

HART 协议解析

丁 颖，盛惠兴

(河海大学 计算机及信息工程学院 江苏 常州 213022)

摘 要：简要介绍了 HART 协议及其在工业生产领域的重要性，对 HART 协议的构成进行了剖析，对 HART 消息的具体构成单元、意义、使用环境、规则等进行了详细的说明。

关键词：HART；消息结构；长结构；短结构

中图分类号：TN915.04

文献标识码：B

文章编号：1004-373X (2004) 01-014-04

Analysing HART Protocol

DING Ying, SHENG Huixing

(Computer & Communication Institute, Hehai University, Changzhou, 213022, China)

Abstract: In this article, we introduce HART protocol and its significant place in industry. And analyse the structure of HART protocol, that is, giving a clear explanation of HART message for its units, meaning, using condition and rules.

Keywords: HART; message structure; long frame; short frame

随着信息技术的快速发展，工业过程自动化和制造自动化中设备和仪表之间的互连正逐步脱离传统的分散控制系统 (DCS)，而采用现场总线控制系统 (FCS)。现场总线是连接智能现场设备和自动化系统的数字式、双向传输、多分支结构的通信网络。现在，在现场总线标准尚未完全取代 4~20 mA 信号方式的过渡期，我们需要一种既支持新型智能仪表的数字信号又兼容传统的模拟信号的过渡期协议，1986 年 Rosemount 公司提出的 HART 协议就是最具代表性和普遍性的一种。

可寻址传感器数据通路 (HART, Highway Addressable Remote Transducer) 是在 4~20 mA 的模拟信号上叠加 FSK (Frequency Shift Keying, 频移键控) 数字信号，可以兼容模拟和数字 2 种信号。1993 年成立了 HART 通信基金会 HCF (HART Communication Foundation)，随着越来越多公司的加盟，基于 HART 协议产品的增多，他的重要性得到了普遍的认同。

1 HART 协议的分层

HART 现场总线使用国际标准化组织 ISO 规定的开放式系统互联 OSI 七层模型中的第 1 层，第 2 层和第 7 层，即物理层、数据链路层和应用层。

(1) 物理层 规定了信号的传输方法、传输介质，HART 支持模拟信号和数字信号在同一线路上传输，其通讯速率为：在 4~20 mA DC 模拟信号上叠加 FSK 数字信号时为 1 200 b/s；用屏蔽双绞线单台距离可达 3 000 m；而多台互连距离可达 1 500 m。采用双绞同轴电缆作为传输介质时，最大传输距离可达到 1 500 m，如图 1 所示。

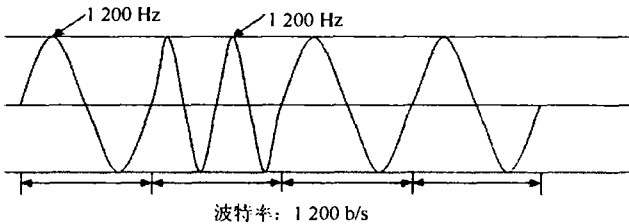


图 1 HART 调制频率信号

(2) 数据链路层 规定了 HART 帧的格式，实现建立、维护、终结链路通讯功能，HART 协议根据冗余检错码信息，采用自动重复请求发送机制，消除由于线路噪音或其他干扰引起的数据通讯错误，实现通讯数据无差错传送。数据链路层中的数据结构长度不固定，最长 25 B，寻址范围 0~15，当地址为 0 时，则处于 4~20 mA 的 DC 与数字通信兼容状态；当地址为 1~15 时，则处于全数字通信状态，通信模式为“问答式”或“突发式”。

(3) 应用层 规定了 3 类命令：第 1 类是通用命令，适用于遵守 HART 协议的所有产品；第 2 类是普通命

收稿日期：2003-09-01

令, 适用于遵守 HART 协议的大部分产品; 第 3 类是特殊命令, 适用于遵守 HART 协议的特殊产品。HART 协议是一个开放的协议, 对于厂家生产的具有特殊功能的产品, HART 提供了设备描述语言 DDL (Device Description Language) 以确保互操作性。

2 HART 协议

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。下面我们将对每一部分逐一进行介绍:

2.1 物理形式

物理形式, 我们已经在上面对 HART 分层中的物理层进行了介绍, HART 就是利用 BELL202 标准的 FSK 信号以 1 200 b/s 加载在 4~20 mA 的模拟信号上。它具有 0 平均值, 不会干扰模拟信号。

2.2 消息结构

如图 2 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场设备状态, 他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]	CHK
----------	-------	------	-----	------	----------	--------	-----

图 2 HART 消息结构

HART 5.0 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。HART 5.0 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“惟一”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

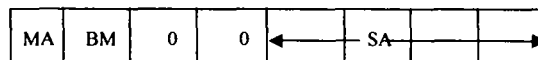
“惟一”标识码来决定结构格式为“长”还是“短”。

我们从图 2 中可以简单地看出一般消息帧的组成, 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“惟一”标志码。如图 3 和图 4 所示。



MA 为主机地址, BM 为突发模式, SA 为从机地址

图 3 短帧地址结构

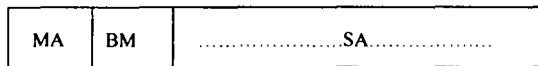


图 4 长帧地址结构

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，他们可以是单一的意义，也可以有多种意义，我们通过特殊命令进行定义、规定。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。

通常情况下，在“应答模式”下1s可以2次通讯，在“突发模式”下，每秒钟可以传送3条消息。

2.3 操作命令

2.3.1 操作命令分类介绍

操作命令处于应用层，包括通用命令、普通命令和特殊命令。通用命令的范围从0~30，如表1所示。

表1 通用命令

命令	功能
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。他提供了大多数设备的功能命令，如表2所示。

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的设备的特殊信息，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。

表2 普通命令

命令	功能
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HART 5.0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。

2.3.2 常用重要命令介绍

(1) 0号和11号命令 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HART 4.0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HART 5.0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HART 5.0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) 2和3号命令 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，但是却必须受限与传感设备。

(3) 6号命令 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

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。

(4) 12号和19号命令 用于读、写一系列设备信息。HART 4.0版本及以前使用4号和5号命令实现此功能。

2.4 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。成功的“写”或“命令”命令的响应消息与命令消息中的变量成分、格式相同;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。

3 看实例了解HART消息结构

3.1 例1:主机到从机

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

3.2 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,

3.3 例3:突发模式

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

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 3F A0 00”,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”,“BF 06 60 00”,“41 95 00 00”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”。

4 结 语

本文主要介绍了HART协议的结构,即消息结构,又分成长结构和短结构,对其中的每个字节的意义和个数都详细地加以了说明,最后对每一种情况都

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。

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”。

给出了典型的实例并进行了具体的解析,这是在研究过程中对HART信号的分析,希望大家能够对HART信号有更深入的了解。

参 考 文 献

- [1] 郭福田,姜军,刘贤梅,等.基于HART协议的通信技术[J].大庆石油学院学报,2000,24(1).
- [2] Rosemount Inc. HART smart communication protocol, the rosemount Smart Family. Product data sheet [S]. PDS2695.
- [3] Hart User Group. Hart field communication protocol [S]. Product Data Sheet, PDS200.
- [4] 吴安定,林铭锻.基于HART协议的过程控制系统接口卡[J].自动化仪表,2001,22(5).
- [5] 王锦标.现场总线控制系统[J].微计算机信息,1996,12(6).