

一种实用的通信协议分析方法

路红, 谢吉华

(东南大学电气工程系, 210096, 南京)

[摘要] 以空调控制器的通信部分为实例, 提出获得通信协议^[1]的具体方法和步骤, 并对通信码型的获得、差分曼彻斯特码的识别、应用进行了探讨。

[关键词] 差分曼彻斯特码, 通信协议, 信息码

[中图分类号] TM 762; [文献标识码] B; [文章编号] 1672-1292(2002)01-0025-04

0 引言

通信协议是实现空调控制器自动控制的关键技术之一。在空调控制器上位机与下位机的通信系统中, 下位机接收上位机发送的温度设定值、功能设定及风速设定等信息驱动相应的继电器工作实现环境温度的自动控制, 同时上位机接收下位机发送的系统故障信息并在上位机显示故障类型, 以提醒用户及时排除故障, 维持空调控制器的正常运行。

实际工作中, 通常由于技术保密缘故或厂家提供的资料不足等诸多原因, 并未给出详细的通信协议, 而在通信部分的设计中, 要求用通信系统原来的通信协议, 这势必增加了设计的难度。分析原设备获得正确的通信协议势在必行。

一般情况下, 通信内容依照一定的编码方式由一系列连续码型实现。因此, 获得通信码型序列, 并根据通信码型序列分析出通信起始标志、通信编码方式、编码规则及信息码传递的内容是获得通信协议的关键。

本文以空调控制器上、下位机之间的通信为例, 引入一种实用的获得通信协议的方法。

1 通信码型序列的获得及通信起始位置的确定

1.1 软件方式获得通信码型序列

通信码型序列的获得可以有多种方式, 总体可分为两大类: 软件方式, 硬件方式。

硬件方式指用逻辑分析仪、示波器等硬件设备捕捉通信码型序列。实践中, 由于逻辑分析仪并不普及, 示波器也价格不菲, 在精度要求不很高的情况下, 软件方式就显得尤为经济实用。

软件方式是通过编制相应的程序获得通信码型序列中高低电平对应的长度数据, 再把这些连续的高低电平转化成连续直观的码型。该例中利用 PIC16C73 单片机^[2]的定时器 TMR1 和 INT 引脚中断(边沿触发中断)测量高低电平的长度, 根据 DATA_BUF 中接收的数据比较高低电平之间, 高电平与高电平之间, 低电平与低电平之间的长度比例关系, 按接收到的高低电平顺序转化成如图 3.1~图 3.4 的通信电平序列。软件流程如图 1 所示。

1.2 确定通信编码的起始位置

任何通信协议都有自己的通信起始标志^[3]。找到了这个标志就可确定一帧完整的信息码。由 DATA

收稿日期: 2002-03-18

作者简介: 路红, 女, 1973-, 东南大学电气工程系硕士研究生, 从事电力电子与电力传动方面的研究。

_BUF 中接收的数据可以比较得出,总是周期性的出现一个超出单位低电平(码型图中最短的低电平)几倍的低电平和一个相邻的超出单位高电平(码型图中最短的高电平)几倍的高电平,且这个起着起始标志作用的低电平及高电平的长度总是一定的.如图 3.1~图 3.4 中最左边较长的低电平和相邻的高电平,这个低电平和高电平就是起始标志,每发送或接收这样的一个高电平和低电平标志着新一轮的发送或接收通信开始了.

2 编码方式及编码规则的确定

2.1 确定编码方式

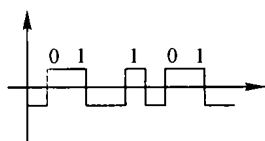
空调控制器通信部分应用的是基带局域网信号技术.其中常用的编码方式有四种:

(1) 差分曼彻斯特编码(Differential Manchester).

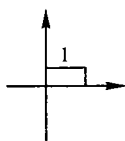
1 和 0 分别用电平跳变或不跳变来表示.若用电平跳变来表示 1,则称为传号差分码;若用电平跳变来表示 0,则称为空号差分码.即:若在前一码元末尾(本码元开始)处无电平跳变来表示 1,则有电平跳变来表示 0.反之亦然.应用:IEEE802.5.如图 2.1:对应有电平跳变为 0 无电平跳变为 1 时的编码结果.

(2) 极性非归零码(P-NRZ: Polar Non-return to Zero).若高电平表示 1,则低电平表示 0,反之亦然.如图 2.2:对应高电平为 1 低电平为 0 时的编码结果.其特点是实现简单,但当信息中包含长串的连接 1 或 0 时,将失去时钟信息,不具有检测错误的能力,且有直流.

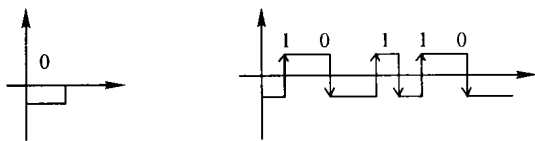
(3) 曼彻斯特码(Manchester)又叫数字双相码(Digital Biphas)或分相码(Biphase, Split-phase),用一个周期的方波表示 1,用它的反相波形表示 0,反之亦然.应用:IEEE802.3.如图 2.3 示.



2.1 差分曼彻斯特码



2.2 极性非归零码



2.3 曼彻斯特码

图 2 几种常见的编码方式

(4) 4B/5B 码:适用于光纤 LAN.由于空调控制器通信部分没有用到光纤介质,先排除 4B/5B 码.在编码方式分别为极性非归零码、曼彻斯特码、差分曼彻斯特码的情况下各自列出对同一串通信电平序列(如图 3.1)编码后的信息码,共得到 6 组(3 种编码方式各对应两种编码规则).据编码结果,很明显:若为极性非归零码,则得到的两组信息码的位数达 80 位以上,不符合实际需要.若为曼彻斯特码,则得到的两组编码序列分别为全 0 和全 1,无实际意义.因此以上两种编码方式都可排除.在差分曼彻斯特码下得到两组信息码都为 32 位,可看作 4 个 8 位二进制数.由此可确定该通信编码使用的是差分曼彻斯特编码.

2.2 确定编码规则

改变空调控制器的工作条件,获得不同条件下的通信码型序列,以其中一串完整的码型为研究对象进行分析.如图 3.1:对应 29, 低风,制热条件下的码型.

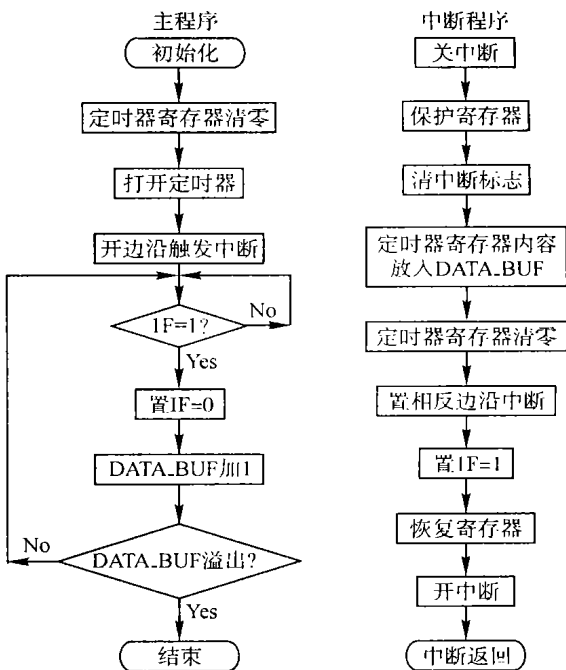


图 1 程序流程框图

首先,设:有跳变为 0,无跳变为 1,编码得到如下一帧 32 位信息码:

0001 1010 0001 1101 0000 0000 0011 0111

其次,设:有跳变为 1,无跳变为 0,同样编码得到一帧 32 位信息码:

1110 0101 1110 0010 1111 1111 1100 1000

前者的 32 位码中出现了连续的 0,而后的 32 位码中相应位置出现的是连续的 1,这直接影响着校验方式.前者由于后 8 位二进制数恰好是其前的 3 个 8 位二进制数的和(即:00011010 + 00011101 + 00000000 = 00110111)可初步确定校验方式使用的是校验和^[4].后者的 32 位码可以验证不符合任何校验规律.根据编码规则有跳变为 0,无跳变为 1,检验图 3.2、图 3.3 和图 3.4 均可证明符合校验和的规律.由此可确定编码规则为:有跳变为 0,无跳变为 1.同时可确定 b24~ b31 为校验和位.

3 设备功能与信息码一一对应

空调控制器的目的是实现环境温度的自动控制,则信息码中必定有表示温度的部分.温度本身是数字,可直接转化成二进制数,比较容易与编码得到的信息码相比较找到规律.因此,测出其他条件相同,温度条件不同的情况下的通信码型图,比较它们的不同之处,就可找到温度在这帧信息码中的具体位置.以下是在不同条件下接收到的相应的码型图,按第 2 部分确定的编码规则编码得到的信息码标在相应码型图的正上方(如图 3.1~ 图 3.4 示).

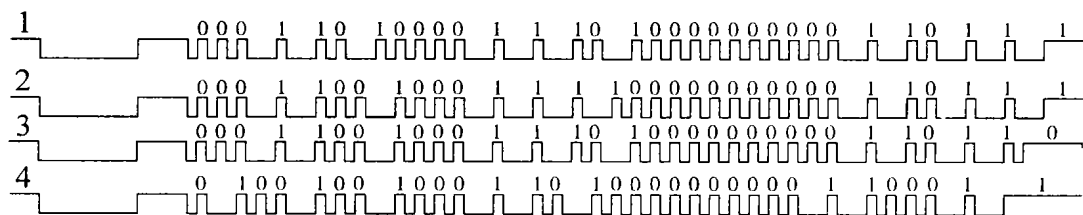


图 3 不同条件下接收到的码型图

如图 3.1: 29, 低风, 制热条件下的码型图; 如图 3.2: 30, 低风, 制冷条件下的码型图;

如图 3.3: 29, 低风, 制冷条件下的码型图; 如图 3.4: 26, 高风, 制热条件下的码型图.

图 3.2 和图 3.3 对应的唯一不同的条件是温度,经编码后各自对应的一帧 32 位信息码如下: 图 3.2: 0001 1001 0001 1110 0000 0000 0011 0111; 图 3.3: 0001 1001 0001 1101 0000 0000 0011 0110. 可以看出,二者有两处不同,即:图 3.2 中的 1110 和 0111 分别与图 3.3 中的 1101 和 0110 中必有一处代表温度显示值.

据图 3.2: 若 1110 代表温度,其对应的十进制数为 14,与 30 相差甚远,考虑其与前 4 位或后 4 位组成 8 位是否有可能,则有:0001 1110 和 1110 0000,两者对应的十进制分别为 30 和 224,显然,出现了要找的数值 30,由此初步确定 0001 1110 处的位置为温度值.再看图 3.3: 相应的 1101 跟前后的 4 位数组成的 8 位码为: 0001 1101 和 1101 0000,分别对应的十进制数为: 29 和 208.显然具有同样的规律,再次证明了该 8 位码处为温度值.

为进一步验证以上结论,再测得两组同温度条件下的码型图,对比温度值所处的位置处的信息码是否相同,相同则表示第一步确定的温度值位置是正确的.对比图 3.1 和图 3.3,可以得出结论: b8~ b15 为温度位置.同理,可再测几组不同条件下的码型序列进行验证.

考察另一处不同之处: 0111. 由于前面已确定了温度值的位置仅与前面的不同之处有关,因此可以排除此处为温度位置的可能性.同时,进一步证实了该处为校验和的结论.反之,则对此处的 0111 用前面的分析过程及方法来进行分析,得出结论.

以同样的方法来确定功能位、风速位等处在信息码中的具体位置及其占用的字节数.比较图 3.1 和

图 3.3 知: 获得的这两帧信息码的唯一不同的条件是功能, 分别对应制热、制冷。根据这个线索, 只需比较两帧信息码的不同之处就可进行区分了。编码情况分别如下:

图 3.1: 0001 1010 0001 1101 0000 0000 0011 0111; 图 3.3: 0001 1001 0001 1101 0000 0000 0011 0110.

显然有两处不同: 一处为 1010 和 1001; 另一处为 0111 和 0110. 再列出图 3.2 的编码情况进行比较. 图 3.2: 0001 1001 0001 1110 0000 0000 0011 0111

据图 3.3 和图 3.2 测试的前提功能条件同为制冷, 则在码型中必然有同样代表制冷的位置. 图 3.2 和图 3.3 相同之处为: 0001, 1001, 0001, 0000, 0000, 0011.

由分析知: 这个代表功能位的位置一定存在于图 3.1 与图 3.2 的不同之处, 且这个位置又是图 3.2 和图 3.3 的相同之处. 根据这个规律, 可得到只有 1001 处符合要求. 因此可以确定 b4~ b7 为制冷、制热功能位. 同理, 用这种方法可以一一确定其它功能信息, 如: 上电标志位、出错标志位、出错显示值位、风速位等等. 其中校验方式、校验位置在确定校验规则部分得以解决并在本部分得到了验证等.

获得已知设备通信协议的主要目的是为了尽可能利用原设备资源, 减少生产成本. 本文是在实践中总结得到一种获得通信码型并对通信码型进行编码、分析得到通信协议的有效方法, 虽然限于篇幅, 有的地方只提供了一些策略性的原则, 但的确包括了主要分析过程和重要步骤. 实际应用中, 可根据实际情况考虑和借鉴其中的内容.

[参考文献]

- [1] 阳宪惠. 现场总线技术及应用[M]. 北京: 清华大学出版社, 1999
- [2] 窦振中. PIC 系列单片机原理和程序设计[M]. 北京: 北京航空航天大学出版社, 1998
- [3] 戴梅萼. 微型计算机技术及应用[M]. 北京: 清华大学出版社, 1995
- [4] 李华. MCS-51 系列单片机实用接口技术[M]. 北京: 北京航空航天大学出版社, 1997

A Practicable Method of Analyzing Communications Protocol

Lu Hong, Xie Jihua

(Department of Electrical Engineering, Southeast University, 210096, Nanjing, PRC)

Abstract: This paper presents the analyzing method and the procedure for acquiring communications protocol, with a case studied in communications of the air controller. It also discusses the capture of communications code type as well as the identification and use of Differential Manchester.

Key words: Differential Manchester, communications protocol, information code

[责任编辑: 刘健]