

# 三菱 Q 系列 PLC 串口自由通讯方法的探究

范蟠果, 王超然, 张红伟, 刘经纬

(西北工业大学 自动化学院, 西安 710129)

**摘要:** 多种工业控制场合需要使用智能设备, 并以串行通信将数据发送至上位机; 三菱 Q 系列 PLC 无顺序通信方法仅支持接收“固定长度”与“变长度有固定结尾”两种数据对象, 与发送“变长度无固定结尾”数据的智能设备不能妥善匹配; 为此设计了一种 Q 系列 PLC 串口自由通信方法, 该方法采用顺序控制程序实现了“变长度无固定结尾”数据接收、异常数据消除与通信模块故障自恢复, 具有破除通信模块设定局限、可自行定义通信协议的特点; 经实验其可同时支持多种智能设备, 具有良好的适应性和通用性。

**关键词:** Q 系列 PLC; 串口; 自由通信

## Research on Mitsubishi Q Series PLC Serial Port Free Communication Method

Fan Panguo, Wang Chaoran, Zhang Hongwei, Liu Jingwei

(School of Automation, Northwestern Polytechnical University, Xi'an 710129, China)

**Abstract:** The intelligent device which transmits data to the upper computer by serial communication is needed in many industrial control occasions. When using the nonprocedure protocol Mitsubishi Q-series PLC which only supports receiving “fixed length” and “variable length fixed end” data objects, which can not match with the intelligent devices which send “variable length without fixed end” data properly. For this reason, a free serial communication method of Q series PLC is designed. By using sequence control program, this method realizes “variable length without fixed end” data reception, abnormal data elimination and self-recovery of communication module. Such method has the characteristics of breaking the limitation of communication module itself and making self-defining communication protocol available. Experiments show that it can support multiple intelligent devices at the same time and has good adaptability and versatility.

**Keywords:** Q series PLC; serial communication; free communication

## 0 引言

工业用 PLC 环境适应性强, 可靠性高, 对工业环境中常见的电磁干扰<sup>[1]</sup>、潮湿状态具有很好的耐受力, 对自身的各类异常具备良好的自我检测能力<sup>[2]</sup>。工业用 PLC 大多能够加装各类扩展模块, 以支持丰富多样的用户需求<sup>[3]</sup>, 三菱 Q 系列 PLC 是其中的典型代表<sup>[4]</sup>。

三菱 Q 系列 PLC 主要使用 QJ71C24 系列通信模块与外部智能设备通信<sup>[5]</sup>。该系列模块可选用无顺序协议通过自定格式报文与自定控制步骤实现通信功能。无顺序协议在接收方式上分为用于接收固定长度数据的“接收结束数据数”与接收可变长度且具有固定结尾数据的“接收结束代码”两种<sup>[6]</sup>。

智能设备在工业应用中具有运行效率高、故障诊断能力强的特点<sup>[7]</sup>。但其连续通信时所发送报文的长度与报文结尾可能不固定, 设备与 Q 系列 PLC 通信协议不匹配现象时有发生。再者, 智能设备使用的通信连接接口各异, 对于三线式 RS-232 通信及两线式 RS-485 通信, 通信模块

的线路连接与数据处理方法并不直接。因此开拓一种使 Q 系列 PLC 能够接收变长度无固定结尾数据并兼容多种通信协议的自由通信方法, 对于扩展 Q 系列 PLC 对智能设备的支持范围、节省用户使用成本具有重要意义。如无特别标注, 本文所指通信模块特指 QJ71C24N。

## 1 通信连接扩展

智能设备的通信端口各异, 通信模块原生支持标准 DB9 式 RS-232 以及螺栓端子排式 RS-422 串行通信接口, 于此硬件基础上可扩展出三线式 RS-232 (TXD、RXD、GND) 与两线式 RS-485 (A、B) 串行通信的接口线路连接与配套数据处理方式。

对于三线式 RS-232 通信智能设备。由于通信模块于通信过程中持续对 RS-232 端口的 RTS/CTS、DTR/DSR 端子进行检测, 故三线式连接时不可简单将 TXD、RXD、GND 端子直接引出。经实验, 可通过图 1 方式接线绕过端子检测并建立三线式 RS-232 串口通信。显然的, 依此接线时不可进行 DTR/DSR 控制, 但可进行 DC 代码控制。为了对抗可能影响通信的较大外部噪声, 应利用连接电缆的屏蔽层将设备与通信模块的 FG 端子连接, 并且将 RXD、TXD 信号连接线分别与 GND 双绞连接<sup>[6]</sup>。

收稿日期: 2019-06-26; 修回日期: 2019-08-08。

作者简介: 范蟠果(1960-), 男, 陕西西安人, 硕士, 副教授, 主要从事飞机测试系统方向的研究。

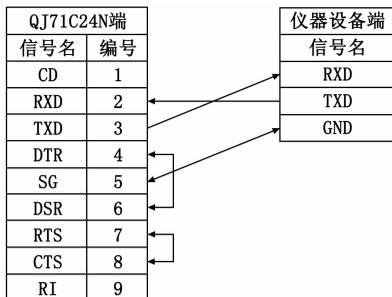


图 1 三线式 RS-232 串口通信链接

对于两线式 RS-485 通信设备。通信模块的 RS-422 与 RS-485 共用接口，使用两线制 RS-485 通信时应如图 2 接线，终端电阻为  $110\ \Omega\ 0.5\ W^{[6]}$ 。然而受模块限制，RS-422 与 RS-485 所在通信通道无法被设定为半双工模式，这意味着使用图 2 接线方式时，模块发出的数据必然会被自身所接收，由此应采取如下数据处理方式：使用固定结尾接收方式时，需去除前  $n$  位， $n$  为发送报文长度。而使用固定接收长度方式时，需要将原指定接收长度延长  $n$  位长度，以包容发送报文，再于接收报文处理时将报文前  $n$  位去除。类似于 232 接口，可连接电缆的屏蔽层与模块 FG 端子应对外部噪声<sup>[6]</sup>。

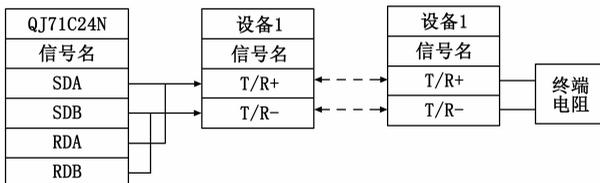


图 2 两线式 RS-485 串口接线

## 2 通信顺序控制程序

通信模块默认支持 3 大通信协议：MELSEC 通信协议、无顺序协议、双向协议。MELSEC 通信协议是由目标通信设备主动对 CPU 的软元件数据、程序进行读写；无顺序协议通信是由通信模块以任意用户定义的报文格式及传送控制步骤对任意数据发送接收；双向协议为通信双方设备使用“双向协议”报文格式及传送控制步骤实现收发功能的通信方式。智能设备可使用的通信方式出厂即已固定，因此通信方式上只有无顺序协议通信可选。

无顺序协议通信原生支持“接收结束数据数”与“接收结束代码”两种数据接收方式。“接收结束数据数”方式即当所接收报文达到指定接收长度后认为报文完结，用于接收固定长度数据。“接收结束代码”方式即当接收到指定结束代码时认为报文完结，用于接收变长度有固定结尾的数据<sup>[6]</sup>。

若用户使用的智能设备通信方式与智能模块配合良好（长度始终固定或存在固定结尾），此时使用模块的自动刷新功能不失为一种方便可靠的通信实现方法。反之应使用顺控程序配合无顺序协议通信以求最大的兼容范围及使用

灵活性。

顺控程序的一般过程为：首先保证通信前线路净空。发送数据时，将 PLC 中准备好的通信数据存储至某一系列连续软元件组，调用发送指令，数据由模块发出。接收数据时，依据接收读取请求信号调用数据接收指令，将缓冲存储区内数据存储至目标连续软元件组。为保证半双工接口线路净空可使用应答式通信，即 PLC 向目标设备发出通信要求后于一定时间范围内等待目标回文，若通信错误或超时则重发通信要求重试通信，通信要求多次重发后仍没有正确回文则认为通信失败，置位相应标志位。

常用收发控制指令为 G.INPUT 与 G.OUTPUT<sup>[8]</sup>。数据发送指令 G.OUTPUT 在结构化梯形图模式中构建方式如图 3 所示。其中参数数组包括发送通道指定（1 或 2）、发送数据长度指定、由系统赋值的发送结果三项。发送许可置位后，指令将以缓存软元件为起始的连续指定个数的软元件内的数据发出。结束数组由指令是否结束与结束是否正常两个标志位组成。此外发送指令还有上升沿触发的 GP.OUTPUT 形式。

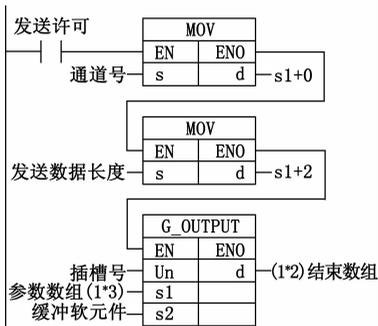


图 3 G.OUTPUT

类似地，数据接收指令 G.INPUT 构建方式如图 4 所示。特别地，参数数组包括接收通道指定、接收数据允许数指定、由系统赋值的接收结果、接收数据计数值共 4 项。其中接收数据计数值用于统计当前缓冲存储器中已接收到的数据位数，接收数据允许数用于指定缓存软元件中可存储的接收数据的长度。连续的数据由串口输入 PLC 后将持续存入模块的操作系统区域，模块依据“接收结束代码”或“接收结束数据数”方式对操作系统区域内数据进行接收完成判断<sup>[6]</sup>。若接收完成则接收读取请求（X3/X4）置位，实际接收数据由操作系统区域复制存储于 601H/A01H 开始的缓冲存储器地址中，接收数据计数值保存于地址 600H/A00H。顺控程序调用 G.INPUT 则是将缓冲存储器中的数据赋值给用户于 G.INPUT 指令中指定的接收数据计数值与接收数据存储软元件，并返回接收状态。一个方便的顺控程序接收方式是将“接收许可”直接指定为 X3/X4，如此当有接收结尾被确认则直接可将指定软元件赋值。

显然地，若接收到的报文内容异常，即“接收结束代码”确认方式中结束代码丢失或改变，或“接收数据数”方式中数据丢失或增添任何一个单位数据，则接收结尾失

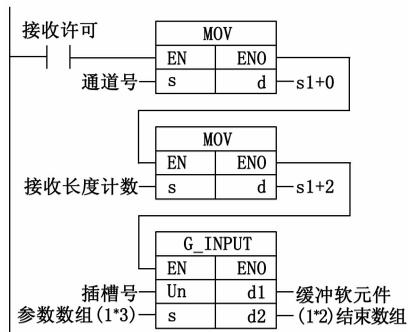


图 4 G. INPUT

效。理想情况下, 使用“接收结束代码”方式时本次接收数据会同下次的接收数据发生单次“拼接”, 而使用“接收数据数”方式会致使往后的所有数据在发生“拼接”的同时均前后移动出现“错位”, 即连续发生“错位拼接”。对于单次“拼接”情况可由报文中的校验位将个别异常报文予以滤除。对于连续“错位拼接”情况应舍弃干扰接收的操作系统区域内的残余数据, 并给顺控程序予一个开关量提示。模块提供一个专用指令 ZP. CSET<sup>[8]</sup>, 构建方式如图 5 所示。参数数组包括两个固定项: 执行类型 (指定为 0)、请求类型 (指定为 4), 一项系统赋值的结束状态, 以及其他 108 项系统用软元件。若某一通道正在执行 OUTPUT、INPUT、CSET 指令时不可使用 CSET 指令, 否则将触发“专用指令同时执行错误” (错误代码 0x7FF0, 该错误将使模块报故, 顺控程序停止), 正在执行 CSET 指令时调用 INPUT 指令不会出现该错误。需要注意的是, 指令梯形图中插槽号软元件为字符串形, 如 0 槽应为“U00”。

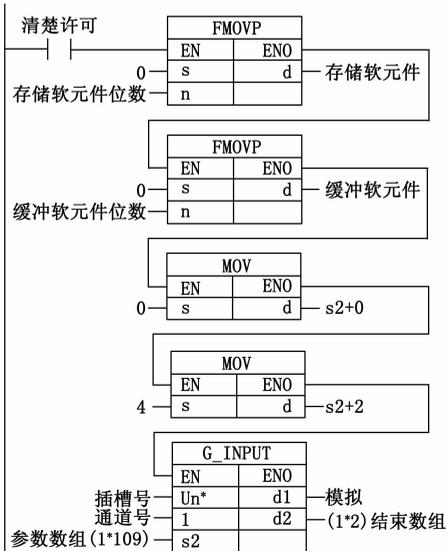


图 5 ZP. CSET

### 3 变长度无固定结尾通信实现

通信模块对于变长度无固定结尾报文并未提供直接接收方法。这里提出一种改良自“接收结束数据数”接收方

式, 可接收变长度无固定结尾报文的接收方法, 其大体思路如下:

智能设备大多可采取应答式的收发方式, 主机发送通信要求后智能设备产生的正确回文的数据位数是一定的, 连续的通信可被拆分为若干次针对预估正确回文长度的固定长度报文通信。

虽然模块“接收结束数据数”接收方式的结束数据数设定在初始化时即已被烧写入模块, 但该参数还被保存于一个缓冲存储器中, 可通过缓冲存储器访问指令将其修改。

具体操作流程为: 将智能模块以“接收结束数据数”接收方式初始化, 接收结束代码设定为 0xFFFF 即无接收结束代码。主机发送通信要求前调用缓冲存储器数据写入指令将存有接收结束数据数的缓冲存储器 0xA4/0x144 置为正确回文的数据位数, 并启动一个定时器。通信顺利情况下智能设备回文正确地被通信模块以固定长度报文接收, 在下次通信要求发送前再次修改接收结束数据数至新的正确回文长度, 重复该流程。反之异常情况有两种: 一种是通信模块接收到指定长度报文, 但原始回文比设定长度更长或者所收到报文与原始回文内容不同而长度相同, 这种情况可通过回文的校验位将异常报文排除, 之后由主机重新发送通信要求, 再次通信。另一种异常情况是主机一直没有收到回文或收到的回文长度小于指定长度, 此时“接收读取请求”无法置位, 这类异常可通过设定报文长度时启动的定时器排除, 即于定时时间内未完成通信要求则主机重发通信要求, 再次要求通信。多次超时异常可作为智能设备离线的判断依据。

### 4 通信模块故障后自恢复

通信过程中模块可能发生溢出出错、成帧出错、奇偶性出错等通信模块故障, 通信模块“ERR”灯被点亮, 它们将使通信模块完全停止工作。这类故障于有人值守系统可通过 PLC 的机械复位开关复位解决, 无人值守长时运行系统则需要 PLC 使用顺控程序自行排除故障。系统在调试阶段应尽可能模拟实际使用中的外部电磁条件, 收集与推测可能出现的故障错误代码并制定故障排除方案。

以无顺序协议通信模块 1 通道成帧出错 (错误代码 7F68) 的排除为例: 模块故障, ERR 灯亮起, 根据出错端口的不同 X0E/0F 被置位, 这里被置位的为 X0E。从缓冲存储器地址 0x201/202 中读取亮灯原因, 0x201 此时 b1 即 SIO 位置位, 0X202 的 b15 即 CH1 ERR 被置位。以此跳转至地址 0X258 通道 1 接收出错错误码存储缓冲存储器中获取错误代码。其他错误对应的缓冲存储器还有 0x268 通道 2 接收出错、0x203 开关设置与模式切换出错、0x257/267 数据发送出错等。以保存的错误代码为索引执行相关处理步骤, 这里强制执行 G. INPUT 指令将不必要数据舍去并执行 ZP. CSET 指令清空操作系统区域内数据。于出错信息初始化请求区 (地址 0x00/01) 赋值 00FF /C0FF 清除出错代码, 并将线圈出错信息初始化请求 Y0E/0F 置位,

完成故障灭灯，模块故障排除通信重启。

### 5 通信测试实例

如图 6 所示，验证系统由三线式 RS-232 通信下的一台 RW3-3035 冷却机，两线式 RS-485 通信下的数台 D08-8C 温度控制器与数台 AI518P 流量积算仪组成。通信线缆额外由通信模块端子根部接出至测试 PC 串口，测试 PC 通过该线路在 PLC 与智能设备通信时发送若干干扰或模拟异常设备发送错误报文，以检测本通信方法对异常的耐受能力。测试 PC 还通过 PLC 数据线监视当前 PLC 缓冲存储区与相应软元件储值情况，作为测试结果评判依据。

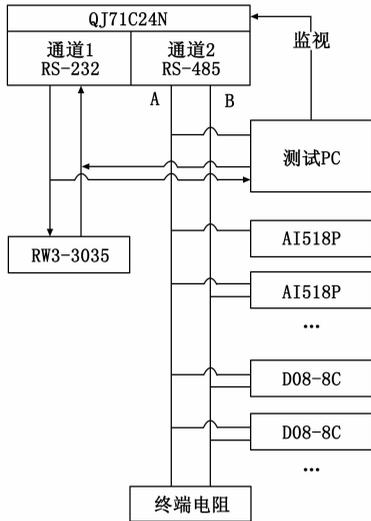


图 6 验证系统

温度控制器使用 AIBUS 通信协议<sup>[9]</sup>，流量积算仪使用自有通信协议，冷却机使用 Modbus 通信协议<sup>[10]</sup>。前两者接入同一 RS-485 端口，采用应答式通信，出厂预设通信报文首字节均为本智能设备地址，且波特率、数据位、停止位相同，这也是他们共线通信的基础。

自由通信方法可实现不同协议下“变长度无固定结尾”数据的接收，即能够共线但使用不同协议的智能设备可与 PLC 在没有固定报文结尾的情况下实现变长度报文通信。PLC 以 AIBUS 通信协议发送“81 81 52 0C 00 00 53 0C”意为要求地址为 81 的温度控制器回报当前设定精度。返回报文“C4 08 B8 0B 64 60 81 00 62 75”报文共 10 字节无固定结尾，校验位“62 75”校验正确，目标参数“81 00”即小数精度 0.01 同时显示减一位，实时温度“C4 08”即 22.44℃，设定温度“B8 0B”即 30.00℃。此时温度控制仪表面画面显示：实时温度 22.4℃（精度 0.1），设定温度 30.00℃，此时智能模块正确完成一次无干扰 10 字节数据接收。PLC 以流量积算仪自有协议发送“02 03 00 02 00 08 E5 FF”意为要求访问地址为 02 的流量积算仪的状态。返回报文“02 03 10 02 01 08 10 03 00 01 13 0F 0F 00 00 00 12 11 80 49 60”，该报文共 21 字节无固定结尾，其中 CRC 校验“49 60”校验正确，瞬时流量“02 01 08 10”即 0.812 L/Min，

累积流量“03 00 01 13 0F 0F”即 3.103 L。流量积算仪面板显示流量 0.812 L/Min，累积流量 3.092 L，智能模块接收 21 字节报文正常。通过以上两次连续收发可证实智能模块此时具备对可共线智能设备使用不同通信协议接收变长度无固定结尾报文的能力。

自由通信方法可实现对于异常数据的滤除：将 PLC 与智能设备间连接断开，由测试 PC 模拟异常智能设备，发送超长、不足长度、错误内容的回文，并使用 GX Works2 监视 PLC 软元件置位情况<sup>[11]</sup>，以此检测通信方法对异常数据的适应性。PLC 发送“01 05 00 18 00 FF 0D 8D”意为对 01 地址流量积算仪流量清零，智能设备发送的正确回文应与 PLC 发送报文相同。测试 PC 回文“01 05 00 18 00 FF 0D”模拟回文缺失字节情况，PLC 于指定时间内未收到足够长度数据，定时器超时，正确认定数据异常。重发流量清零报文，要求重新通信。测试 PC 回文“AA 05 00 18 00 FF 0D”模拟字节错误情况，由监视发现报文 CRC 校验失败，数据异常被正确识别，PLC 再次重发流量清零报文。测试 PC 回文“01 01 05 00 18 00 FF 0D 8D”模拟回文超长情况，此时 PLC 缓存软元件收数据如图 7 所示，超长部分不被接收，且由于已接收部分 CRC 校验失败，此次通信数据异常判定正确。由于连续 3 次接收数据异常，PLC 正确认定智能设备或通信线路失能，对应离线标志位置位。测试 PC 通过监视还发现以上三次通信均由于正确触发数据异常判定而调用过 ZP.CSET 指令，操作系统区域内错误数据按设定被清除，正确消除单次通信失败对往后通信的负面影响。至此可认为智能模块对异常数据报文的适应性良好。

软元件	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0	
D70	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0101
D71	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0005
D72	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0018
D73	0	0	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0DFF
D74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000
D75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0000

图 7 超长回文缓冲软元件监视

自由通信方法具备通信模块故障的自恢复能力：在 PLC 与智能设备通信过程中由测试 PC 强行于线路中发送若干干扰数据，以此引发通信模块故障。由 PLC 错误履历中发现若干次成帧出错、奇偶性出错，但肉眼未见模块 ERR 灯亮起，同时由监视发现通信过程中除少量报文由于异常报文滤除功能出现丢失外继续进行。可推断通信模块曾出现过使模块失能的故障，PLC 执行了错误自恢复程序，故障被顺控程序消除。可见通信方法错误自恢复能力良好，具备长时无人值守工作能力。

### 6 结束语

以上介绍了 Q 系列 PLC 基于 QJ71C24N 通信模块的扩展通信方法，该方法实现了模块的自由通信，拓宽了模块的应用场景，具备“变长度无固定结尾”数据接收、异常数据消除与通信模块故障自恢复能力。

(下转第 178 页)