

HART 协议

2009-10-28 08:33:43| 分类: [观点](#) | 标签: | 字号大中小 订阅

现代工业生产中存在着多种不同的主机和现场设备,要想很好地使用他们,完善的通讯协议是必须的。**HART** 协议最初是由美国 **Rosemount** 公司开发,已应用了多年。**HART** 协议使用 **FSK** 技术,在 **4~20mA** 信号过程量上叠加一个频率信号,成功地把模拟信号和数字信号双向同时通讯,而不互相干扰。**HART** 协议参照了国际标准化组织的开放性互连模型,使用 **OSI** 标准的物理层、数据链路层、应用层。**HART** 协议规定了传输的物理形式、消息结构、数据格式和一系列操作命令,是一种主从协议。当通讯模式为“问答式”的时候,一个现场设备只做出被要求的应答。**HART** 协议允许系统中存在 2 个主机(比如说,一个用于系统控制,另一个用于 **HART** 通信的手操仪),如果不需要模拟信号,多点系统中的一对电缆线上最多可以连接 15 个从设备。 物理层

附件: 您所在的用户组无法下载或查看附件 物理层规定了信号的传输方法、传输介质。采用 **Bell202** 标准的 **FSK** 频移键控信号,在低频的 **4~20mA** 模拟信号上叠 加一个频率数字信号进行双向数字通信。数字信号的幅度为 **0.5 mA**,数据传输率为 **1200bps**, **1200Hz** 代表逻辑“1”,**2200Hz** 代表逻辑“0”。数字信号波形如上图所示。数据链路层 数据链路层规定 **HART** 协议帧的格式,可寻址范围 **0~15**,“0”时,处于 **4~20mA** 及数字信号点对点模式,现场仪表与两个数字通信主设备(也称作通信设备或主设备)之间采用特定的串行通信,主设备包括 **PC** 机或控制室系统和手持通信器。单站操作中,主变量(过程变量)可以以模拟形式输出,也可以以数字通信方式读出,以数字方式读出时,轮询地址始终为 **0**。也就是说,单站模式时数字信号和 **4~20mA** 模拟信号同时有效。“1~15”处于全数字通信状态,工作在点对多点模式,通信模式有“问答”式、“突发”式(点对点、自动连续地发送信息)。按问答方式工作时的数据更新速率为 **2~3 次 / s**,按突发方式工作时的数据更新速率为 **3~4 次 / s**。在本质安全要求下,只使用一个电源,至多能连接 15 台现场仪表,每个现场设备可有 256 个变量,每个信息最大可包含 4 个变量。这就是所谓的多点(多站)操作模式。这种工作方式尤其适用于远程监控,如管道系统和油罐储存场地。采用多点模式, **4~20mA** 的模拟输出信号不再有效(输出设在 **4mA** 使功耗最小,主要是为变送器供电,各个现场装置并联连接),系统以数字通信方式依次读取并连接到一对传输线上的多台现场仪表的测量值(或其它数据)。如果以这种方式构成控制系统,可以显著地降低现场布线的费用和减少主设备输入接口电路,这对于控制系统有重要价值。**HART** 协议根据冗余检错码信息,采用自动重复请求发送机制,消除由于线路噪声或其他干扰引起的数据误码,实现数据无差错传送。能利用总线供电,可满足本质安全防爆要求。**HART** 协议信息帧的格式如下图所示。 **HART** 协议的帧格式以 8 位为一个字节进行编码,对每个字节加上一个起始位、一个奇偶校验位和一个停止位以串行方式进行传输。通常采用 **UART**(通用异步接收/发送器)来完成字节的传输。由于数据的有无和长短不恒定,所以 **HART** 数据的长度不能超过 25 个字节。 消息结构

如下所示,一条消息包括源地址、目的地址和一个校验位。每一个应答消息中包括现场设备状态,用于确保持续通讯的顺畅进行。数据位可有可无,视具体情况而定。一般每秒种可以传输 2~3 条消息。 **PREAMBLE START ADDR COM BCNT STATUS DATA PARITY** 序文 定界符 地址 命令号 数据长度 响应码 数据字节 奇偶校验

HART5.0 以前版本的设备一般采用“短结构”,单一的现场设备如果只利用 **4~20 mA** 电流信号进行测量时,从设备的地址都是 **0**;否则,对于多设备而言,从设备的地址是从 **1~15**,这种短结构的地址采用“随选”的方法,随机分配 **1~15** 中的一个。**HART5.0** 版本推出了“长结构”,这种

格式的从设备地址具有独一无二性，如同每个网卡中物理地址一样，全世界范围内都没有重复，一般占 5 个地址字节中的 38 位。这 38 位地址信息包含了生产厂家的代码、设备型号码和设备识别码。这种格式减少了误传输和误接收的可能性。现在大多数主机设备既能支持长结构又兼容短结构，当从机的应答信号中没有“唯一”标识码时，HART5.0 及其以上的版本提供的 0 号命令，就可以用于短帧中的设备地址识别。也就是说，主机将根据应答信号中是否具有“唯一”标识码来决定结构格式为“长”还是“短”。一般消息帧的组成，其中：

(1) **PREAMBLE** 导言字节，一般是 5~20 个 FF 十六进制字节。他实际上是同步信号，各通讯设备可以据此略做调整，保证信息的同步。在开始通讯的时候，使用的是 20 个 FF 导言，从机应答 0 信号时将告之主机他“希望”接收几个字节的导言，另外主机也可以用 59 号命令告诉从机应答时应用几位导言。

(2) **START** 起始字节，他将告之使用的结构为“长”还是“短”、消息源、是否是“突发”模式消息。主机到从机为短结构时，起始位为 02，长帧时为 82。从机到主机的短结构值为 06，长结构值为 86。而为“突发”模式的短结构值为 01，长结构为 81。一般设备进行通讯接收到 2 个 FF 字节后，就将侦听起始位。

(3) **ADDR** 地址字节，他包含了主机地址和从机地址，如前所述，短结构中占 1 字节，长结构中占 5 字节。无论长结构还是短结构，因为 HART 协议中允许 2 个主机存在，所以我们用首字节的最高位来进行区分，值为 1 表示第一主机地址，第二主机用 0 表示。“突发”模式是特例，0，1 值将交替出现，也就是说，在该模式下，赋予 2 个主机的机会均等。次高位为 1 表示为“突发”模式，短结构用首字节的 0~4 位表示值为 0~15 的从机地址，第 5，6 位赋 0；而长结构用后 6 位表示从机的生产厂商的代码，第 2 个字节表示从机设备型号代码，后 3~5 个字节表示从机的设备序列号，构成“唯一”标志码。

MA 主机地址 BM 突发模式 0 0 SA 从 SA 机 SA 地 SA 址

短 帧 地 址 结 构 另外，长结构的低 38 位如果都是 0 的话表示的是广播地址，即消息发送给所有的设备。

(4) **COM** 命令字节，他的范围为 253 个，用 HEX 的 0~FD 表示。31，127，254，255 为预留值。

(5) **BCNT** 数据总长度，他的值表示的是 BCNT 下一个字节到最后（不包括校验字节）的字节数。接收设备用他可以鉴别出校验字节，也可以知道消息的结束。因为规定数据最多为 25 字节，所以他的值是从 0~27。

(6) **STATUS** 状态字节，他也叫做“响应码”，顾名思义，他只存在于从机响应主机消息的时候，用 2 字节表示。他将报告通讯中的错误、接收命令的状态（如：设备忙、无法识别命令等）和从机的操作状态。

如果我们在通讯过程中发现了错误，首字节的最高位（第 7 位）将置 1，其余的 7 位将汇报出错误的细节，而第 2 个字节全为 0。否则，当首字节的最高位为 0 时，表示通讯正常，其余的 7 位表示命令响应情况，第 2 个字节表示场设备状态的信息。

UART 发现的通讯错误一般有：奇偶校验、溢出和结构错误等。命令响应码可以有 128 个，表示错误和警告，他们可以单一的意义，也可以有多种意义，我们通过特殊命令进行定义、规定。现场设备状态信息用来表示故障和非正常操作模式。

(7) DATA 数据字节，首先我想说明的是并非所有的命令和响应都包含数据字节，他最多不超过 25 字节（随着通讯速度的提高，正在要求放宽这一标准）。数据的形式可以是无符号的整数（可以是 8, 16, 24, 32 b），浮点数（用 IEEE754 单精浮点格式）或 ASCII 字符串，还有预先制定的单位数据列表。具体的数据个数根据不同的命令而定。

(8) CHK 奇偶校验，方式是纵向奇偶校验，从起始字节开始到奇偶校验前一个字节为止。另外，每一个字节都有 1 位的校验位，这两者的结合可以检测出 3 位的突发错误。应用层 操作命令处于应用层，包括通用命令、普通命令和特殊命令。通用命令通用命令是所有现场装置都配备的包括 1) 读制造商码和设备类型 2) 读一次变量 PV 和单位 3) 读当前输出和百分量程 4) 读取多达 4 个预先定义的动态变量 5) 读或写 8 字符标签 16 字符描述符日期 6) 读或写 32 字符信息 7) 读变送器量程单位阻尼时间常数 8) 读传感器编号和极限 9) 读或写最终安装数 10) 写登录地址 常用命令常用命令提供的功能是大部分但不是全部现场装置都配备的包括 1) 读 4 个动态变量之一 2) 写阻尼时间常数 3) 写变送器量程 4) 校准置零置间隔 5) 设置固定的输出电流 6) 执行自检 7) 执行主站复位 8) 调整 PV 零点 9) 写 PV 单位 10) 调整 DAC 零点于增益 11) 写变换函数平方根/线性 12) 写传感器编号 13) 读或写动态变量用途专用命令专用命令提供分别对特殊的现场装置适用的功能包括 1) 读或写低流量截止值 2) 起动停止或取消累积器 3) 读或写密度校准系数 4) 选择一次变量 5) 读或写结构材料信息 6) 调整传感器校准值 通用命令的范围从 0~30: 0, 11: 设备识别（厂商、设备类型、版本） 1, 2, 3: 读测量值 6: 置随选地址 12, 13, 17, 18: 读、写用户输入文本信息 14, 15: 读设备信息（传感器序列号，传感限，报警操作，范围，传输结构） 16, 19: 读、写最终装配号 普通命令是从 32 到 126，提供了大多数设备的功能命令。

普通命令中的 123 和 126 号命令并非“公共”的，他们专用于生产厂家在生产设备时输入设备的特殊信息，一般用户是不会改动的，像设备识别号之类。也可以用于直接读、写存储器。 33, 61, 110: 读测量值 34~37, 44, 47: 设置操作变量（范围、时限、PV 值、传输功能） 38: 复位“结构变化”标志 39: EPROM 控制 40~42: 对话功能（固定电流模式、自测、复位） 43, 45, 46: 模拟输入、输出整流 48: 读附设备的状态 49: 写传感器序列号 50~56: 用传输变量 57, 58: 单元信息（标志、描述、数据） 59: 写所需导言号 60, 62~70: 使用复合模拟输出 107~109: 突发模式控制 特殊命令的范围是从 128~253，他提供给现场设备专用的功能。早先的设备特殊命令常常将设备型号码作为数据中的第 1 个字节，以保证命令传输给正确的设备。在 HART5. 0 版本之后，由于惟一标识码的使用，就省略掉了这步骤。用户若要使用不同设备的特殊命令时可以参照厂家提供的设备文档。常用重要命令介绍

0, 11: 用于识别现场设备。我们知道无论采用长结构还是短结构都可以标识现场设备，应答 0 号命令的信息中就包含了对不同设备的标识；然后，主机建立不同的标志，为随后的长结构命令做准备。在 HART4. 0 版本及以前，传输类型码分为 2 字节：一个是生产厂商代码，另一个是设备类型代码。而两个字节还可以省略。到了 HART5. 0 版本就必须使用扩充的代码表示设备信息，还用 ID 号代替了最终流水线号。

一个主机通常以 0 号命令开始通讯，赋予随选地址 0，然后扫描 1~15 地址，看谁期待操作，显然由于 HART5. 0 版本后的设备，主机可以使用 11 号命令，再带一个全 0 的广播地址，外加命令中的标志作为数据，等待着具有相同标志的从机响应，而应答的 11 号命令等同于 0 号命令。

2, 3: 用于读取不同形式中的测量变量。命令 2 和 3 中有以 mA 为单位的电流值，电流值只有在设定输出范围内才可以作为主参量 PV，而在其他时候，像复用模式、输出量可变、饱和或设备错误都不能如此使用。尽管 PV 和其他动态变量不受设定输出范围的限制，但是却必须受限于传感设备。

6: 用于随选地址的设定。设定为 0，该设备就在点到点的模式工作，产生模拟输出信号；设 61 定为 1~15，设备就工作在多点模式中，输出电流值固定为 4 mA。

12, 19: 用于读、写一系列设备信息。HART4. 0 版本及以前使用 4 号和 5 号命令实现此功能。数据格式

如果传送的命令不成功，那么响应中就不包含数据。然而响应值是从现场设备内存中取出的，是一个近似值。数据所占的字节和格式视不同的命令而定，具体的规则可以查询相关的资料。看实例了解 HART 消息结构例 1：主机到从机

FF FF FF FF FF 82 A6 06 BC 61 4E 01 00 B0

上面是主机到从机发送的一条消息。前 5 个字节值都为 FF，显然他是导言字节。接着的 82 起始字节，表示主机到从机发出的长结构的消息。后 5 个字节“A6, 06, BC, 61, 4E”是地址字节化为二进制表示如下：

A6 06 BC 61 4E 1010 0110 0000 0110 1011 1100 0110 0001 0100 1110

可见首字节 A6 的最高位为 1 表示主机，次高位为 0 表示非突发模式，后面的 38 b 表示设备的惟一标号：“100110”是生产厂家代码，值为 38，是 Rosemount 公司的代码；后一字节 06 是设备型号代码，06 代表的型号是 3051C；后面的 3 个字节是设备识别号，本例中的值为 12345678；再接下来的 01 是命令字节，表示 1 号命令，即读取 PV 值后面的 00 是表示数据的长度；本例中无数据，值为 0；最后是校验字节 B0； 例 2：从机到主机

FF FF FF FF FF 86 A6 06 BC 61 4E 01 07 00 00 06 40 B0 00 00 45

上面表示的是从机到主机的一条消息。本例大部分与例 1 相似，不同的是数据字节不再为 0，其中的 06 表示单位 PSI；后面的 4 个字节是用浮点数表示的值，为 5. 5。并且由于本例是由从机到主机的应答消息，所以存在着状态位，即本例中的“00 00”，表示“OK”。 例 3：突发模式

FF FF 53 03 00 41 3F 41 3F 42 47 BF 06 41
FF FF 81 04 E6 03 1A 60 A0 00 27 A0 00 39 60 00 06 60 00 39 95 00 D4
FF D7 00

上面是突发模式发出的一条消息。第 1 个字节 81 表示突发的长结构模式，与前例中相似的地方我们不再介绍。注意到状态字节“00 60”后的字节“41 3FA000”，他表示的是当前的电流值，计算后是 11. 976 6；后面的 27 表示单位 mA，像后面的 39 表示“%”一样。数据字节中的“42 47 60 00”，“BF06 60 00”，“41 95 0000”分别表示“SV”，“TV”，“FV”表示方法与 PV 相同。

经过解释后的消息可以表示为：“LBTXS / RdAllPv / 026 / 0060 / 11. 9766 / mA / 11. 9766 / % / 49. 8438 / psi / -0. 524902 / % / 18. 625 / D4”。HART 协议适配器的应用 请将检测好的 HART 协议适配器按照说明连接好，并确定适配器处于工作状态。按照说明启动串口调试程序或者由上位机发送相关的命令进行数据的转换，客户端可以将采集的数据进行分析，计算得到有用的数值。在这里我们以 K-TEK 公司型号为 AT100 的 HART 协议的液位计为例进行详细说明。命令及命令的格式 标准的 HART 协议命令格式如下表所示 读设备序号命令格式说明如下：

起	序	定	地	命	数	校	结
始位	文	界符	址	令	据长度	验位	束符

由于要确保待发的命令完整的发送，我们特意在标准命令格式序文前加了一个起始位“23”和在

校验位后加了一个结束符“40”。例如：发送读取设备序号命令 23 FF FF FF FF FF 02 80 00 00 82 40
命令注解如下表所示：

起始位	23
序文	FF FF FF FF FF
定界符	02
地址	80
命令	00
数据长度	00
校验位	82
结束符	40

返回的命令格式如下表所示：

序文	定界符	地址	命令	数据长度	数据	校验位
----	-----	----	----	------	----	-----

返回的数据为： FF FF FF FF FF 06 80 00 0E 00 40 FE 50 7F 06 05 01 01 08 00 6B 73 3A 30
返回数据命令注解如下表所示：

序文	ff ff ff ff ff
定界符	06
地址	80
命令	00
数据长度	0E
数据	00 40 FE 50 7F 06 05 01 01 08 00 6B 73 3A
校验位	30

返回数据 6B 73 3A 就是这台设备的序号。起始位和结束符只在发送命令时做确定命令的完整发送，它不改变命令本身，更不会影响数据的转换。 发送读取液位计动态变量命令 命令格式说明如下表所示：

(AT100) 82 90 7F 固定	6B 73 3A 设备序号	03 为命令
---------------------	---------------	--------

返回的数据为：FF FF FF FF FF 86 90 7F 6B 73 3A 03 15 00 40 40 D4 E0 00 2D 3E 09 1C 2D 2D 3E 92 E3 9E 20 41 D4 B2 B8 01 返回数据命令注解如下表所示：

电流	40 D4 E0 00
液位	3E 09 1C 2D
界面	3E 92 E3 9E
温度	41 D4 B2 B8

返回数据计算 经过反复实验和推理论证而推导出了基于 HART 协议数据的计算公式。下面以电流和液位为例加以说明。电流值的计算： $dlH=((\text{parseddataHart}[13] + \text{parseddataHart}[12] * 256.0 + (\text{parseddataHart}[11] \& 127) * 65536.0))/8388608.0 + 1$; $dlD=(((\text{parseddataHart}[10]*1) \& 127) * 256 + ((\text{parseddataHart}[11]*1) \& 128)) / 128 - 127$; 液位值的计算： $ywH=((\text{parseddataHart}[18] + \text{parseddataHart}[17] * 256.0 + (\text{parseddataHart}[16] \& 127) * 65536.0))/8388608.0 + 1$; $ywD=(((\text{parseddataHart}[15]*1) \& 127) * 256 + ((\text{parseddataHart}[16]*1) \& 128)) / 128 - 127$; 启动串口调试程序或者由上位机发送相关的命令进行数据转换，客户端可以将采集的数据进行分析，计算得到有用的数值。将计算所得的数据送到相应的存储区，客户可以根据自己的需要来处理这些数据。也可以根据自己的需要来提取有用的数据量，具体的读取命令，请参阅相关的技术书籍或向 HART 仪表厂商和经销商获取仪表专用协议。操作系统及上位机组态软件只要支持 RS-232 便可以轻松实现与 HART 仪表的通讯。此 HART 协议适配器的转换是全透明的，它只处理 HART 信号与串口信号的互相转换问题，工作在应用层,只针对符合 HART 协议的产品，与具体的供货商无关，读取命令和数据没有任何关系及影响。