Modbus协议在电动机保护装置中的应用

贺春, 任春梅, 张冉
(国家继电器质量监督检验中心,河南 许昌 461000)

摘要: 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,这样才能开发出满足电力系统需要的产品,从而使产品更具有市场竞争力,从实际使用的角度出发,全面地分析了电动机保护通信的过程和数据,提出一种既符合 Modbus规约、又符合电力系统习惯的使用方法。

关键词: Modbus; 通信规约; 电动机保护

中图分类号: TM73; TM764; TM77 **文献标识码**: B **文章编号**: 1003-4897(2006)12-0073-04

0 引言

低压电动机保护装置大量使用 Modbus协议作为信息交换的接口,自诞生以来,Modbus在工业控制领域大量得到使用,国际 Modbus组织和 IEC TC65标准化委员会也准备将其作为国际标准正式发布,我们国家 TC124(IEC TC65对口单位)标准化委员会也于 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,通过测试发现了许多规约应用中存在的问题,为了更好地推广和使用 Modbus规约,本文从检测实践入手,有针对性地论述在电动机保护中使用 Modbus规约应该注意的问题,使 Modbus规约成为工业控制领域信息交换的有力工具。

1 Modbus协议介绍

Modbus协议是 ISO/OSI模型第 7层上的应用层报文传输协议,它在连接至不同类型总线或网络的设备之间提供客户机/服务器通信。

从 1979年开始,Modbus作为工业串行链路的事实标准,使成千上万的自动化设备能够保持通信。目前,对简单实用的 Modbus结构的支持仍在不断增长,互联网用户能够使用 TCP/IP栈上的保留系统端口 502访问 Modbus。

Modbus是一个请求/应答协议,并且提供功能码规定的服务。Modbus功能码是 Modbus请求/应答 PDU的元素。

目前,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;

③Modbus PLUS,一种高速令牌传递网络。

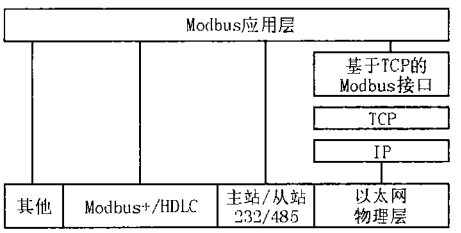

图 1 基于 TCP/IP的 Modbus协议栈

Fig 1 Modbus communication stack based on TCP/IP

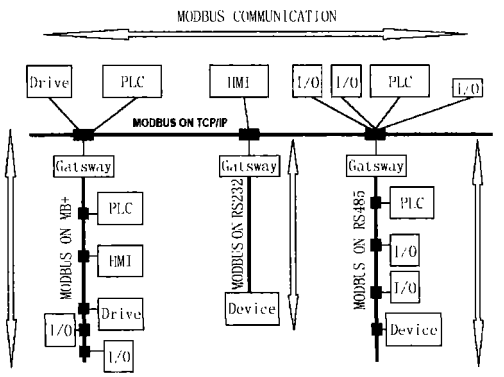

图 2 Modbus网络结构示例

Fig 2 Example of Modbus network architecture

2 电动机保护信息及功能分析

2.1 电动机保护信息分析

电动机保护信息按照访问类型可以分为读写参数和只读参数两种。

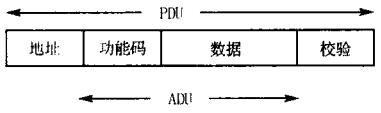

图 3 基本 Modbus帧

Fig 3 General Modbus frame

2.1.1 电动机保护只读参数分析

电动机保护只读参数一般有遥信量、遥测量、启动信息、故障信息 (SOE)、装置时间以及装置自身信息等 (如表 1所示)。

表 1 只读参数表

Tab. 1 Read only parameters

参数名称	内容
遥信量	开关量输入状态
遥测量	A、B、C相电流,零序电流,A、B、C相电压,负荷百分比,累计运行时间,不平衡度,有功功率,无功功率,功率因数以及频率
启动信息	起动时间,启动类型,A、B、C相最大电流
故障信息 (SOE)	故障类型,故障不平衡度,故障时间,故障时相应的值 (A、B、C相电流,零序电流等)
装置自身信息	装置型号,软件版本号,运行指示状态

2.1.2 电动机保护读写参数分析

电动机保护读写参数一般有装置定值、装置时间、通信参数以及线圈状态 (如表 2所示)。

表 2 读写参数表

Tab. 2 Read-write parameters

参数名称	内容
线圈状态	继电器输出状态
装置定值	A、B、C三相电压倍率,A、B、C三相电流倍率,合闸输出允许,分闸输出允许,速断输出允许,限时输出允许,零序输出允许,过压输出允许,欠压输出允许,过频输出允许,欠频输出允许,PT断线检测允许,重合闸允许,开出量形式选择,A、B、C三相速断保护参数,A、B、C三相限时保护参数,A、B、C三相限时时间,A、B、C相定时保护参数,A、B、C相定时保护时间,零序过流保护参数,零序过流保护时间,A、B、C相过电压保护参数,A、B、C相过电压保护时间,A、B、C相欠电压保护参数、A、B、C相欠电压保护参数,A、BC相欠电压保护时间、过频保护参数、过频保护时间、欠频保护参数、欠频保护时间以及重合闸时间
装置时间	年、月、日、时、分、秒
通信参数	子站地址、通信传输速率以及奇偶校验方式

2.2 电动机保护功能分析

电动机保护一般具有的功能有读遥信量功能,读模拟量功能,读起动数据功能,读定值功能,读故障信息,读装置 ID功能,对时功能,修改定值功能,控制功能,复位功能等。

对电动机保护功能的分析是为了更好地将应用功能与 Modbus规约的功能码进行合适的映射,从而实现设备之间良好的互操作性。

一般来说,要实现设备之间应用功能上良好的互操作,需要设备之间使用相同的语法和语义,但是 Modbus规约本身是一个面向存储器 (寄存器)的规约,如果要完成电力系统所需的应用功能,需要在 Modbus规约的基础上,约定双方通信的过程,例如电力系统控制中使用的选择 - 控制过程,不同的企业在实现这一过程时使用的方法不同,就可能影响设备之间的互操作。我们将在后续文章中深入剖析这个问题。

3 使用方法

3.1 不同功能使用的功能码

目前许多厂家对应用功能进行了一个简单的映射,能够满足基本应用的需要,表 3是对常用功能映射的一个总结。

表 3 应用功能与功能码对照表

Tab. 3 Relationship between application function and function code

参数类型	功能	功能码 (十进制)
只读参数	读遥信量功能	02
	读模拟量功能	04
	读启动信息功能	04
	读故障信息功能	04
	读装置 ID功能	17
读写参数	写线圈状态功能	05
	读装置定值功能	03
	读装置时间功能	03
	读线圈状态功能	01
	读通信信息功能	04
	写装置定值功能	06/16
	写装置时间功能	06/16
	写通信信息功能	06/16

3.2 功能码的应用

3.2.1 功能码 01和功能码 02的应用

Fun01和 Fun02都是读位状态,但是 fun01读取读写参数,例如线圈状态、继电器状态等; fun02读取只读参数,例如开关量输入量等。

Fun01和 fun02在应用时都需注意,子站在响应时应该每一个离散量按每位一个离散量状态进行打包,状态被表示成 1 =ON和 0 =OFF,每位在打包时应该按照从低位到高位的顺序排列。如果返回的离散量数量不是 8的倍数,将零填充最后字节中的剩

余位(一直到字节的高位端)。

3.2.2 fun03和 fun04的应用

Fun03和 fun04都是读寄存器值,但是 fun03读保持寄存器即参数类型为读写参数,例如装置定值,装置时间等;fun04读输入寄存器即参数类型为只读参数,例如模拟量、遥信量,故障信息(SOE)等。

Fun03和 fun04在应用时需注意,子站在响应报文中的寄存器数据打包成每个寄存器有两个字节,对于每一个寄存器,第一个字节为高位字节,第二个字节为低位字节。特别注意的是读取 SOE,因为 SOE包含的信息比较多,在使用 fun04读取 SOE时,根据需要将 SOE包含的不同信息分别分配寄存器地址,保证寄存器数据打包成每一个寄存器打包成两个字节。

3.2.3 fun05的应用

Fun05写单个线圈时,请求帧数据域中的常数 FF00H请求线圈状态为 ON,0000H请求状态为 OFF,其他所有值均为非法的,并且对线圈不起作用。

Fun15可以用来写多个线圈状态,但是根据电力系统的特点一般不使用 fun15。

3.2.4 fun06和 fun16

Fun06和 fun16都是写寄存器值,但是 fun06是写单个寄存器值,fun16是写多个寄存器值。Fun06和 fun16在写寄存器值时,将数据打包成每个寄存器两个字节。

3.2.5 fun17

Fun17读取装置 ID、当前状态以及附加信息,其中装置 ID和附加信息与特定装置有关。

4 常见问题分析

4.1 常见问题总结

Modbus作为工业串行链路的事实标准,Modbus使成千上万的自动化设备能够通信。目前,对简单而精致的 Modbus结构的支持仍在增长,但是使用者在应用 Modbus协议时,还会出现一些比较普遍的问题,现将问题总结如下。

1) 主站用广播模式(广播地址为 0)向子站发送请求,子站进行响应,且响应的子站地址为 FEH。

2) 在串行链路 Modbus协议 RTU传输模式下,主站在附加 CRC差错校验时,高字节在前,低字节在后;当主站发送的帧 CRC校验错误时,子站用异常码 04进行异常响应。

3) 主站利用 fun01读取线圈状态,子站对主站读取的线圈起始地址和线圈数量不进行判断,即无论主站请求的起始地址和线圈数量是什么,子站的响应都相同。

4) 主站利用 fun02读取离散量输入状态,当主站读取的离散量输入数量超出子站允许的范围时,子站用异常码 02异常响应;当主站读取的离散量输入数量为 0时,子站正常响应并且响应报文中字节计数为 1。

5) 主站利用功能码 03读取保持寄存器值,当主站读取的寄存器数量超出子站规定的范围时,子站用异常码 02异常响应;当主站读取的寄存器数量为 0时,子站正常响应,并且响应报文中的字节计数为 10;当主站读取的寄存器起始地址无效,子站响应帧的格式不正确。

6) 主站利用功能码 04读取输入寄存器值,当主站读取的寄存器数量超出子站允许的范围时,子站用异常码 02异常响应;当主站读取的寄存器数量为 0时,子站不响应。

7) 主站利用功能码 04读取 SOE数据,子站在响应报文中将一个寄存器数据打包成 18个字节。

8) 主站利用功能码 05发送控制命令,当子站处于非远程控制模式时,子站正常响应,但是子站实际上并没有动作;主站对只读地址进行写操作,子站正常响应。

9) 主站利用功能码 06写寄存器值,当主站写入的寄存器值超出子站允许的范围时,子站正常响应,但是子站实际值并没有修改。当主站写入的寄存器值超出子站允许的范围时,子站正常响应,并进行修改,这样由于子站的一些参数是无效值,造成子站在启动以及采样方面出现了问题。

10) 主站利用功能码 16写多个寄存器,当主站写入的寄存器数量或字节计数无效时,子站用异常码 02异常响应;当主站写入的字节计数不等于寄存器数量的 2倍时,子站正常响应。

11) 主站利用功能码 16修改子站时间,当主站写入的时间超出子站允许范围时,子站用异常码 03异常响应,但是子站时间已经修改。

12) 一些使用者为了简便,不区分读写参数和只读参数,用功能码 03和功能码 04都可以进行读取。

4.2 建议

总结以上出现的问题可以分为三个方面:广播命令、CRC校验以及 Modbus异常响应。下面针对以上问题提出一些建议和意见。

1) 对于主站的广播请求子站不进行响应。

2) 在串行链路 Modbus协议 RTU传输模式下,主站附加 CRC校验时应该低字节在前高字节在后;当主站发送的帧 CRC校验错误时,子站将该帧丢弃。

3) 异常响应

如果子站接收到无通信错误的请求但是不能处理这个请求时,子站将返回一个异常响应,通知主站错误的实际情况。

异常响应的报文有两个与正常响应不同的域:

功能码域:在正常响应中,子站在响应的功能码域复制原始请求的功能码。在异常响应中,子站设置功能码的 MSB为 1。这使得异常响应中的功能码值比正常响应中的功能码值高 80 H。

通过设置功能码的 MSB,主站的应用程序能够识别异常响应,并且能够检测异常码的数据域。

数据域:在正常的响应中,子站可以在数据域中返回数据或统计值(请求中要求的任何信息)。在异常响应中,子站在数据域中返回异常码。这定义了产生异常的子站状态。异常码的使用见表格 4。

表 4 异常响应码的使用

Tab. 4 Usage of exception code

Modbus异常码		
代码	名称	含义
01	非法功能	从站接收到的功能码是不支持的功能码
02	非法数据地址	从站接收到的数据地址是不允许的地址。如果起始地址 +请求的数量超出允许的范围,应该用异常码 02响应。
03	非法数据域	从站接收到的数据域中包含不允许的数据,例如线圈和寄存器数据不在允许的范围内
04	从站设备故障	从站在试图执行主站请求的操作时,产生不可恢复的差错

5 结语

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,这样才能开发出满足电力系统需要的产品,从而使产品更具有市场竞争力。

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 I: 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 II: 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 III: Modbus Protocol Implementation Guide over TCP/IP[S].

收稿日期: 2006-01-04; **修回日期**: 2006-02-15

作者简介:

贺 春(1973 -),硕士,主要研究方向为电力系统自动化、通信规约及规约测试;E-mail: Hechun@ncqtr.com

任春梅(1980 -),本科,主要研究方向为电力系统规约测试和系统测试;

张 冉(1982 -),本科,主要研究方向为电力系统规约测试和系统测试。

Application of Modbus protocol in motor protection equipment

HE Chun, REN Chun-mei, ZHANG Ran

(National Center for Quality Supervision & Testing of Relay & Protection Equipment, Xuchang 461000, China)

Abstract: As a common communication protocol in industrial automation field, the Modbus protocol has its great impact. But due to the particularity and special conventions of implementation, it's needed that the characteristics of Modbus be combined with power system convention so that the products that meeting demands of power system could be successfully developed. The paper is based on the point view of actual application, and it analyzes the communication process and data of motor protection comprehensively and finally puts forward a solution considering both the Modbus protocol and power system conventions.

Key words: Modbus; communication protocol; motor protection