# The Master Software Implementation of PROFIBUS-DP-Based Motor Protection Device

**Jin Mao, Zhihuo Wang**
*Northwestern Polytechnical University, Xi'an, China*
*Email: jinmincn@sina.com, zhihuo2010@yahoo.cn*

**Abstract:** With the features of good property of real-time, high transmitting rate, low cost, and being widely applied in industrial production, profibus is considered as one of the openly international standards. Profibus includes profibus-dp, profibus-fms and profibus-pa, and we just adopt dp only in this design. And give information of dp's structure, analysis of message and the implementation of communication between master and slave.

**Keywords:** profibus-dp; master; software implementation

# 基于 PROFIBUS-DP 协议的电机保护装置上位机软件实现

毛　晋，王志伙
[1]西北工业大学，西安，中国，710129
Email: jinmincn@sina.com，zhihuo2010@yahoo.cn

**摘　要：**PROFIBUS 现场总线因具有通信实时性强、高传输率、低成本、适于各种生产场所等优点而成为开放的国际标准，包括 PROFIBUS-DP、PROFIBUS-FMS 、PROFIBUS-PA，本文主要采用的 DP 协议，介绍了 DP 协议的结构、报文分析以及软件实现了模拟主站和从站的的通信过程。

**关键词：**PROFIBUS-DP；上位机；软件实现

## 1 引言

而现场总线的应用则是工业自动化的关键。当现场总线技术在我国广泛而简单的应用而其核心技术却不掌握在外国公司手中是不能认为我们的工业自动化达到一个很高的程度。因此需要加强对现场总线的核心技术的研究。

在众多现场总线中，Profibus 现场总线是其中最具影响力的现场总线之一，它有总线传输速度高，可应用于对时间要求苛刻的复杂控制系统，包含多种行规，并且可以在不同厂家的产品之间使用。并且 Profibus 在我国得到了非常广泛的应用，但国内对 Profibus 的研究起步较晚，应用于该总线的现场设备几乎全部是外国产品，尤其是西门子，价格比较昂贵。所以对 Profibus 技术进行深入研究以提高深层次的应用有现实意义。

## 2 PROFIBUS 现场总线

### 2.1 PROFIBUS-DP 协议

PROFIBUS-DP 协议是为自动化制造工厂中分散的 I/O 设备和现场设备所需要的高速数据通信而设计的。DP 常见的配置是单主从结构。DP 主站和从站之间的通信基于主从原理，只有当主站请求时总线上的 DP 从站才可能活动。DP 主站按轮询表依次访问 DP 从站。DP 主站和 DP 从站间的用户数据连续的交换，而并不考虑用户数据的内容。

## 3 主站从站通信的实现

### 3.1 调试设备及工具

软件实现是基于 VB，所以程序的编程环境是 Visual Basic6.0 可视化软件开发工具有丰富的控件，这些控件能很方便的实现一些复杂的功能。由于按照 PROFIBUS-DP 规约，通信一般是要用 D 型的串口，故 MSComm 控件用来进行数据地传输和接收，提供串行通信的功能。

### 3.2 各模拟功能的具体实现

### 3.2.1 程序的总体流程

程序完成了一类主站和从站的通信过程包括对从站的诊断、参数设置、组态以及数据交换。流程如下：首先选择从站，然后具体的实现步骤：

1 从站状态查询。即 FDL 状态诊断，查看从站是否在总线上。如果总站在总线上，而且正常就会对主站回应，主站就回收到和发送数据位数相同的一帧数据。进行分析后可以知道从站目前的状态，如果是正常的，则可以进行下一步；而如果不正常或没有回应就会再次发送进行诊断直到有正确回应或到最大次数后屏蔽此从站进入轮询表的下一从站。

2 发送诊断信息。即初次诊断，查看从站能不能正常工作。与状态查询对比，第一步只是看从站是否在线，第二步则是要进行简单检测，看从站是不是正常。发送数据后就等待从站回应。如果从站正常就会回应一帧比发送数据多几位的回复，报告从站的正常，这是可以进入参数设置。

3 设置从站参数。对从站的一些参数做相应的设置，从站给主站做短应答，然后可以进入下一步。

4 从站组态。对从站的一些 I/O 进行组态，完成以后，从站会给主站一个短回应。

5 诊断。即再次诊断，初次诊断是来确定从站是不是正常，再次诊断是来检查看参数设置和组态是不正确。之后进入数据交换。

### 3.2.2 初始化流程

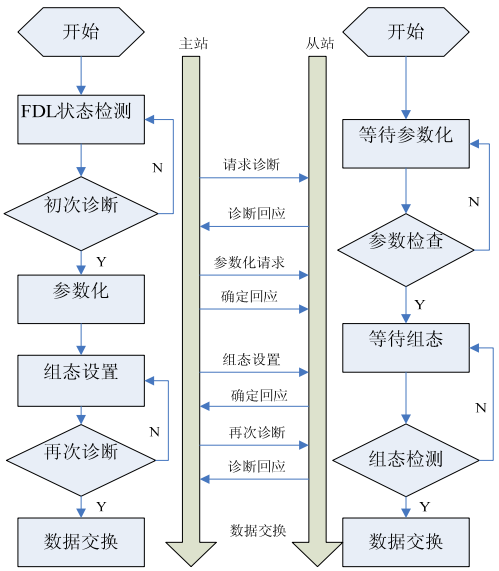


**Figure 1. 状态诊断流程图**

**图 1. 初始化流程图**

在主站和从站设备进行数据交换前，主站必须对从站进行参数设置，并配置其通信接口，因此主站首先要检查从站在不在总线上，如果在总线上则就要通过诊断从站诊断数据来检查 DP 从站的准备情况。当从站报告准备好接收参数时则主站要对从站进行参数设置同时检测通信接口配置，如果正常则从站就要对其回应。当接收到回应以后，主站会再次进行从站的诊断，看前面是不是有出错。当诊断回应也正常以后就完成了初始化过程可以进行数据交换。主站和从站在初始化过程中的动作如下图所示：

1 .FDL(现场总线数据链路)状态诊断

流程如下：

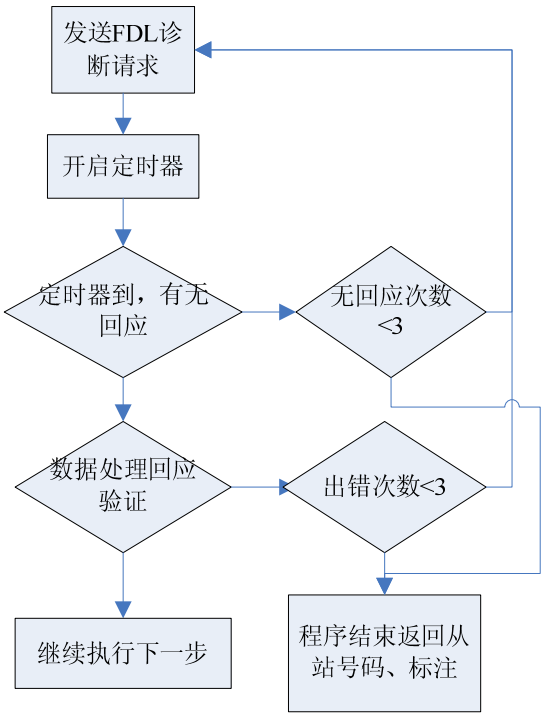


**Figure 2. FDL State diagnosis flowchart**

**图 2. FDL 状态诊断流程图**

在 FDL 诊断过程中主要用到了的 MScomm 控件以及 Timer 控件。由于主站对数据的接收一般要用到查询方法，故在软件实现过程，使用 Timer 定时去查看接收数据。

主站对从站发送的 FDL 帧为 10 02 01 49 4C 16

从站对主站的回应为 10 01 02 00 03 16

2 初次诊断过程

诊断过程为向从站发送诊断帧，同时开定时器等待从站回应，待收到回复数据后进行校验



978-1-935068-40-2 © 2010 SciRes.

诊断帧的格式为：主站发送的诊断请求帧：68 05 05 68 82 81 6D 3C 3E EA 16
从站的回应信息应该是：68 0B 0B 68 81 82 08 3E 3C 00 3C 00 FF 03 04 C7 16
此帧表明，从站未被主站锁定，支持同步/锁定功能

3 参数化的实现流程

参数化之前要先检查从站是否被其他主站锁定，只有未被锁定才能对其参数化，过程是发送数据同时开启定时器等待回应，收到回应后对数据进行校验。参数化是主站对从站发送参数设置帧，当从站设置完成后会对主站回应短应答帧主站对从站发送参数设置信息：68 0C 0C 68 82 81 7D 3D 3E B8 01 0D 0B 03 04 00 D3 16
参数化成功后从站对主站的回应为 SC 短应答： E5
如果参数化失败从站不对主站回应
参数化完成后进入组态诊断过程

4 组态诊断过程

组态诊断的流程为发送数据同时开启定时器等待回复，收到回复后进行数据校验。

组态报文的作用主要是对 I/O 的类型及性质进行设定，还可指定制造商的一些特殊 I/O 设置。组态请求报文的 DU 单元至少有 1 个字节，最多有 244 个字节。本程序的的 DU 单元包括 3 个字节。具体报文：68 06 06 68 82 81 7D 3E 3E DF DF EF 11 16

组态成功后从站对主站的回应为 SC 短应答： E5

如果组态失败从站不对主站回应。

5 再次诊断过程

再次诊断过程类同第一次诊断过程，目的是检查从站的参数化过程，组态过程是否正确，是否准备好进入数据交换过程：主站发送：68 05 05 68 82 81 6D 3C 3E EA 16
如果从站准备好，则从站对主站回应：68 0B 0B 68 81 82 08 3E 3C 00 3C 00 FF 03 04 C7 16

### 3.2.3 数据交换过程

数据交换过程是主站周期的，循环的给从站发送数据请求，从站同时周期的对主站进行回应。本程序的数据交换过程完成了三个功能，遥信、遥测、遥控。

遥测功能实现：

遥测功能是读取从站的线圈的闭合状态。实现过程首先是主站向从站发送遥测的数据请求报文，同时打开定时器，然后应收到从站的数据回应，如果定时器时间到时仍未收到从站回应则再次发送数据请求。当收到数据回应后，主站调用数据分析函数，解析数据后把结果保存，并显示在界面上面。同时进入下一次数据交换的循环中。具体的流程图如下

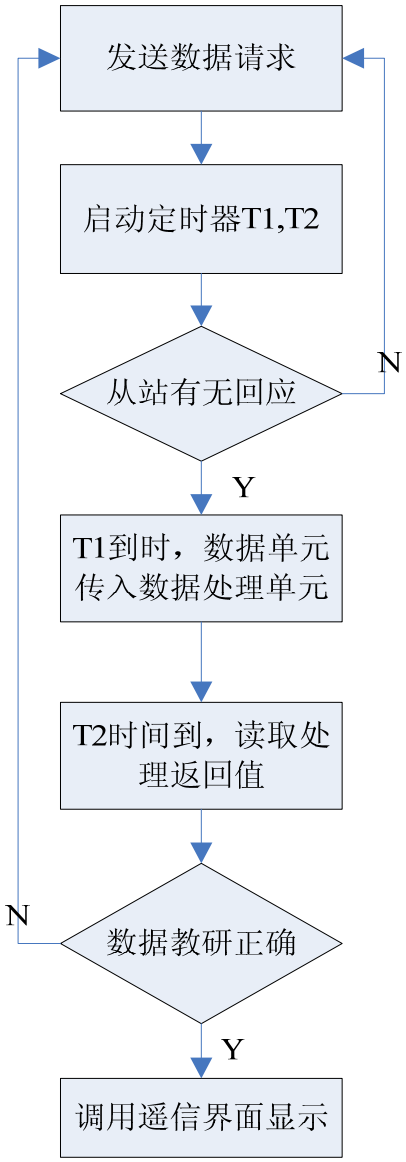


**Figure 3. Telemetry function flowchart**
**图 3. 遥测功能流程图**

在遥信阶段，主站对从站发送的数据请求帧报文为： 68 04 04 68 02 01 7C 02 81 16

特别说明一下在诊断过程中 DA,SA 的高 8 位最高位为 1，而在数据交换过程中 DA,SA 的高 8 位为 0

遥信帧，主站对从站的发送的数据单元只有一个字节，02 表示这个帧是向从站要遥信数据。

当从站收到此帧报文以后，按照组态报文里面固定的 16 个输出，向主站回应 16 个输出口的当前状态

从站的回应信息为：68 06 06 68 01 02 08 02 XX XX XX 16

从站对主站的回应的数据单元包括 3 个字节

02 同主站报文，表示是对遥测请求的回应

XX XX 表示 16 个输出开关的状态，表示方法是转化为二进制后，从低位到高位，该位为 1 则表示闭合，为 0 则表示开。例如 01 07 表示 1 位 2 位 3 位 9 位闭合，其他位开。

遥测功能的实现：

遥测功能是主站向从站发送请求从站的参数（电压，电流）然后等待从站采集后回应主站。

流程图与遥信相同，区别在最后调用界面显示从站的采集的信息。

主站向从站发送的遥测数据请求报文：68 04 04 68 02 01 7C 04 83 16

遥测帧，主站对从站的发送的数据单元只有一个字节，04 表示这个帧是向从站要遥测数据。从站收到此帧以后，按照组态规定，将当前采集参数发送主站。

从站对主站的回应信息为：68 36 36 68 01 02 08 DU XX 16

数据单元 DU 包括 33 个字节，第一个字节固定为 04 表示是对主站遥测的回应信息后 32 个字节表示遥测的数据信息，每两字节表示一个采集信息，共 16 个，所以要 32 位

遥控过程的实现：

遥控过程的是对从站的开关的状态进行控制，所以在控制之前要先读取该开关的状态，也就是在遥控工程的实现中要先有一个遥信过程然后才是遥控。读取从站开关之后进行如同遥信的流程，最后调用的是遥控结果的界面返回。

遥控时，主站对从站的发送遥控请求报文： 68 06 06 68 02 01 7C 05 XX XX XX 16

DU 数据单元包括 3 个字节

05 表示是遥控请求数据

XX 表示遥控号，从 01 到 10 共 16 路

XX 表示是开，还是关，FF 表示开，00 表示关，只有这两种情况

如果遥控成功，从站对主站的回应为短应答 SC ：E5

数据处理过程的流程如下：

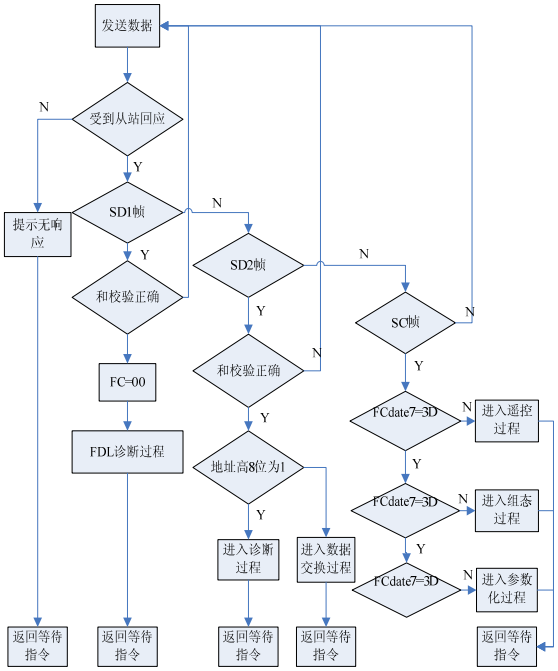


**Figure 4. Data processing unit flowchart**

**图 4. 数据处理单元流程图**

数据处理单元在本程序中处于核心的地位，在此列出数据处理单元流程图。

## 4 结束语

选取的当前运用最成熟的 PROFIBUS 现场总线进行了研究，主要工作如下：

详细介绍了主从通信的软件实现，包括两个过程：初始化和数据交换，以及各个功能的实现。给出了了各个部分实现的使用的报文，并对报文进行了解释。最后提供的数据处理的流程图。

实现上位机程序和实际的下位机 PLC 的通信。只实现了遥信、遥测和遥控功能，没能做进一步的深入来实现更多功能。暂时只实现了单主从的通信，没能做到多主从通信的功能。

## References (参考文献)

[1] Guohai Liu, Kangji Li, Wenping Xue. The Fieldbus PROFINET[M]. Beijing: Electronic Industry Press.2007-9-1
刘国海，李康吉. 薛文平现场总线 PROFINET[M]. 电子工业出版社，2007-9-1.

[2] Zhengjun Li,. The Fieldbus and Application Technology[M]. Beijing: China Machine Press.2005
李正军，现场总线及其应用技术[M]. 机械工业出版社，2005，

[3] Huafeng Xing., Development of the Embedded Intelligent Slave Station Based on PROFIBUS-DP Technology [D]. DaLian: Dalian Maritime University



978-1-935068-40-2 © 2010 SciRes.

邢化峰，基于 PROFIBUS_DP 技术嵌入式智能从站的研制[D]. 大连海事大学.

[4] Yonghua Wang, A.Verwer The fieldbus Technology and Application Tutorial. Beijing: China Machine Pres. 2007
王永华，A.Verwer. 现场总线技术及应用教程[M]. 机械工业出版社. 2007

[5] Chunfeng Lv. Based on 51 Series of Single Chip PROFIBUS_DP Salve Research[D]. Kunming University of Science and Technology
吕春峰，基于 51 系列单片机的 PROFIBUS_DP 智能从站研究[D]. 昆明理工大学.

[6] Hao Chen .Research and Design Based on Intelligent Slaver of Profibus-DP Fieldbus[D]. Beijing: China Academy of Machinery Science and Technology
陈浩，基于 Profibus_DP 现场总线智能从站的开发与研究[D]. 机械科学研究院.