和从、发和收的关系不是恒定的，而取决于此时数据传送方向。如果主机要发送数据给从器件，则主机首先寻址从器件，然后主动发送数据至从器件，最后由主机终止数据传送；如果主机要接收从器件的数据，首先由主器件寻址从器件．然后主机接收从器件发送的数据，最后由主机终止接收过程。在这种情况下．主机负责产生定时时钟和终止数据传送。



通信原理

SDA（串行数据线）和SCL（串行时钟线）都是双向I/O线，接口电路为开漏输出．需通过上拉电阻接电源VCC．当总线空闲时．两根线都是高电平，连接总线的外同器件都是CMOS器件，输出级也是开漏电路．在总线上消耗的电流很小，因此，总线上扩展的器件数量主要由电容负载来决定，

数量。



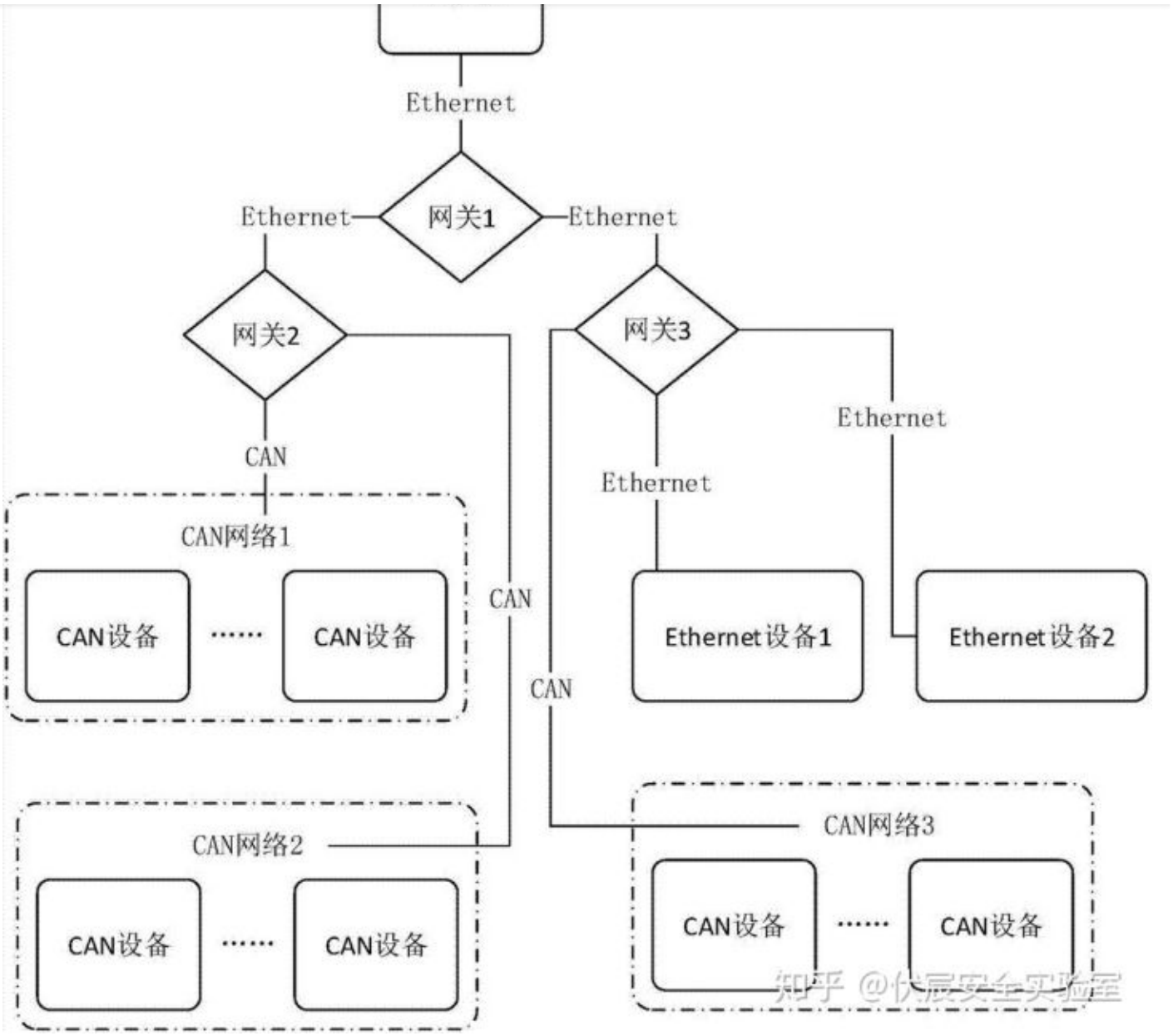
主器件用于启动总线传送数据，并产生时钟以开放传送的器件，此时任何被寻址的器件均被认为是从器件．在总线上主和从、发和收的关系不是恒定的，而取决于此时数据传送方向。如果主机要发送数据给从器件，则主机首先寻址从器件，然后主动发送数据至从器件，最后由主机终止数据传送；如果主机要接收从器件的数据，首先由主器件寻址从器件．然后主机接收从器件发送的数据，最后由主机终止接收过程。在这种情况下．主机负责产生定时时钟和终止数据传送。

逻辑分析仪采集 I2C 总线数据，可以看到 SDA 和 SCL 的数据波形，查看每次的指令和数据、地址等。

CAN 协议

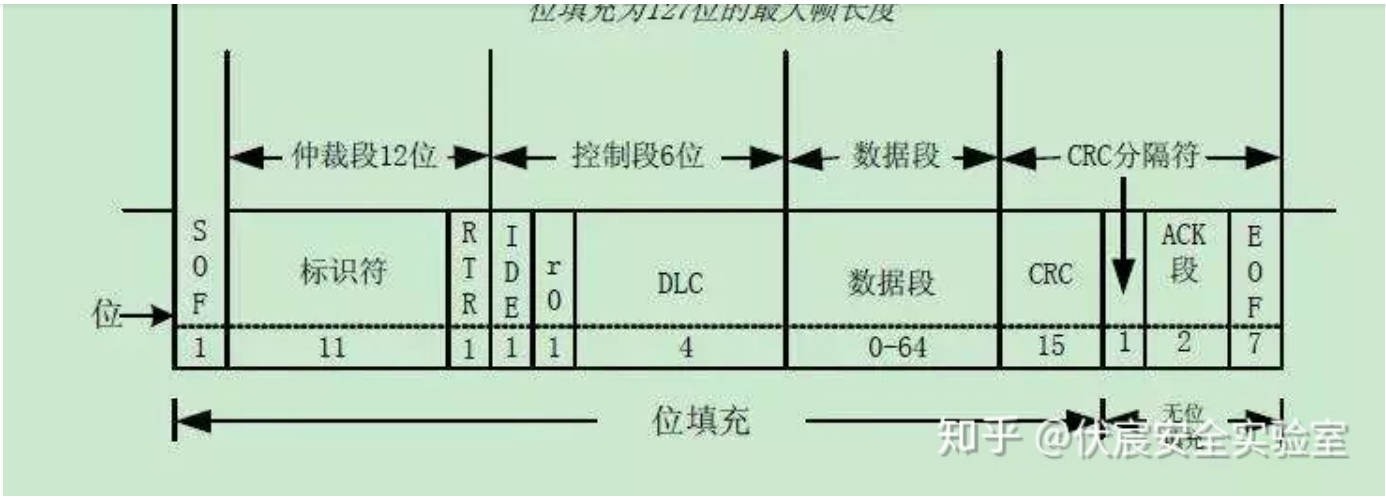
协议概括

控制器局域网总线（CAN，Controller Area Network）是一种用于实时应用的串行通讯协议总线，它可以使用双绞线来传输信号，是世界上应用最广泛的现场总线之一。CAN协议用于汽车中各种不同元件之间的通信，以此取代昂贵而笨重的配电线束。该协议的健壮性使其用途延伸到其他自动化和工业应用。CAN协议的特性包括完整性的串行数据通讯、提供实时支持、传输速率高达1Mb/s、同时具有11位的寻址以及检错能力。



通信原理

CAN总线使用串行数据传输方式，可以1Mb/s的速率在40m的双绞线上运行，也可以使用光缆连接，而且在这种总线上总线协议支持多主控制器。 CAN与I2C总线的许多细节很类似，但也有一些明显的区别。当CAN总线上的一个节点(站)发送数据时，它以报文形式广播给网络中所有节点。对每个节点来说，无论数据是否是发给自己的，都对其进行接收。每组报文开头的11位字符为标识符，定义了报文的优先级，这种报文格式称为面向内容的编址方案。在同一系统中标识符是唯一的，不可能有两个站发送具有相同标识符的报文。当几个站同时竞争总线读取时，这种配置十分重要。

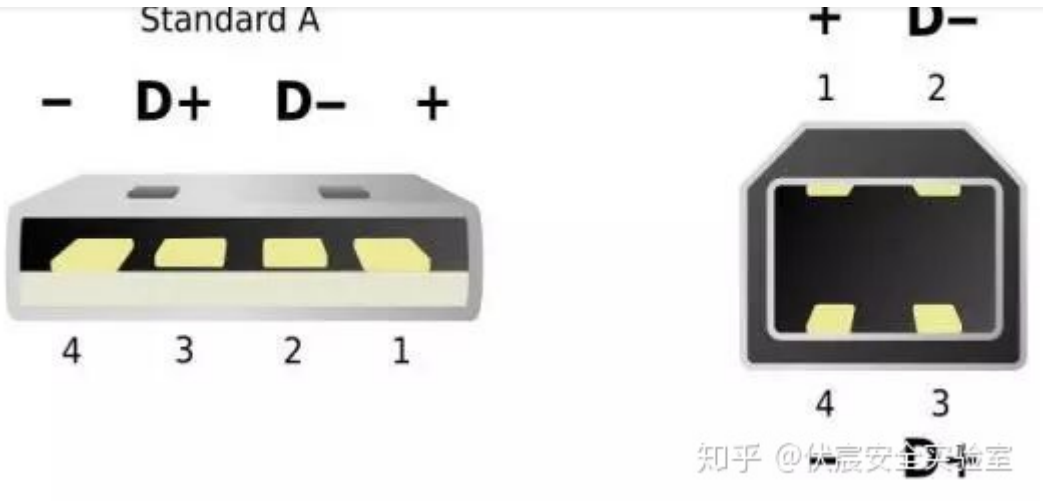


当一个站要向其它站发送数据时，该站的CPU将要发送的数据和自己的标识符传送给本站的CAN芯片，并处于准备状态；当它收到总线分配时，转为发送报文状态。CAN芯片将数据根据协议组织成一定的报文格式发出，这时网上的其它站处于接收状态。每个处于接收状态的站对接收到的报文进行检测，判断这些报文是否是发给自己的，以确定是否接收它。由于CAN总线是一种面向内容的编址方案，因此很容易建立高水准的控制系统并灵活地进行配置。我们可以很容易地在CAN总线中加进一些新站而无需在硬件或软件上进行修改。当所提供的新站是纯数据接收设备时，数据传输协议不要求独立的部分有物理目的地址。它允许分布过程同步化，即总线上控制器需要测量数据时，可由网上获得，而无须每个控制器都有自己独立的传感器。

USB 协议

协议概括

通用串行总线（英语：Universal Serial Bus，缩写：USB）是连接计算机系统与外部设备的一种串口总线标准，也是一种输入输出接口的技术规范，被广泛地应用于个人电脑和移动设备等信息通讯产品，并扩展至摄影器材、数字电视（机顶盒）、游戏机等其它相关领域。

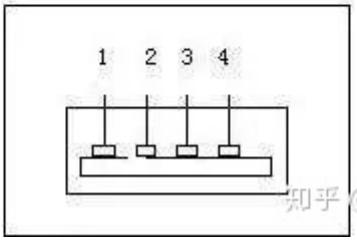


通信原理

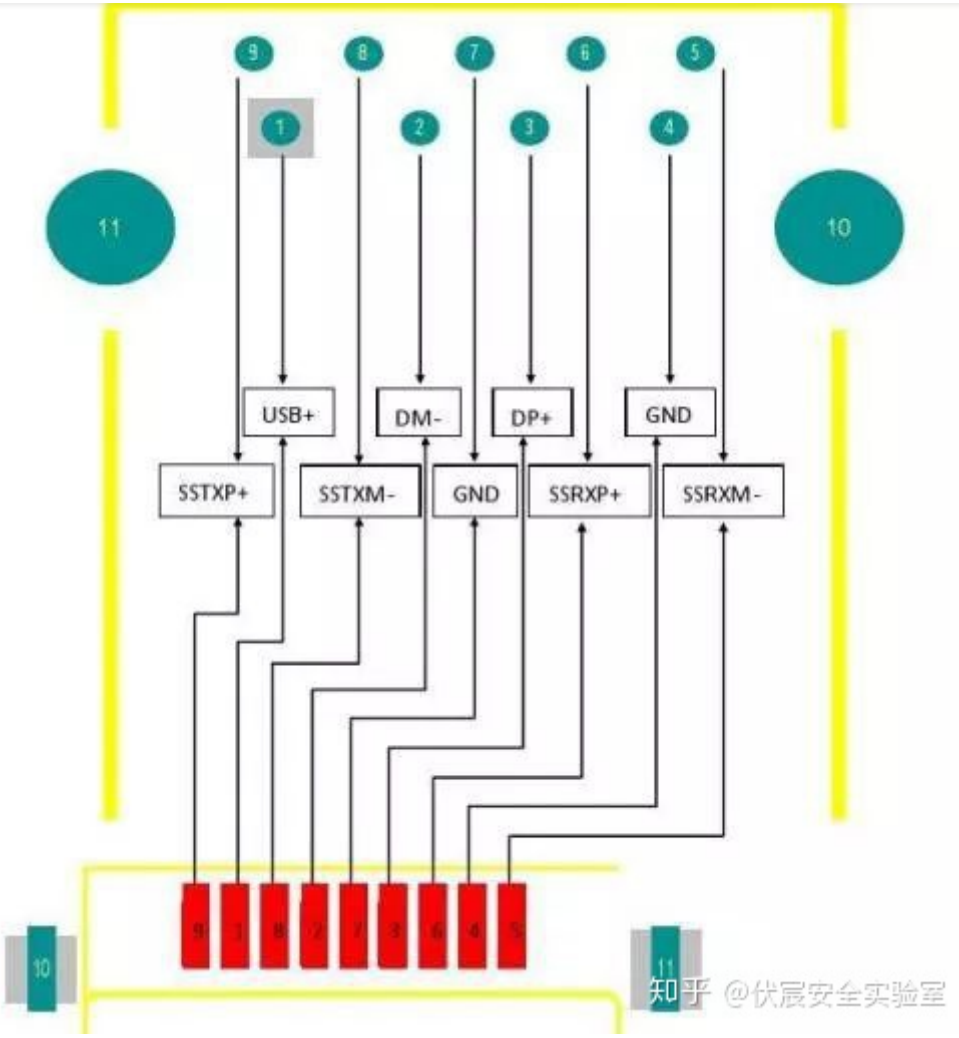
USB总线属于一种轮询式总线，主机控制端口初始化所有的数据传输。每一总线动作最多传送三个数据包，包括令牌(Token)、数据(Data)、联络(HandShake)。

按照传输前制定好的原则，在每次传送开始时，主机送一个描述传输动作的种类、方向、USB设备地址和终端号的USB数据包，这个数据包通常被称为令牌包(TokenPacket)。USB设备从解码后的数据包的适当位置取出属于自己的数据。数据传输方向不是从主机到设备就是从设备到主机。

Pin	Name	Description
1	GND	Ground
2	CLK	Clock
3	Data	Key Data
4	VCC	+5 VDC



USB 2.0 接口



USB 3.0 接口

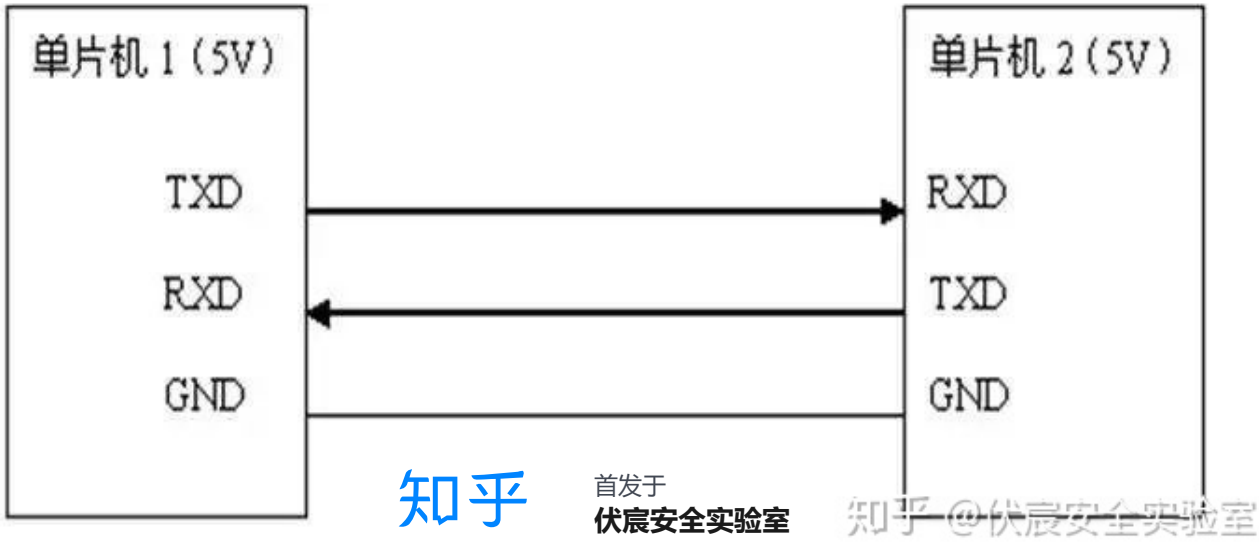
在传输开始时，由标志包来标志数据的传输方向，然后发送端开始发送包含信息的数据包或表明没有数据传送。接收端也要相应发送一个握手的数据包表明是否传送成功。发送端和接收端之间的USB数据传输，在主机和设备的端口之间，可视为一个通道。USB中有一个特殊的通道一缺省控制通道，它属于消息通道，设备一启动即存在，从而为设备的设置、状态查询和输入控制信息提供一个入口。

UART 协议

协议概括

通用异步收发传输器（Universal Asynchronous Receiver/Transmitter)，通常称作UART，是一种异步收发传输器，是电脑硬件的一部分。它将要传输的资料在串行通信与并行通信之间加以转

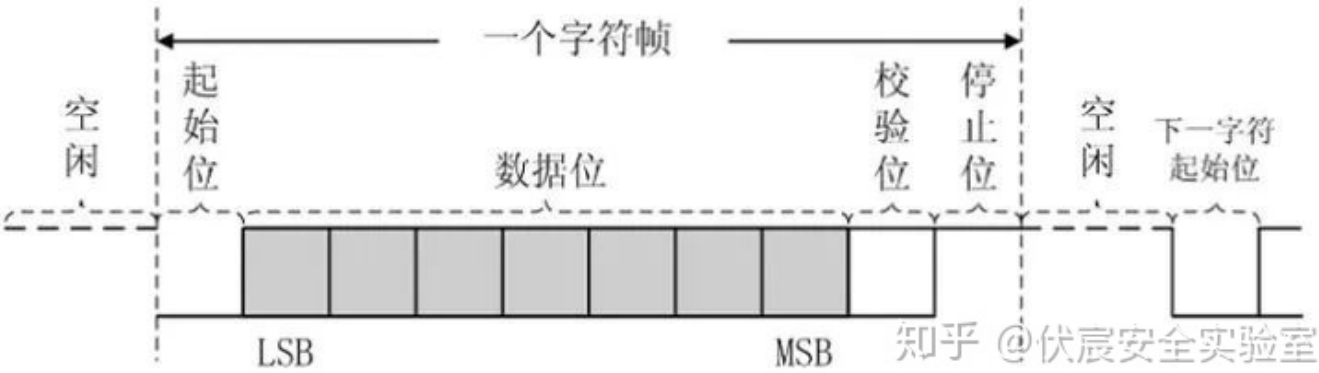
具体实物表现为独立的模块化芯片，或作为集成于微处理器中的周边设备。一般是RS-232C规格的，与类似Maxim的MAX232之类的标准信号幅度变换芯片进行搭配，作为连接外部设备的接口。在UART上追加同步方式的序列信号变换电路的产品，被称为USART(Universal Synchronous Asynchronous Receiver Transmitter)。



通信原理

计算机内部采用并行数据，不能直接把数据发到Modem，必须经过UART整理才能进行异步传输，其过程为：CPU先把准备写入串行设备的数据放到UART的寄存器（临时内存块）中，再通过FIFO（First Input First Output，先入先出队列）传送到串行设备，若是没有FIFO，信息将变得杂乱无章，不可能传送到Modem。

UART作为异步串口通信协议的一种，工作原理是将传输数据的每个字符一位接一位地传输。



其中各位的意义如下：

- 起始位：先发出一个逻辑”0”的信号，表示传输字符的开始。
- 资料位：紧接着起始位之后。资料位的个数可以是4、5、6、7、8等，构成一个字符。通常采用ASCII码。从最低位开始传送，靠时钟定位。
- 奇偶校验位：资料位加上这一位后，使得“1”的位数应为偶数(偶校验)或奇数(奇校验)，以此来校验资料传送的正确性。
- 停止位：它是一个字符数据的结束标志。可以是1位、1.5位、2位的高电平。 由于数据是在传输线上定时的，并且每一个设备有其自己的时钟，很可能在通信中两台设备间出现了小小的不同步。因此停止位不仅仅是表示传输的结束，并且提供计算机校正时钟同步的机会。适用于停止位的位数越多，不同时钟同步的容忍程度越大，但是数据传输率同时也越慢。
- 空闲位：处于逻辑“1”状态，表示当前线路上没有资料传送。
- 波特率：是衡量资料传送速率的指标。表示每秒钟传送的符号数（symbol）。一个符号代表的信息量（比特数）与符号的阶数有关。例如资料传送速率为120字符/秒，传输使用256阶符号，每个符号代表8bit，则波特率就是120baud，比特率是120*8=960BIT/S。

通过逻辑分析仪抓取 uart 总线数据，可以清楚的看到数据帧格式。