# Modbus 协议在电力系统中的应用

张海源[1]， 任春梅[2]， 张冉[2]

（1. 宁夏电网建设运行公司，宁夏 银川 750001；2. 国家继电器质量监督检验中心，河南 许昌 461000）

**摘要**：Modbus 协议在 1987 年由施奈德公司制定，由于其简单而精致的结构得到大家的支持，目前，在电力行业 Modbus 协议也得到了广泛的应用，但是由于 Modbus 协议自身的特点与电力系统的使用习惯还有不相符的地方，在 Modbus 协议实现中还有一些问题，现从参数地址的编制、功能码的选择以及应用功能等方面讨论 Modbus 协议实现中的一些问题，并从特殊应用功能和常用应用功能对电力系统应用功能进行分析和举例。

**关键词**：Modbus； 通信规约； 参数地址编制； 功能码； 应用功能

## Application of Modbus protocol in power system

ZHANG Hai-yuan[1]， REN Chun-mei[2]， ZHANG Ran[2]

（1.Ningxia Electric Power Network Construction and Operation Company,Yinchuan 750001,China;
2.National Center for Quality Supervision & Testing of Relay & Protection Equipment，Xuchang 461000,China）

**Abstract:** Modbus protocol formulated in 1987 by Schneider Co.,Ltd, obtained everybody as a result of its simple and the fine structure the support.At present, Modbus protocol is also obtained the widespread application in the power system but because the Modbus protocol own characteristic and the electrical power system use custom also had the place which did not tally, so had some questions in the Modbus protocol realization, this paper from parameter address establishment, functional code choice as well as application function, discusses in the Modbus protocol realization, analyses the electrical power system application function and gives an example from especial application function and common application function.

**Key words:** Modbus; communication protocol; parameter address establishment; functional code; application function

中图分类号： TM73; TM764; TM77 文献标识码： B 文章编号： 1003-4897(2007)17-0031-04

## 0 引言

1978 年由施奈德公司制定了 Modbus 协议，当时它主要是用于电子控制器上的一种通信语言，实现控制器之间，控制器由网络和其他设备之间的通信，支持传统的 RS232/RS422/RS485 和最新发展的以太网设备。

在 1996 年施奈德公司又推出了基于 TCP/IP 的 Modbus 协议成本低廉适用于各种应用的解决方案，在自动化设备中得到了广泛的应用。

我国国家质量监督检验检疫总局和国家标准化管理委员会联合于 2004 年 9 月正式发布了 Modbus 协议的国家标准 GB/Z 19582.1/2/3-2004，从 2004 年开始，国家继电器质量监督检验中心针对 Modbus 规约进行了一系列的测试 。

为了更好地推广和使用 Modbus 规约，本文从检测实践入手，有针对性地论述在使用 Modbus 规约实践中应该注意的问题，使 Modbus 规约成为电力系统信息交换的有利工具。

## 1 Modbus 协议介绍

Modbus 是一种请求/应答方式的协议；

目前可以通过下列方式实现 modbus 通信：

1）以太网上的 TCP/IP；

2）各种介质（有线：EIA/TIA-232-F、EIA-422、EIA/TIA-485-A；光纤、无线等）上的异步串行传输；

3）Modbus PLUS，一种高速令牌传递网络 Modbus 规约一般结构

4）应用数据单元（ADU）的一般结构（如图 1 所示）。

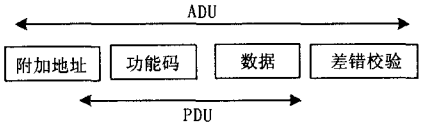


**图 1 应用数据单元（ADU）的一般结构**
Fig.1 General MODBUS frame

## 2　实现标准 Modbus 协议的重点

Modbus 协议是对针对寄存器进行访问的一种协议，Modbus 协议处理的所有数据都放置在设备应用存储器中，存储器的物理地址需要与寄存器的逻辑地址关联起来，那么实现标准的 Modbus 协议有两个关键问题需要注意：参数地址的编制和功能码的选择。下面就两个问题进行分析讨论。

## 3　参数地址的编制

### 3.1 Modbus 数据模型

我们首先来看一下 Modbus 数据模型，Modbus 的数据模型是以一组具有不同特征的表为基础建立的。4 个基本表见表 1。

表 1　基本表

Tab.1 Primary table

| 基本表 | 对象类型 | 访问类型 | 注释 |
|---|---|---|---|
| 离散量输入 | 单个位 | 只读 | I/O 系统可提供这种类型数据 |
| 线圈状态 | 单个位 | 读写 | 通过应用程序可改变这种类型数据 |
| 输入寄存器 | 16 位字 | 只读 | I/O 系统可提供这种类型数据 |
| 保持寄存器 | 16 位字 | 读写 | 通过应用程序可改变这种类型数据 |

根据表 1，我们可以将电力系统中 Modbus 协议的数据分为四类：开入量（离散量输入）；开出量（线圈）；只读模拟量（输入寄存器），例如遥测值等；可读写模拟量（保持寄存器），例如保护定值、设备参数等。

很显然，必须将 Modbus 处理的所有数据（位，寄存器）放置在设备应用存储器中。但是，存储器的物理地址不应该与寄存器编号混淆，仅要求将寄存器编号与物理地址链接。

### 3.2 参数地址的编制

在 Modbus 协议中数据模型常用的有两种：带有 4 个独立块的 Modbus 数据模型和仅有 1 个块的 modbus 数据模型，对于不同的数据模型参数地址的编制有所不同。

第一种数据模式：带有 4 个独立块的 Modbus 数据模型；

说明：图 2 只是地址分配的一个示例，用户在使用时可以根据实际需求来分配。

图 2 表示了含有数字量和模拟量、输入量和输出量的设备中的数据组织，由于不同块中的数据不相关，每个块是独立的，那么对于不同类的参数地址是独立的，参数地址的编制可以重复，但是每一类参数的地址必须从 0 开始编制，并且一个参数一个地址，参数地址的编号必须是连续的。

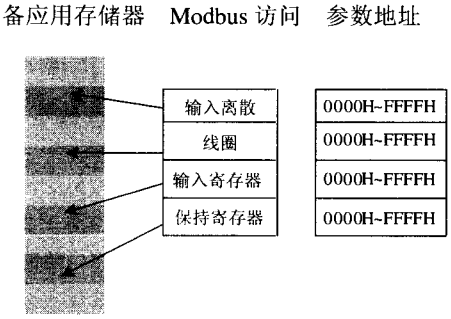


图 2 带有独立块的 Modbus 数据模型

Fig .2 Modbus data model with separate block

第二种数据模式：仅带有 1 个块的 Modbus 数据模型：

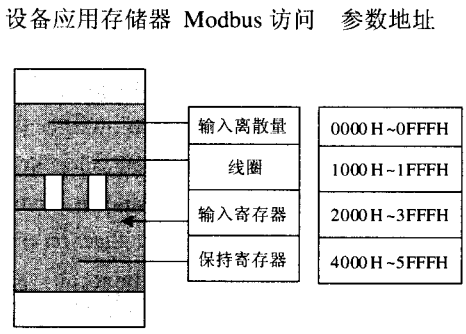


图 3 仅带有 1 个块的 Modbus 数据模型

Fig.3 Modbus data model with only 1 block

说明：图 3 只是地址分配的一个示例，用户在使用时可以根据实际需求来分配。

图 3 也同样含有数字量和模拟量、输入量和输出量，但是由于设备仅含有一个数据块，因此不同类的参数地址不能重复，某一种参数地址从 0 开始编制，一个参数一个地址，参数地址的编号必须是连续的。

下面总结一下参数地址编制的几个方面：

1) 将装置的参数按照 Modbus 数据模型进行分类；

2) 确定数据模式；

3) 参数第一个有效地址从 0 开始编制；

4) 参数地址必须是连续的，暂时没有用到的地址应最好注明备用。

## 4　选择合适的功能码

选择合适的功能码也是实现标准 Modbus 协议

重要的一个方面，目前很多厂家为了方便尽可能少用几个功能码，这就造成功能码的挪用、多用现象，也就由于各个厂家在互连的时候同一个功能或同一类参数使用不同的功能码而造成一些功能不能实现。参数类型与功能码的对应关系见表 2。

**表 2 参数类型与功能码的对应关系**

Tab.2 Corresponding relation of parameter type with function code

| 基本表 | 功能码（读功能） | 功能码（写功能） |
|---|---|---|
| 离散量输入 | Fun02 | - |
| 线圈状态 | Fun01 | fun05，fun15 |
| 输入寄存器 | Fun04 | - |
| 保持寄存器 | Fun03 | fun06，fun16 |

## 5　应用功能的实现

作为工业控制领域常用的通信协议 Modbus，在工业控制领域显示了巨大的影响力，由于其简单而精致的结构，近年来在电力系统中也得到了广泛的应用，但是由于 Modbus 开始是应用在工业控制领域的，它自身的特点与电力系统中的应用习惯并不是很一致，那么从 Modbus 协议到电力系统应用功能的映射就会有一些问题，下面主要从电力系统中特殊功能和常用功能两方面介绍电力系统应用功能的实现。

### 5.1 特殊功能的实现

#### 5.1.1 选择/执行功能的实现

表面上看 Modbus 协议不支持选择/执行功能，但是由于电力系统中的特殊要求或者电力用户的要求必须实现选择/执行命令，面临这个问题的时候很多厂家放弃了使用 Modbus 协议而使用其他通信协议。其实没有这个必要，下面介绍利用参数地址关联实现选择/执行命令的方法。

例如对于线圈 1 来说实现选择/执行命令：

第一步：参数地址的编制。在这里线圈 1 代表的不是一个参数，而是两个参数，分别是线圈 1（选择）和线圈 1（执行），两个参数放在两个寄存器中（寄存器地址可以相邻也可以不相邻，以下以寄存器相邻为例）。具体的参数地址见表 3。

**表 3 线圈地址**

Tab.3 Coil address

| 参数地址 | 参数名称 |
|---|---|
| 0000H | 线圈 1(选择) |
| 0001H | 线圈 1（执行） |

第二步：功能码的选择。对于遥控命令我们可以选择 fun05 和 fun15，如果一次控制单个线圈状态则使用 fun05；如果一次控制多个线圈状态使用 fun15（根据电力系统的特点一般使用 fun05）。

第三步：遥控过程。下面利用通信报文说明遥控过程（假设子站地址为 1）。

选择（合）命令：

主站请求：01 05 00 00 FF 00 8C 3A

子站响应：01 05 00 00 FF 00 8C 3A

执行（合）命令：

主站请求：01 05 00 01 FF 00 DD FA

子站响应：01 05 00 01 FF 00 DD FA

为了遥控的安全性可以对遥控条件进行逻辑判断，例如只有在选择后才能进行执行命令、选择命令和执行命令是否是同一参数地址等等。

#### 5.1.2 读 SOE 数据

在电力系统中读 SOE 数据是一个常见的功能，但是由于其包含的数据信息很多，很多在使用 Modbus 协议完成读 SOE 数据功能时就觉得标准中没有定义读 SOE 数据的功能码和帧格式，那么就会自定义一些功能码或者使用功能码 04 或 03 而改变其帧格式。显然，这种做法是不符合标准要求的，也就给实际工程中的互操作问题埋下伏笔。在这里我们介绍如何使用规定的功能码和帧格式实现读 SOE 数据功能。

例如在装置中有 3 条 SOE 数据，每一条 SOE 数据中包含的信息有故障类型、故障时间（年、月、日、时、分、秒）、ABC 相电流、零序电流，下面以此为例介绍读 SOE 数据功能。

第一步：参数地址的编制（如表 4 所示）。

**表 4 SOE 数据地址**

Tab.4　SOE data address

| 参数地址 | 参数名称 |
|---|---|
| 0100H | 最新故障类型 |
| 0101H | 年、月（高字节为年、低字节为月） |
| 0102H | 日、时（高字节为日、低字节为时） |
| 0103H | 分、秒（高字节为分、低字节为秒） |
| 0104H | A 相电流 |
| 0105H | B 相电流 |
| 0106H | C 相电流 |
| 0107H | 零序电流 |
| 0108～010F | 备用 |
| … | 上次故障（SOE）信息（格式与最新故障信息相同） |
| 0118～011F | 备用 |
| … | 再上次故障（SOE）信息（格式与最新故障信息相同） |

第二步：功能码的选择。在电力系统中 SOE 信息一般是只读数据，因此我们建议使用功能码 04 完成读 SOE 数据功能。

第三步：读取 SOE 数据过程。下面利用通信报文说明读 SOE 信息过程（假设子站地址为 1）。

读最新故障（SOE）信息：

主站请求：01 04 01 00 00 08 F0 30

子站响应：01 04 10 00 01 06 05 09 10 15 30 13 90 13 86 13 88 00 00 4D B4

读再上次故障（SOE）信息：

主站请求：01 04 01 20 00 08 F1 FA

子站响应：01 04 10 00 02 06 05 09 10 16 31 13 90 13 86 13 88 00 00 F3 2A

注：必须保证在子站响应报文中每一个寄存器打包成 2 个字节数据。

5.1.3 功能码 07 的使用

功能码 07 用来读取 8 个异常状态，该功能提供一种简单的访问异常状态的方法，异常状态可以是装置在线状态、故障状态、报警状态、新事件产生状态（是否有新事件产生）等 8 个状态，这 8 个异常状态存放在设备存储器中，不需要给定寄存器地址。主站不断的利用功能码 07 读取这 8 个异常状态可以快速得到常用的状态信息然后再确认是否需要利用相应的功能码读取详细信息。

目前在国内很少厂家使用功能码 07，主站主要通过周期轮询的方式读取数据，随着电力系统的发展和电力设备的升级，设备中的信息不断增加，使用功能码 07 可以实现重要信息优先上送。

例如 8 个异常状态代表的实际意义为设备在线状态（bit 0）、报警状态（bit 1）、跳闸状态（bit 2）、新事件产生状态（bit 3）、遥信变位状态（bit 4）、备用（bit 5）、备用（bit 6）、备用（bit 7）。

通信报文如下：

主站请求：01 07 41 E2

子站响应：01 07 1F 63 F8

从子站响应的报文可以看出设备处于在线状态、设备有报警、设备有跳闸、设备有新事件产生、设备有遥信变位。根据子站上送的信息主站可以根据相应的功能码读取详细信息。

注意:功能码07仅适用于链路上实现的Modbus协议。

### 5.2 常用功能的实现

下面主要总结电力系统中常用的应用功能，从参数地址的编制和应用功能与功能码的对应关系两方面讨论。

5.2.1 参数地址的编制

根据前面我们讲到的参数分类办法先将常用的参数进行分类并编制参数地址（如表 5 所示）。

**表 5 参数分类和参数地址编制**

Tab.5 Parameter categorise and parameter address documentation

| 参数类型 | 参数名称 | 地址 |
|---|---|---|
| 读写位参数 | 线圈 1 | 0000H |
| | 线圈 2 | 0001H |
| | … | … |
| 只读位参数 | 开入 1 | 0000H |
| | 开入 2 | 0001H |
| | … | … |
| 读写字参数 | 过流Ⅰ段保护定值 | 0000H |
| | 过流Ⅱ段保护定值 | 0001H |
| | 装置时间（年、月） | 0002H |
| | 装置时间（日、时） | 0003H |
| | 装置时间（分、秒） | 0004H |
| | … | … |
| 只读字参数 | A 相电流 | 0000H |
| | B 相电流 | 0001H |
| | … | … |

注：1)上述地址编制的数据模型是带有 4 个独立数据块的 Modbus 数据模型；2)“…”表示同类参数的其它参数和参数地址。

5.2.2 应用功能与功能码的对应关系

**表 6 应用功能与功能码的对应关系**

Tab.6 Corresponding relation of application function with function code

| 应用功能 | 功能码 |
|---|---|
| 读遥信状态 | Fun02 |
| 读遥测量 | Fun04 |
| 读装置自身信息 | Fun04 |
| 读线圈状态 | Fun01 |
| 读装置定值信息 | Fun03 |
| 修改装置定值 | Fun06 和 Fun16 |
| 读装置时间 | Fun04 |
| 对时 | Fun06 和 Fun16 |
| 读装置通信参数 | Fun03 |
| 遥控 | Fun05 和 Fun15 |
| 远程复位功能 | Fun06 |

## 6 结论

从本文的分析我们可以看出，作为工业控制领域常用的通信协议—Modbus，在工业控制领域显示了巨大的影响力，在电力行业，由于其特殊性和独特的应用习惯，需要将 Modbus 协议自身的特点与电力习惯很好地结合，在使用过程中需要正确编制

（下转第 57 页 continued on page 57）

状及其展望[J]. 电力自动化设备, 2005, 25(2): 1-9.
FU Xu, WANG Xi-fan, DU Zheng-chun. Survey of Power Systems Voltage Stability Study[J]. Electric Power Automation Equipment, 2005, 25(2): 1-9.

[4] 苏永春, 程时杰, 文劲宇, 等. 电力系统电压稳定性及其研究现状（一）[J]. 电力自动化设备, 2006, 26(6): 97-101.
SU Yong-chun, CHENG Shi-jie, WEN Jin-yu, et al. Power System Voltage Stability and Its Present Investigation (I)[J]. Electric Power Automation Equipment, 2006, 26(6): 97-101.

[5] 苏永春, 程时杰, 文劲宇, 等. 电力系统电压稳定性及其研究现状（二）[J]. 电力自动化设备, 2006,26(1): 97-100.
SU Yong-chun, CHENG Shi-jie, WEN Jin-yu, et al. Power System Voltage Stability and Its Present Investigation (II)[J]. Electric Power Automation Equipment, 2006, 26(7): 97-100.

[6] Morison G K, Gao B. Voltage Stability Analysis Using Static and Dynamic Approaches[J]. IEEE Trans on Power Systems, 1993, 8(3): 589-597.

[7] 段献忠, 何仰赞, 陈德树. 电压崩溃机理探讨[J]. 电力系统及其自动化学报, 1991, 3(2):1-6.
DUAN Xian-zhong, HE Yang-zan, CHEN De-shu. The Research for Voltage Collapse Mechanism[J]. Proceedings of the Electric Power System and Automation, 1991, 3(2):1-6.

[8] van Cutsem T.Voltage Instability:Phenomena, Countermeasures, and Analysis Methods[J]. Proceedings of the IEEE, 2000, 88(2): 208-227.

[9] VU K T, LIU Chen-ching, Taylor C W, et al. Voltage Instability: Mechanisms and Control Strategies[J]. Proceedings of the IEEE, 1995, 83(11): 1442-1455.

[10] Taylor C W. Power System Voltage Stability [M]. New York McGraw-Hill, 1994.

[11] 张琳. 电力系统静态电压安全评估[D]. 南宁:广西大学, 2005.
ZHANG Lin. Static Voltage Security Assessment of Power Systems[D]. Nanning: Guangxi University, 2005.

[12] 罗玉孙, 徐泰山, 许剑冰, 等. Windows 98/NT下的FASTEST—NARI暂态稳定分析软件包[J]. 电力系统自动化, 1999, 23(18):36-38.
LUO Yu-sun, XU Tai-shan, XU Jian-bing, et al. FASTEST-NARI Transient Stability Analysis Software Package in Windows98/NT[J]. Automation of Electric Power Systems, 1999, 23(18):36-38.

[13] Gao B, Morison G K, Kundur P. Voltage Stability Evaluation Using Modal Analysis[J]. Trans on Power Systems, 1992, 7(4):1529-1542.

收稿日期：2007-02-09；　修回日期：2007-03-31

作者简介：
孙　静（1975-），女，博士，主要从事混杂电力系统的综合集成建模与智能优化控制及电力系统稳定性分析方面的研究工作; E-mail:speez@126.com
张　斌（1976-），男，硕士，从事电网调度、电能质量分析及电压无功控制的研究工作;
杜明星（1975-），女，大专，助理工程师，长期从事变电运行工作。

（上接第 34 页　continued from page 34）

参数地址、选择合适的功能码并且注意特殊应用功能的实现等方面问题，就可以在电力系统中更好的使用 Modbus 协议，从而使产品的互操做性更好，更具有市场竞争力。

## 参考文献

[1] GB/Z 19582,1-2004 基于 Modbus 协议的工业自动化网络规范 第 1 部分：Modbus 应用协议[S].
GB/Z 19582.1-2004,Modbus Industrial Automation Network Specification Part 1: Modbus Application Protocol[S].

[2] GB/Z 19582.2-2004,基于 Modbus 协议的工业自动化网络规范,第 2 部分：Modbus 协议在串行链路上的实现指南[S].
GB/Z 19582.2-2004,Modbus Industrial Automation Network Specification Part 2: Modbus Protocol Implementation Guide Over Serial Link[S].

[3] GB/Z 19582.3-2004,基于 Modbus 协议的工业自动化网络规范,第 3 部分：Modbus 协议在 TCP/IP 上的实现指南[S].
GB/Z 19582.3-2004 Modbus Industrial Automation Network Specification Part 3: Modbus Protocol Implementation Guide Over TCP/IP[S].

[4] 贺春，任春梅，张冉. MODBUS 协议在电动机保护装置中的应用[J]. 继电器，2006，34（12）：73-76.
HE Chun, REN Chun-mei, ZHANG Ran.Application of MODBUS Protocal in Motor Protection Equipment[J].Relay, 2006，34（12）：73-76.

收稿日期：2007-01-04；　修回日期：2007-05-17

作者简介：
张海源（1973-），男，硕士，主要研究方向为电力系统电气工程、通信规约及规约测试;
任春梅（1980-），女，本科，主要研究方向为电力系统规约测试和系统测试; E-mail:chunmeir@ncqtr.com
张　冉（1982-），男，本科，主要研究方向为电力系统规约测试和系统测试。