HART协议与软件开发

遵照一套标准的协议来开发一套系统，其最大的好处是不论硬件设备提供商还是软件开发人员，都可以独立地按照标准的规范进行设计，分别提供标准的接口，从而大大提高工作效率，在最后的软件和硬件的联合调试中会带来最大的方便。由于HART协议是本数据平台软件和整个控制系统软件设计的理论依据，只有充分理解和消化了HART协议各层规范后，才可以根据具体规范对协议的各层进行软件实现，从而达到上位机软件与基于HART协议的现场仪表之间进行通信，以完成数据交换的目的。目前，国内对HART协议进行系统的翻译，总结和消化的文献还不多见，因此在本章，郑州波特电子有限公司将根据在研究工作中对HART协议的消化和理解，简要地对在软件设计中涉及到的HART协议规范进行总结。

1. HART协议概述:

HART（Highway Addressable Remote Transducer）协议，是一项4-20mA信号与数字通信技术兼容的过渡性标准，现已有Rosemount ,Smar ,ABB ,Fuji , Moore, E+H, Honeywell, Fisher Controls, Arcom Control Systems Ltd. 等70多家公司参加了HART 协议基金HCF。由于HART 协议众多不容置疑的优点，使它成为全球应用最为广泛的现场通信协议，1994年，HART变送器占世界智能变送器市场的76%，已成为事实上的工业标准。据业内人士估计，HART 协议在国际上的使用寿命为15-20年，国内由于客观条件所限，这个时间还会更长些，因此，在今后很长一段时间内，HART 产品仍有十分广泛的市场。

HART 协议保留了4-20mA过程控制信号的工业标准，允许在同一个环路上同时存在模拟信号和数字通信信号而不相互影响。这一点是通过采用Bell202的通信标准实现的，Bell202采用频移键控FSK（Frequency Shift Keying ）技术。HART 协议的通信是在4-20mA的电流上施加一频率信号而实现的。有两个信号频率，一个是1200HZ，代表逻辑“1”，另一个是2200HZ，代表逻辑“0”，信号的幅值是0.5mA。

在整个通讯过程中，既有模拟信号（4-20mA），也有数字信号（1200HZ和2200HZ），由于在一个信号周期中，通信信号的平均值为0，从而不对4-20mA的模拟信号产生影响，这是HART协议最重要的特点之一。

HART协议参考了国际标准化组织（ISO）提出的OSI（Open Systems Interconnection）模型。该模型提供了通信系统所必须的结构和要素。而HART只使用了一个简化的OSI模型，仅用了其中的一，二，七层，如下图所示。

层号	层名	OSI层次	HART层次
7	应用层	格式化数据	HART命令
6	表示层	转换数据	无

Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.

5	会话层	控制会话	无
4	传输层	确保信息完整	无
3	网络层	路由传送	无
2	数据链路层	差错处理	协议规则
1	物理层	连接设备	BELL 202

HART协议与OSI参考模型的关系

HART协议包括物理层，数据链路层和应用层，及DLL语言这四部分。

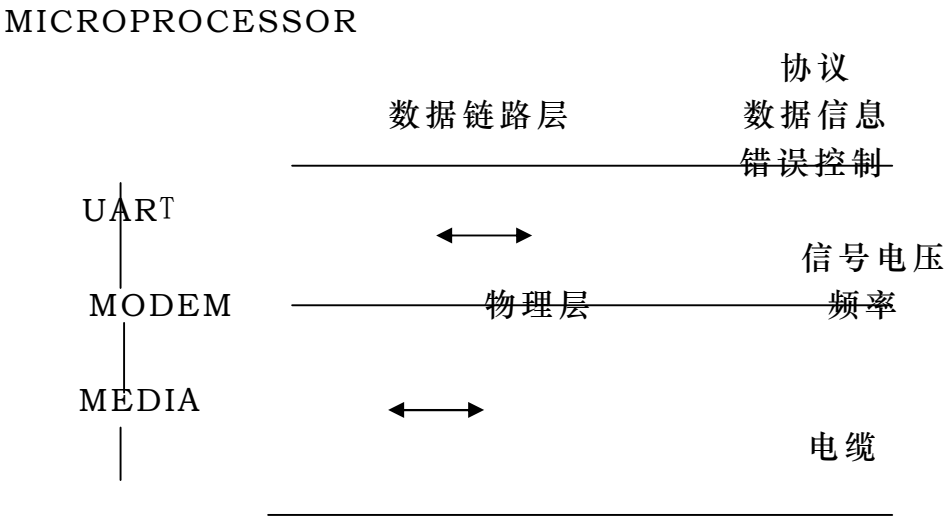
2. HART协议物理层规范

物理层规定了信号的传输方法，信号电平，设备阻抗和介质。通常物理层使用双绞线作为介质，在双绞线上单独传输数字信号或者同时传输数字与模拟信号。有效通信距离为5000英尺（1500米）。HART数字信号的传输是模拟信号传输的简单扩展，在电流模式中，是在现有的低频率模拟电流（典型的是4-20 mA）上叠加一个高频率电流。在电压模式中，是在现有的直流电压信号（典型的是1-5VDC）上叠加HART电压信号。这两种信号传输方式共享同样的硬件，而在频率上是分离的。

HART使用1200bit/s的二进制相位连续频移键控（FSK）。

信息格式：1个起始位（0），8个数据位，1个校验位（奇校验）和一个停止位。

数据链路层和物理层的关系



3. HART协议数据链路层规范

3.1设备类型

通讯协议能确认三种不同类型的设备，最普遍与最基本的类型是从设备，接收与提供带有测量值或其他数据的数字信号，除了有特别要求之外，

Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.

即该设备在主从关系中总是作为从动装置起作用。从设备如现场仪表，压力变送器，温度变送器，执行器等。

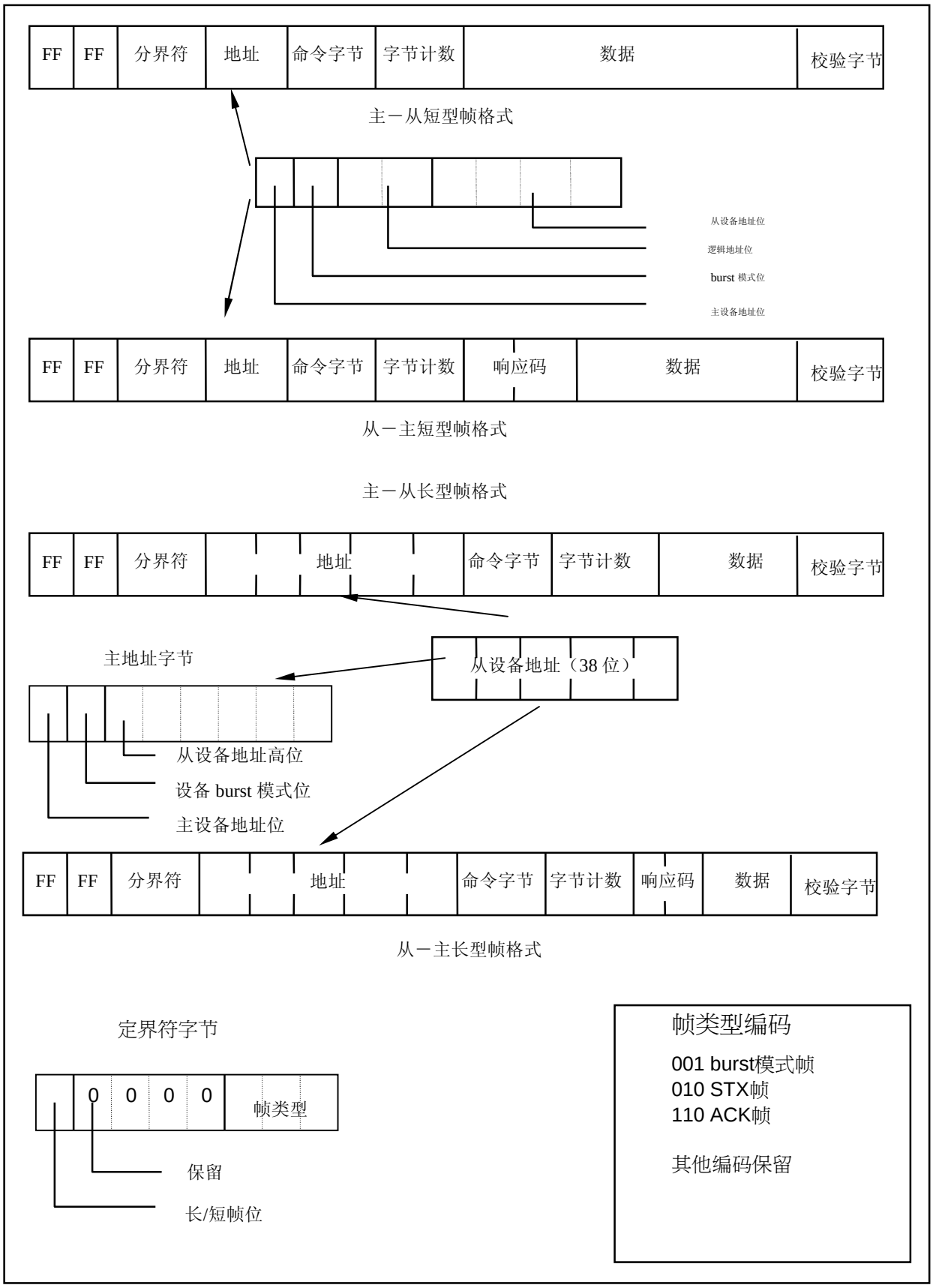
第二种类型的设备是burst模式设备，这种设备在固定的时间间隔发出带有测量值或其他数据的数字信号响应，而不包含被特别请求的数据，即该设备通常是作为一个独立广播的设备。

第三种类型的设备是主设备，主设备负责初始化、控制和终止与从设备或burst模式设备的交互。将主设备分为一级主设备和二级主设备是为了在HART通讯链路上同时使用这两种主设备，一级主设备和二级主设备除了使它们区分开的时限需要定制以外使用相同的协议规则。一级主设备通常指上位PC机，二级主设备指HART设备的手操器。

3.2 帧格式

下图给出了HART协议的所有类型的帧格式。根据每一帧发送者的不同可分为：主-从型帧，从-主型帧。根据帧的长度可分为：长型帧，短型帧。
注：每格表示1个字节，每字节中最高和最低位的顺序为从左向右。

Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.



HART协议的帧格式

Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.

①．先导字符（preambles）

所有从主设备、从设备或burst模式设备发送的帧都有特定个数的十六进制“FF”字符放在前面，这些字符被称为一个帧的先导字符。某些物理层协议需要它们去作用调制解调器的电路。定界符前的先导字符可能有多个，但协议规定只有两个连续的先导符后的定界符才标志着一个帧的开始。

②．定界符 （delimiter）

此字段的低3位表示了不同的帧类型；最高位标志着该帧是长帧还是短帧；其余位保留。

③．编址

每一个HART帧都需要地址字段来标明其源和目的地址。

（1）长帧格式地址：实际上是每一台从设备的唯一标识符，除了最高两位外的低38位即标识了此唯一标识符。最高位指明与此帧相关的主设备。一级主设备为“1”，二级主设备为“0”。从设备必须将该域不变的返回。次高位指明从设备是否处于BURST模式，是则此位为“1”，否则为“0”。

（2）短帧格式地址：只有0号短帧命令支持短帧地址。该地址指明了主机与现场设备之间的网络地址，在链路初始化时短帧0号命令返回所有与指定网络相连接的现场设备的唯一标识符，即这些设备所处网络端口地址。

④．命令域

只有一个字节，指明该帧所封装的HART命令号。从设备返回的命令字节值应与主设备所发送的帧中的命令号相同。

⑤．数据字节记数域

只有一个字节，指明此字节与一帧最后的校验字节之间的数据字节个数。

⑥．数据域

在主-从长型帧中，此域存放了用户对设备的请求数据。即为了得到从设备的返回值而必须对从设备进行设定的值。

在从-主长型帧中，此域存放了现场设备响应主设备（上位机）的请求，返回的数据。

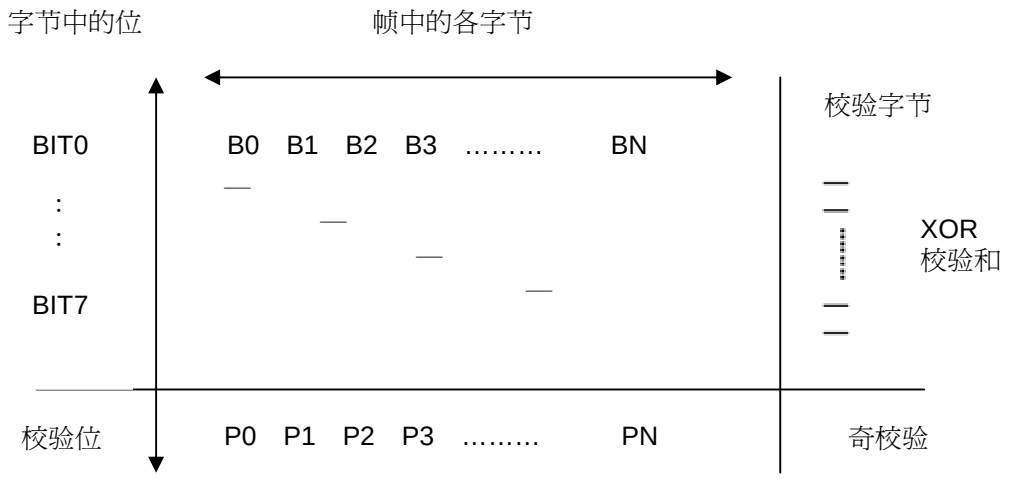
⑦．校验字节

此字节用来存放对帧中的所有字节（不含此字节）进行径向（Longitudinal Parity）校验的结果。HART协议通信中，在两个维数上对传送的信息进行校验，入下图所示：

（1）径向校验值为所有字节依次按位异或后所得的结果；

（2）垂直校验（Vertical Parity）值为在通信过程中硬件自动对每个字节的所有位进行奇偶校验后产生的结果。即前面提到的HART协议物理层规范中规定的数据流格式中的奇校验位。

Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.



HART 协议双向校验

⑧. 响应码字段

该字段包含2个字节，只在从-主长型帧中出现。它指明了HART通信的状态。若响应码第一个字节的最高位（BIT7）为1，说明主、从设备之间的通信出现了错误，该字节的其余各位给出了通信错误的总结信息。BIT7为0时，该字节的其余各位给出了现场设备对该帧所对应的命令的响应情况的总结信息。

响应码的第2个字节指出了现场设备的工作状态。此字节只在响应码第一字节的BIT7为0，即没有通信错误时有效。

3.3 HART协议的服务

HART协议所提供的服务包括：

“至少一次” 可靠地在同等实体之间的交互服务。该服务的设计不提供双重检测。

可选择的，可靠的，同等实体之间提供端对端分段和双重检测的交互服务。

设备标志和设备组态的管理服务。

为实现服务而定义的原语分为两个部分，一部分在正常使用过程中与用户数据相关的称为用户原语；另一部分关于初始化协议，如建立地址，建立地址之间和同等实体之间唯一联系的原语称为管理原语。协议实现时必须支持以上提到的原语。

3.3.1用户接口原语

HART协议支持三种数据传输服务。

Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.

传送(Transmit)服务用来提供送消息和接收响应的基本能力。在此不作详细分析。

传输(Transfer)服务使用每一个消息中一系列的域支持双重检测和消息分段。传输服务提供一种可靠的主-从设备之间双向消息传输。实现传输服务的用户接口原语功能是实现HART协议的重要任务之一。

循环服务提供重复广播数据的功能，是针对HART协议BURST模式的设备功能的实现。

这些服务由主设备初始化。从设备和burst模式设备用来作这些服务的回答者。

3.3.2传输服务

传输服务用来支持可靠的数据连接以防止数据丢失或重复的应用（如上装/下载，块传送等）。由于HART链路层协议的主/从关系，传输服务的执行完全由主设备控制。从设备仅行使响应功能。传输服务帧包含了用来分段、双重检测/释放以及丢失帧检测的序列号区域。帧必须按顺序接收。传输服务的安装和控制都通过发送控制请求来实现。

有八条用户原语支持传输服务。其中四条用作控制，另四条在使用服务时用作数据传送。此外，某些参数是可选的，不必出现在所有的原语调用中。这些参数在原语定义中都由方括号（“[”，“]”）括起来。下面只分析4条数据传输原语。

Transfer.request(address,sequence no,[data])：本原语由主设备HART协议用户使用向给定地址上的从设备实体请求传输信息。主设备用户负责所有参数的合法性。协议应用者将在它的能力范围内对参数进行有限的合法性校验（例如地址超出范围）。

Transfer.indicate(address,sequence no,[data])：本原语由数据链路层激发，通知从设备HART协议用户从对等协议实体中收到了一条合法的传送消息。从设备用户可以接收随后的内容和可选的数据（如果有）。

Transfer.response(status,sequence,[data])：本原语由从设备用户执行，响应进入的transfer.indicate。这种机制用来立即返回先前指示的状态，并可由从设备向主设备返回可选的控制数据参数。

Transfer.confirm(local status,response code,sequence no,[data])：本原语向主设备协议用户返回先前的transfer.request的执行结果。最后收到的从设备的响应（如果有）将与一个状态字一起返回。该状态说明了请求的成功或失败。local状态字节是主设备通讯任务的状态。序列号由从设备设置。

由上面可以看出，主设备HART协议用户，即上位机，主要涉及到的是request和confirm原语，而不用实现indicate和response原语。在实际的程序实现中，体现为一条主-从命令的发送和从设备返回的从-主的接收过程。

Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.

4． HART协议的应用层规范

4.1 HART命令

通用命令：所有设备都实现这些命令。命令号范围是：0 ~ 30；
一般行为命令：多数设备支持这些命令的实现。命令号范围：32 ~ 127；
变送器专用命令：只有一个或几个设备支持这些命令。通过执行专用命令来完成一些独有的特殊功能，和数据处理；命令号范围：128 ~ 255；

4.2 数据格式

①. 无符号整数：用来表示原始数字（raw numbers），如“最后安装号”。

②. IEEE 754浮点格式：

通过协议传递的浮点值是基于IEEE 754单精度浮点标准的。

数据字节

#0	#1	#2	#3
S EEEEEEEE	E MMMMMMM	MMMMMMMM	MMMMMMMM

S－尾数的符号；1＝负

E－指数；与十进制数127的差值以二进制补码形式表示。

M－尾数；低23位，小数部分。

上述浮点数的值通过把2的无偏移指数次方与24位尾数相乘得到。

24 位尾数由一个假设的最高位1，后跟一个小数点，和尾数的23位组成。S1.M X

③. ASCII数据格式：

此格式可以参照任何一个ASCII代码表。

④. 压缩ASCII（6位ASCII）数据格式：

这种数据格式是HART协议的一个独特之处。压缩的ASCII是ASCII的子集，它通过去掉每个ASCII字符的高2位而产生。这就允许4个压缩的ASCII字符占用3个ASCII字符的空间。具体的格式安排情况如下：

压缩的ASCII数据字节	#0	#1	#2
…			
ASCII数据字节	#0	#1	#1 #2	#2	#3
…			
ASCII数据位	543210	54	3210	5432	10	543210
…			

由HART字符集可以看出，HART协议不允许有小写英文字母出现。

⑤. 变量描述：

Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.

变送器提供了四个可以访问的变量输出通道。每个变送器变量都对应一个代码，上位机通过给变送器的每个通道设定不同的变量代码来得到相应的变量值。变量代码表由变送器的生产厂商提供。

5．设备描述语言

随着HART协议的发展，对主设备和现场设备开发者来说，又产生了新的障碍。主设备开发者必须为不断涌现的新现场设备提供支持，同时，现场设备开发者必须为数量正迅速增加的主设备开发相应的接口。

设备描述语言(DDL)是用以描述HART现场设备的一种简单结构化英语语言。DDL将主设备与现场设备操作所需的所有信息都集中到了一起，而目前这些信息却是以不同的形式存在于不同的地方。HART文档描述了其中一些信息(如普通命令、通用命令、通用表等)。变送器特有文档说明了特殊设备信息(如来自于通用命令的偏差，同时又支持通用命令和特殊变送器命令)。CAD图提供了手持终端的外观和流程，甚至有些信息是由手持终端的应用来说明的。例如，整定D/A转换器的过程就是按手持终端处理方法定义的。DDL语言组合了所有这些信息，为对现场设备提供了一种清晰的、不含糊的、一致的描述。

一种正在开发的手持终端将只基于设备描述与现场设备进行操作，而不能与没有设备描述的现场设备进行操作。这具有十分诱人的优点。

新的现场设备可以不依赖于手持终端的版本而发布。一旦现场设备的设备描述存在，这种描述就能被载入手持终端，然后现场设备就能与之操作了。现场设备开发者将不再需要确认手持终端的操作，只需要检验设备描述语言。因此，当前存在于现场设备和手持终端版本间的互相依赖的紧密联系将不复存在。

现场设备开发者在怎样将其产品引入现场及怎样为其用户升级方面具有很大的灵活性。设备描述能驻留在现场设备中，所以合适的设备描述总是有效的。升级的设备描述能以模块的形式提供，并且可以引入到手持终端。可以用软盘来进行升级，也可以用PC软件将其下装到手持终端中。软盘升级可以由用户自己或服务中心来完成。

DDL语言将会代替特殊变送器文档和CAD线图，所以，这会消除以前存在的许多文档问题。

由于目前DDL及其编译器价格较贵，各厂家也没有提供支持DDL的相应的设备，不建议采用和实现支持DDL的功能，而是采用将各类设备的专有属性与通用属性分开，专有属性以不同的动态链接库实现。

郑州波特电子有限公司

交流：E_mail:autobaud@126.com

All contents are subjected to change without prior notice (Rev 1.0) Tel:0371-67212303
•E_mail：autobaud@126.com http://www.hnbaud.com
Copyright © 2006 baud electronic co.,Ltd
Assumes no responsibility for any errors which may appear in this document.