

1. 首先选用串口调试程序。建议使用多串口调试程序 (MultiCOMWatch)

下载地址: <http://www.onlinedown.net/soft/6287.htm>

<http://www.skycn.com/soft/9280.html>

2、对于三菱 FX 系列的 PLC, 它的密码校验过程是通过明码方式的, 所以可以通过监视通的办法来获得密码。

它的通讯应答过程是这样的, 编程软件与 PLC 联机时, PLC 便将密码发送到编程器 (电脑) 中, 等待输入正确的密码进行校验。

方法: 启动多串口调试程序 (MultiCOMWatch) 打开 Com1 (根据与 PLC 连接的端口决定)。

确定三菱 PLC 型号。根据 PLC 型号选择的多串口调试程序的 文本 中输入对应字符串。(说明 STX=02 ETX=03)

PLC 型号	文本对应字符串	HEX 格式对应字符串
FX2	\STX0700808\ETX6A	02 30 37 30 30 38 30 38 03 36 41 32
FX2N	\STX0300808\ETX66	02 30 33 30 30 38 30 38 03 36 36 32
FX2_EEPROM	\STX0800808\ETX6B	02 30 38 30 30 38 30 38 03 36 42
FXON/FXOX	\STX0800808\ETX6B	02 30 38 30 30 38 30 38 03 36 42
FX1N/FX1X	\STX0800808\ETX6B	02 30 38 30 30 38 30 38 03 36 42 (正确)

A 系列:

发送: A2 07 00 FF 02 05 AE 00 08 C3

接收: 0B 00 FF 02 00 AA 77 55 BB EF CD AB A4 00 密码: ABCDEF

发送: A2 07 00 FF 02 05 AE 00 08 C3

接收: 0B 00 FF 02 00 AA 77 55 BB C1 B1 A1 A4 密码: A1B1C1

分析: 密码为返回字符串中 BB 至 A4 之间的字符, 以每 2 字符为单位, 从右往左读出。

了解了上述字符串后, 可以自己用 VB 或其他的编程语言专门写一个读写密码的程序。

如果你还想更深入了解 PLC 与电脑之间的通讯, 可以用硬件的监视通讯方法来取得整个过程。监视方法可见 <http://gktd.com/dispbbs.asp?boardID=7&ID=11>

3、发送后在接收框中将显示一串字符串, 就是返回的密码, 如果看不出来的话, 将这些字符串拷贝到 HEX 格式中, 发送一次看看。(发送前记得先断开 PLC)。