北京航空航天大学学报

2006. 12

蓝牙技术在工业控制系统中的集成和开发

马方魁　郇　极

（北京航空航天大学 机械工程及自动化学院，北京 100083）

摘　　要：针对现代工业控制系统对无线通讯技术的需求，分析了蓝牙协议栈，介绍了蓝牙无线通讯技术在工业设备控制领域中的集成和开发技术，包括通过通用异步接收/发送器 UART（Universal Asynchronous Receiver/Transmitter）使用蓝牙主机控制器接口 HCI（Host Controller Interface）的指令分组、事件分组和数据分组实现设备控制器对蓝牙芯片的操作。说明了建立蓝牙网络所必须的两个步骤：主站发现从站的存在和主站与从站建立连接。最后，介绍一个开发实例：数控机床无线手持操作器，采用蓝牙技术代替电缆连接；系统包括自动连接、模式选择、超时报警等功能；设计了无线传输的有效数据包格式，并对电子手轮脉冲的编码与译码进行了分析。

关　键　词：蓝牙技术；嵌入式控制器；数控机床

中图分类号：TN 919.72

文献标识码：A　　**文 章 编 号：**

Development of bluetooth technique in industrial control system

Ma Fangkui　Huan Ji

(School of Mechanical Engineering and Automation，Beijing University of Aeronautics and Astronautics，Beijing 100083，China)

Abstract：To solve the requirement problem of modern industrial control system to wireless communication technology, the bluetooth protocol was analysed and the integration and development of bluetooth wireless communication technique in industrial device control was introduced, which included accessing the bluetooth chip by UART (Universal Asynchronous Receiver/Transmitter) of using HCI (Host Controller Interface) command packets, event packets and data packets, The two steps of establishing bluetooth wireless net is necessary: the master finds slave and the connecting between master and slave is established. Finally a remote operating panel of numerical control machine tool based on bluetooth was designed, the cable was replaced by bluetooth, which included the system function, such as automatic connection, mode selection, over-time alarm. The format of data packet by using wireless communication was designed, and the encode and decode of electro-handwheel pulse was analysed.

Key words：bluetooth technique；embedded controller； NC-machine tool

---

收稿日期：
基金项目：北京市重点实验室建设项目
作者简介：马方魁（1979－），男，湖北石首人，博士生，mafangkui@163.com

在现代工业控制系统中，特别是在一些工业测控、故障诊断领域，或者对移动工业设备进行控制的场合，采用无线通讯技术具有很大的优越性。

蓝牙技术是 1998 年由爱立信等五家公司联合推出的一种工作于 2.4GHz ISM 频段、基于时分双工的近距离无线通讯规范。其有效距离为 10m，增大发射功率可达 100m，理论传输速率可达 721kbps；多个蓝牙节点可以组成微微网，在微微网中，一个蓝牙主站最多可控制 7 个蓝牙从站，多个微微网可以组成一个散射网，并且每一个蓝牙收发器都被唯一地分配了一个遵循 IEEE802 标准的 48 位蓝牙设备地址；支持适用于数据传输的异步无连接（ACL）链路和适用于语音传输的同步面向连接（SCO）链路。蓝牙的主要应用为笔记本电脑、移动电话以及 PDA（Personal Digital Assistant）设备。由于蓝牙技术的协议开放性、高抗干扰性、价格低廉、功耗低等优点，也具有在工业自动化领域的广泛应用前景。

工业现场的电磁干扰频率一般在 1GHz 以下，因此将蓝牙技术用于工业现场环境有其突出的优势[1]。本文通过对数控机床无线手持操作器的研究与开发介绍蓝牙在嵌入式工业控制系统方面的集成和开发技术。

1 蓝牙协议栈

蓝牙协议规范遵循开放系统互联（OSI）模型，从低到高的定义了蓝牙协议栈的各个层次，如图 1 所示。

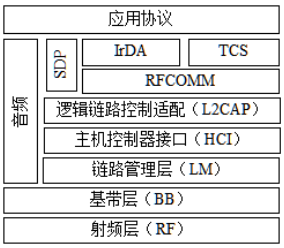

图 1 蓝牙协议栈

蓝牙节点发送数据时，基带（BB）部分将来自高层协议的数据进行信道编码，向下传给射频（RF）进行发送；接收数据时，射频（RF）将经过解调恢复空中数据并上传至基带（BB），基带再对数据进行解码，向高层传输。基带与链路控制器（LC）一起确保微微网内各蓝牙节点之间由射频构成的物理连接；链路管理层（LM）控制链路的建立、加密、控制及功率管理等，用户通过链路管理器可以对本地或远端蓝牙设备的链路情况进行设置和控制；主机控制器接口(HCI)作为蓝牙芯片与设备控制计算机进行数据交换的接口；由于基带数据分组长度较短，而高层协议为了提高频带的使用效率通常使用较大的分组，二者很难匹配，因此逻辑链路控制和适配协议（L2CAP）作为低层协议和高层协议之间不同长度的协议数据单元的桥梁；音频是通过在基带上直接传输同步面向连接数据来实现的；服务发现协议（SDP）是一个服务数据库；RFCOMM 是串口仿真协议，为建立在串口之上的传统应用而提供的接口环境；IrOBEX 是红外对象交换协议，它使高层应用可以同时运行在蓝牙和红外的无线链路上；TCS 是蓝牙电话控制协议规范。用户可以根据不同的需求来选择应用协议。

在工业控制领域中，由于数据的传输量不大但安全性要求比较高，一般可以直接对 HCI 层进行操作。

2 蓝牙 HCI

HCI 提供了一种访问蓝牙模块的物理接口，该接口为用户访问蓝牙模块基带、链路管理器、状态寄存器等硬件提供了统一的命令和方法，对用户来说是透明的。

蓝牙用于工业控制系统中时，蓝牙芯片作为工业设备的外部设备使用，设备控制器通过 HCI 接口直接操作蓝牙芯片，实现无线通讯。对工业设备的物理接口有 RS232、USB 及 UART，其中 UART 最适用于嵌入式系统应用。

采用 UART 接口时，设备控制器和蓝牙芯片间的所有数据的收发都是使用 RX 和 TX 两条信号线来完成的，如图 2 所示。

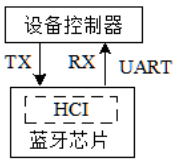

图 2 工业设备和蓝牙芯片间的连接

蓝牙 HCI 具有三种数据类型：指令分组、事件分组、数据分组。指令分组由设备控制器发向蓝牙芯片，用于对蓝牙链路管理器和基带参数进行配置和控制；事件分组由蓝牙芯片发向设备控制器，用于说明指令分组的执行情况；数据分组用于在设备控制器和蓝牙芯片之间双向数据传

输。所有的 HCI 分组都需要附加特殊的标志（蓝牙 RS232 分组指示器）来区分其分组类型，HCI 指令分组标志为 0x01、事件分组标志为 0x04、数据分组标志为 0x02。

例如，在初始化阶段，设备控制器发送 Reset 指令分组即依次发送如下十六进制数据：

0x01	0x030C	0x00

其中，0x01 为 HCI 指令分组标志，0x030C 为 Reset 指令，0x00 为指令所带参数长度。

蓝牙芯片接收到 Reset 指令后将向设备控制器返回一指令完成事件分组：

0x04	0x0E	0x04	0x01	0x030C	0x00

其中，第一个 0x04 为 HCI 数据分组标志，0x0E 表示为指令完成事件。0x0401030C00 为指令完成事件内容。

当蓝牙芯片间建立连接后，设备控制器可以发送或读取 HCI 数据分组：

0x02	连接句柄	数据长度	有效数据

3 蓝牙节点接入过程

正确完成蓝牙节点的接入过程是建立蓝牙网络的关键。该过程通过设备控制器向蓝牙芯片发送 HCI 指令实现。其一般过程如图 3 所示。

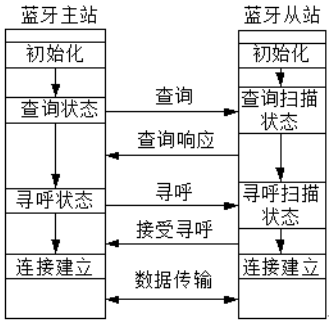

图 3 蓝牙主从站的接入过程

蓝牙节点间要建立通讯联系，在完成各自的蓝牙芯片初始化过程（包括复位、设置事件过滤器、蓝牙从站的查询扫描使能及其扫描时间间隔的设定等）之后，还需要如下两个步骤：

1）主站发现从站的存在（查询模式）：

蓝牙从站要被蓝牙主站发现，需要处于查询扫描状态，而蓝牙主站要发现其它蓝牙节点，应该处于查询状态。蓝牙主站通过查询完成事件来判断周围是否存在其它处于查询扫描状态的蓝牙从站，而通过查询结果事件将得到蓝牙从站的地址等相关信息。

2）主站和从站建立连接（寻呼模式）：

蓝牙从站要被蓝牙主站连接上，需要处于寻呼扫描状态;而蓝牙主站要连接上其它蓝牙设备，应该处于寻呼状态。当主站对某一从站发出寻呼请求时，从站将接收到一个连接请求事件，通过发送接受连接请求或拒绝连接请求指令来建立或拒绝该连接。

查询和寻呼的主要区别在于蓝牙主站是否知道蓝牙从站的设备地址。如果主站已经知道了从站的设备地址，则上述步骤 1）可以省略，这样可以减少蓝牙节点间建立连接的时间。

连接建立后，蓝牙主、从站将分别返回一个包含有连接句柄的连接完成事件，通过该连接句柄，蓝牙主、从站可以互相发送 HCI 数据分组。

4 数控机床无线手持操作器设计

数控机床手持操作器一般通过电缆与数控单元相连，如图 4 所示。在大型机床上，需要较长的电缆，操作不方便。

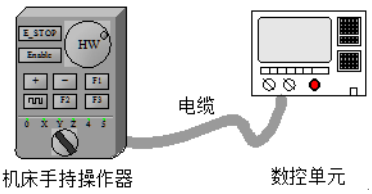

图 4 数控机床手持操作器与数控单元的电缆连接

采用蓝牙技术，可以实现无线操作，作者设计的数控机床无线手持操作器如图 5 所示。

手持操作器作为主站，数控单元作为从站，蓝牙芯片遵从蓝牙 1.1 规范，射频输出为 class2 级（10m）。在手持操作器中内嵌的 AVR 单片机上实现本嵌入式系统软件以及 HCI 驱动。主站采用两节 3V 电池供电，耗电量约为 270mW。

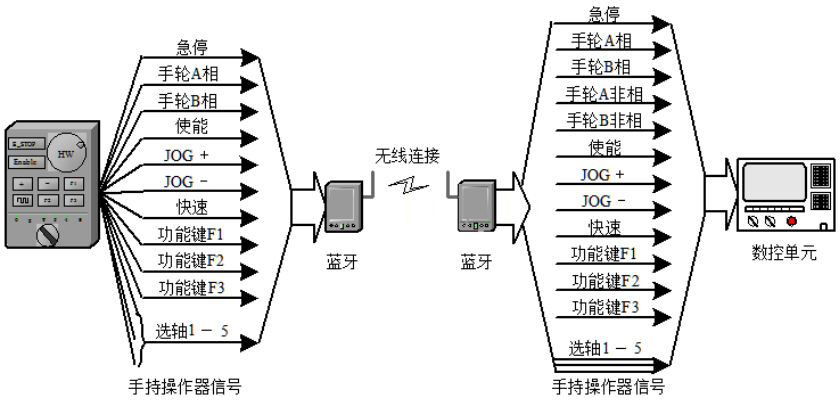

图 5 数控机床手持操作器与数控单元的无线连接

4.1 系统功能：

自动连接：因某种原因（如超出通讯距离）通讯中断后，自动尝试恢复连接；

模式选择：通过跳线选择查询或寻呼模式，采用寻呼模式时，主站直接从单片机内部 EEPROM 中读取从设备地址；

超时报警：在超过设定的时间内没有对手持操作器进行操作时，提示继续操作或关闭主站电源，节省电源电池的消耗；

备用电源：电源供电不足时，自动启动备用电源；

运行状态指示：指示运行状态，如查询、连接以及传输数据等状态。

4.2 数据传输：

主站采集手持操作器上的操作信息打包成 4 个字节的有效数据并每隔 50ms 发送一次。由于蓝牙基带层具有错误重传机制，可以大大减少由于链路质量不好而数据包丢失的可能性。从站接收数据包，在 10ms 时间内完成数据的解码和端口输出，并准备好接收下一个数据包。

蓝牙 HCI 数据分组传输的有效数据为手持操作器上的 I/O 量（手动、选轴、急停、使能、快速及功能选择）、电子手轮增量及转动方向和用于同步主从站间状态指示的数据位，其数据格式如图 6 所示。

LSB MSB

开关量数据（11位）	保留（5位）	手轮增量低8位（8位）	保留（2位）	主从同步显示控制（2位）	手轮增量高2位（2位）	手轮方向（2位）

图 6 机床手持盒数据格式

为了保证手持操作器中“急停”功能的实时性要求，系统对“急停”信号的处理在硬件上采用冗余结构：增加一对无线数据收发模块，软件上采用中断机制保证优先处理该信号。

4.3 电子手轮脉冲的编码与解码：

数控机床手持操作器中，电子手轮输出为二相正交脉冲。以正向旋转为例，如图 7 所示，共有四种状态：0、1、2、3。

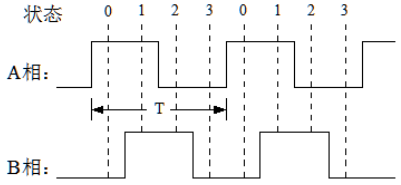

图 7 手轮脉冲状态图

采用一维数组表示如下（位 0 与位 1 表示 A 相和 B 相，位 6 与位 7 表示 A 非相和 B 非相）：

```
hw_status[4]＝{0x81,   //10xxxx01B
              0x03,   //00xxxx11B
              0x42,   //01xxxx10B
              0xC0}; //11xxxx00B
```

当电子手轮转动时，其状态变化如图 8 所示：

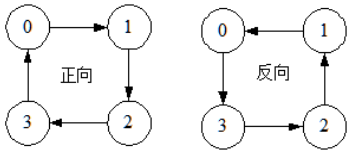

图 8 手轮脉冲状态变化图

主站采样得到脉冲增量和转动方向。从站从接收到的数据包中提取脉冲增量和转动方向数据，利用单片机端口恢复手轮 A、B 相以及 A 非、B 非相信号，脉冲宽度由周期时间 10ms 除以该周期内的脉冲增量数得到。

5 结束语

针对工业控制领域内对无线网络的需求，本文对蓝牙在工业控制系统中的集成与开发技术作

了比较详细的介绍，并介绍了一个开发实例：数控机床无线手持操作器，对实际应用具有重要参考价值。

参考文献(References)

[1] 凌玲，李志国．蓝牙在工业现场的应用[J]．武汉理工大学学报，2001，23（6）：41~43

Ling Ling, Li Zhiguo. The Research of Bluetooth in Industrial Environment[J]. Journal of Wuhan University of Technology，2001，23（6）：41~43(in Chinese)

[2] Großeschallau M, Witkowski U, Rückert U, Low-cost Bluetooth Communication for the Autonomous Mobile Minirobot Khepera[A]. In: IEEE, International Conference on Robotics and Automation[C]. Barcelona, 2005. 4194~4199

[3] Bilstrup U, Wiberg P, Bluetooth in industrial environment[A]. In: IEEE: 2000 IEEE International Workshop on Factory Communication Systems[C]. porto, 2000. 239~246

[4] 马建仓，罗亚军，赵玉亭．蓝牙核心技术及应用[M]．北京：科学出版社，2003

Ma Jiancang, Luo Yajun, Zhao Yuting. Core Technology and Application of Bluetooth[M].Beijing: Science Industry Press, 2003 (in Chinese)