第 19 卷第 1 期　　华 东 交 通 大 学 学 报　　Vol. 19 No. 1
2002 年 3 月　　Journal of East China Jiaotong University　　Mar. 2002

文章编号：1005－0523（2002）01－0017－04

基于 PLC 的变电站 SCADA 系统的研究

刘子英[1]，陈剑云[1]，焦在滨[2]

（1. 华东交通大学 电气与信息工程学院，江西 南昌 330013；2. 西南交通大学 电气工程学院，成都 610031）

摘要：提出了基于 PLC 的变电站 SCADA 系统的硬件结构图. 结合 S7－200 系列 PLC 的特点，制定了通信规约，画出了 PLC 的主程序流程图，并给出了部分调试结果.

关　键　词：PLC；数据采集；监控；通信

中图分类号：TM769　　文献标识码：A

0　引　　言

SCADA（Supervisor Control And Data Acquisition）系统，即监测监控及数据采集系统是实现变电站综合自动化基本功能的系统，它的主要任务是采集和管理各实时生产数据，对生产过程进行监视和控制.

目前，大多数 SCADA 系统的数据采集与处理部分一般采用单片机自制成各种总线方式的智能化模块，但这种方式可靠性和抗干扰性都难以得到有效保证，而且开发周期一般比较长，程序复杂.

PLC 是以单片机为核心，专门用于工业过程自动化控制的新型智能型产品，有着极高的可靠性和稳定性，特别适用于分布式系统，完成现场设备的数据采集和控制功能以及与上位机的通信功能，这对于变电站自动化系统的实现，无疑是十分理想的选择. 基于此考虑，本系统选用 PLC 作为现场主要监测设备以实现变电站的自动化.

1　系统结构

本系统在硬件上采用分层分布式结构，如图 1 所示. 在整个系统中，最上层由以太网连接了主、备前置机和系统服务器，主、备前置机同时挂接在底层现场总线上，互为热备分，负责搜集底层设备的数据，完成一个实时网关的功能. 第二层设备层部分选用了 PLC 来完成变电站的一次设备的数据采集、控制以及和上位机的通信等功能.

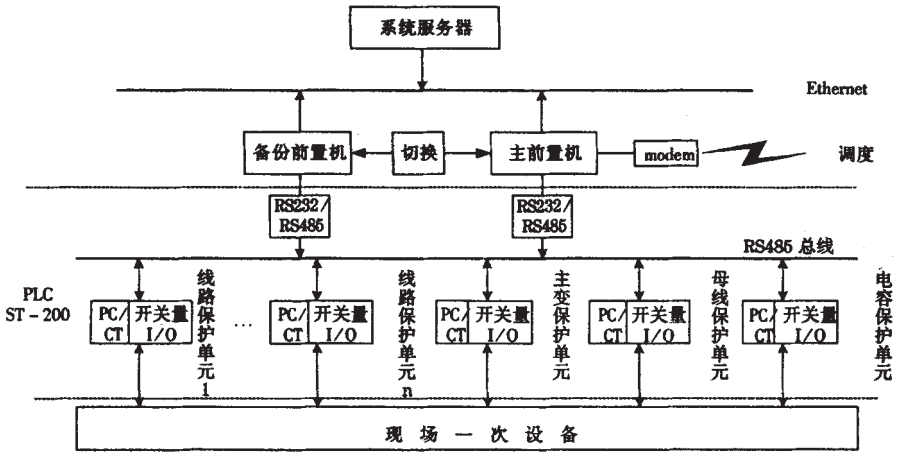

图 1　基于 PLC 的变电站 SCADA 系统硬件结构图

本系统所使用的 PLC 为西门子公司生产的 S7－200系列. 该系列 PLC 采用模块化设

收稿日期：2001－07－19

作者简介：刘子英（1964－），女，江西于都人，华东交通大学副教授.

计, 结构简单、集成度高、体积小、速度快、通信灵活方便、性能价格比高.

因此, 可利用 PLC 的模拟量输入点采集母线电压、有功功率、无功功率等信号, 以达到对线路进行遥测的目的; 利用 PLC 的开关量输入点采集站内一次运行方式的断路器、刀闸、接地刀闸位置等信号, 以达到对线路进行遥信的目的; 利用 PLC 的开关量输出点电流的通断控制断路器的合闸、跳闸, 以达到对线路进行遥控的目的, 实现数据采集与控制功能. PLC 如何把所采集的数据传送给上位机 (前置机), 又如何接收上位机的请求和控制命令, 这些都涉及到 PLC 的通信问题.

其主要特点有:

1) STEP—7 具有良好的开发环境, 提供梯形图和语句表两种编程方式.

(2) I/O 扩展能力强, 可使用扩展模块进行 I/O 扩展.

3) 、具有较强的中断能力.

4) 带有高速计数器, 可采集脉冲量.

5) 具有 RS—485 串口, 拥有强大的通信功能.

2 通信规约的制定

2.1 通信方式的选择

基于 SIMATIC S7—200PLC 的硬件结构及特点, 我们认为选择以 RS—485 现场总线作为 PLC 与上位机之间的连接是较好的一种连接方式. 底层 RS—485 总线的通信规约有应答式(Polling) 和循环式(CDT) 两种. 循环式通信规约即将被淘汰, 现在一般采用应答式通信规约, 即上位机依次查询个 PLC 设备, 相应的设备收到查询后给予响应, 送出相应的数据. 因此选用 Polling 方式作为本系统的通信方式.

2.2 通信报文的格式及种类

以 Polling 方式进行通信的规约有标准规约 IEC870 – 5 – 101、西屋规约以及各部门自定义的规约等许多种. 由于现有规约包含的内容多、结构复杂, 并且系统对所定义的某些内容根本用不上, 因此有必要根据实际情况制定本系统的通信规约.

HY—200 微机远动系统中所使用的规约为自定义规约, 该规约具有内容精练、结构简单明了、易于掌握、易于实现等特点. 现场运行情况表明, 该规约数据传输效率高, 是一种较为成熟的规约, 本系统基本上采用了该规约. 采用该规约后, 我们只需对 PLC 编程, 上位机基本上仍可使用原来的程序, 从而省去了对上位机的编程.

在通信中, 数据的传输是以报文的形式进行传输的. 对于接收方而言, 数据是随机的. 为了使接收方能够确定报文的开始, 发送方往往在一帧报文的开始加上群同步码. 本系统在报文头加了两个同步字节 7EH, 以实现群同步.

2.2.1 报文格式

报文的格式如下:

字节 1: PLC 地址

字节 2: 报文功能代码

字节 3: 数据长度(= N, 包括字节 4)

字节 4: 报文类别代码

字节 4 + 1 ~ 4 + N: 数据区

字节 4 + N + 1 ~ 4 + N + 2: CRC 校验码

由于通信既采用了奇偶校验, 又在报文的最后添加了 CRC 校验码, 因此因误码而导致误报、误动作的可能性大大降低, 增加了监控系统的可靠性.

2.2.2 报文类型

报文类型由报文功能代码和报文类别代码共同决定. 报文功能代码分为六种, 它们的代码和表示的功能如下:

类别询问 (05H): 调度端从 PLC 采集某些类型的变化的数据. 当 PLC 收到该报文时作如下处理: 首先查询询问类别有无变化的数据, 若有就组成数据报告报文 (1BH); 若没有就组成确认报文 (06H). 若收到报文不明确或有错就组成否定确认报文(15H).

●类别更新 (0BH): 调度端要求 PLC 报告最新的一个或多个类别的数据. PLC 收到报文后, 不管有无变化的数据标志, 都组成要求数据报告报文 (1BH); 若收到报文不明确就组成否定确认报文 (15H).

●设置时钟 (0CH): 调度端向 PLC 设置时间和日历. PLC 若收到正确报文, 回答确认报文(06H), 否则回答否定确认报文(15H).

●召唤事件记录 (0FH): 调度端要求 PLC 报告最新的事件记录. PLC 收到后组成事件记录报文 (1BH), 报文不明确回答否定确认报文(15H).

●带反送校核遥控 (1EH): 调度端向 PLC 发出遥控命令. PLC 收到后组成校核数据回答报文 (1CH).

●执行遥控命令(0DH)：调度端收到 PLC 的报文(1CH)后，再进一步校核遥控命令数据，发出该报文．PLC 收到后先发出遥控信号，然后回答确认报文(06H)；报文不明确，回答否定确认报文(15H)，且不发任何遥控信号．报文类别代码分六种，它们是遥信(01H)、遥测(02H)、脉冲(04H)、事件(08H)、遥控(10H)和时间(20H)．

3　PLC 的软件设计

主程序主要完成初始化、遥信自处理、通信处理三方面的工作．只有第一次扫描才执行初始化程序．然后进行遥信自处理程序，若有通信要求，则进行通信处理．完成报文接收中断程序、报文解释和执行子程序，否则结束主程序，完成一次扫描工作．其流程图如图 2 所示．

PLC 初始化程序用于完成 PLC 站号的设置、群同步码的设置、通信参数的填写、CRC 表的产生、静止时间线的设定等任务．遥信自处理程序用以捕捉输入点状态的变化．PLC 报文接收是一个相当复杂的过程，当 PLC 的 port0 口检测到有字符送来时，产生接收字符中断，其中断执行的顺序依次为：接收站地址码中断、功能码中断、数据长度中断和报文数据中断．PLC 接收到的报文必须经过解释之后，才能被正确执行；而 PLC 在向主机发送报文之前，必须先将要发送的报文组装起来．PLC 报文发送程序包含类别询问、类别更新、设置时钟、召唤事件记录及遥控等若干子程序．

4　调试结果

我们对所编制的 PLC 程序进行了调试．调试硬件由一台 PC 机、两台 CPU214 型 PLC、扩展模块 EM223 和 EM221 及 PC/PPI 电缆组成．程序在 PC 机上编制，PC 机通过 PC/PPI 电缆与 PLC 的 Port0 口相连，可完成程序向 PLC 的下载，并且还可监视 PLC 中数据缓冲区的内容．实验中，一台 PC 机作为主机，两台 CPU214 型 PLC 作为从机，且从机接有扩展模块，主从机之间通过 RS485 串行总线相连，以实现数据的采集、完成报文的接收、发送过程．

限于篇幅，下面仅以类别更新报文、带返送校核遥控报文和执行遥控命令报文为例来说明调试结果的正确性．

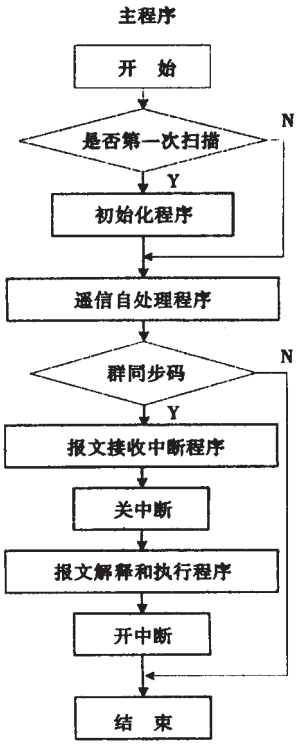

图 2　PLC 主程序流程图

1)　类别更新报文

主机发送类别更新报文，发送站地址为 01H，功能码为 0BH，数据长度为 01H，类别码为 01H；从机 IB0～IB5 当时输入点的状态分别为 10010000(90H)、10001000(88H)、10010100(94H)、10001000(88H)、00100001(21H)、00001010(0AH)．通信完成后，分别读出其数据缓冲区中的内容(十进制)，如表 1 所示：

表 1　类别更新报文

主机发	从机收	从机发	主机收
126	1	126	1
126	11	126	11
1	1	1	7
11	1	11	1
1	176	7	144
1	74	1	136
176		144	148
74		136	136
		148	33
		136	10
		33	202
		10	214
		202	
		214	

主机按要求组装发送报文，表中 126 即为群同步码 7EH，176 和 74 为 CRC 校验码，当从机连续收到两个 7EH 时开始接收报文；若接收报文正确无误，从机根据接收报文的内容组装发送报文，向主

机发送回报. 从表中可看出, 主从机之间均能正确发送和接收报文, 并且从机发送的状态量 IB0 ~ IB5 分别为 144、136、148、136、33 和 10, 经换算, 与从机当时输入点的状态完全一致, 说明从机采集数据正确.

2) 带返送校核遥控报文

主机发送带返送校核遥控报文, 对 01H 号 PLC 输出点的第 2 个字节第 4 位的分闸线圈执行预遥分闸操作, 主从机收发报文的记录内容如表 2 所示:

表 2 带返送校遥控报文

主机发	从机收	从机发	主机收
126	1	126	1
126	30	126	28
1	3	1	3
30	16	28	16
3	2	3	2
16	8	16	8
2	168	2	209
8	239	8	47
168		209	
239		47	

3) 执行遥控命令报文

主机收到从机发来的可以执行遥控命令的回报后, 向从机发送执行遥控命令报文, 从机收到报文后, 执行遥控命令操作, 使第 2 个字节第 4 位输出置 1, 然后向主机发送遥控确认报文. 主从机收发报文的记录内容如表 3 所示:

表 3 执行遥控命令报文主机发从机收从机发

主机发	从机收	从机发	主机收
126	1	126	1
126	13	126	6
1	3	1	1
13	16	6	16
3	2	1	225
16	8	16	133
2	45	225	
8	44	133	
45			
44			

所做试验结果表明, PLC 均能正确接收各种类型报文并产生相应的回报, 且遥控执行命令输出正确, 调试结果比较理想.

参考文献:

[1] 徐国政, 等 . 基于可编程控制器的变电站自动监测系统[J]. 清华大学学报(自然科学版) . 1998, 38(4) : 82—85.

[2] 黄俊辉, 等 . PLC 在电力监控系统中的应用[J]. 微型机与应用 . 1999, 18(1) : 18—20.

[3] 陈剑云 . HY200 微机远动系统研制报告科技文献 [C] . 南昌: 华东交通大学信息与控制工程研究所, 1999.

[4] 西门子公司 . S7 – 200 PLC 用户指南[M]. 1999.

Research of Transformer Substation SCADA System Based on PLC

LIU Zi-ying [1], CHEN Jian-yun[1] , JIAO Zao-bin[2]

(1. School of Electrical and Information Eng., East China Jiaotong Uni., Nanchang 330013;
2. School of Electrical Eng, Southwest Jiaotong Uni. Nanchang 330013, China)

Abstract: The harcture picture of transformer substation SCADA system based on PLC is presented. The communicate stipulations of an agreement is constituted according as the characteristic of S7—200 PLC. The main procedure flow chat is drawn. The part of debugging result is shown.

Key words: PLC ; data acquisition; supervisor control; communication