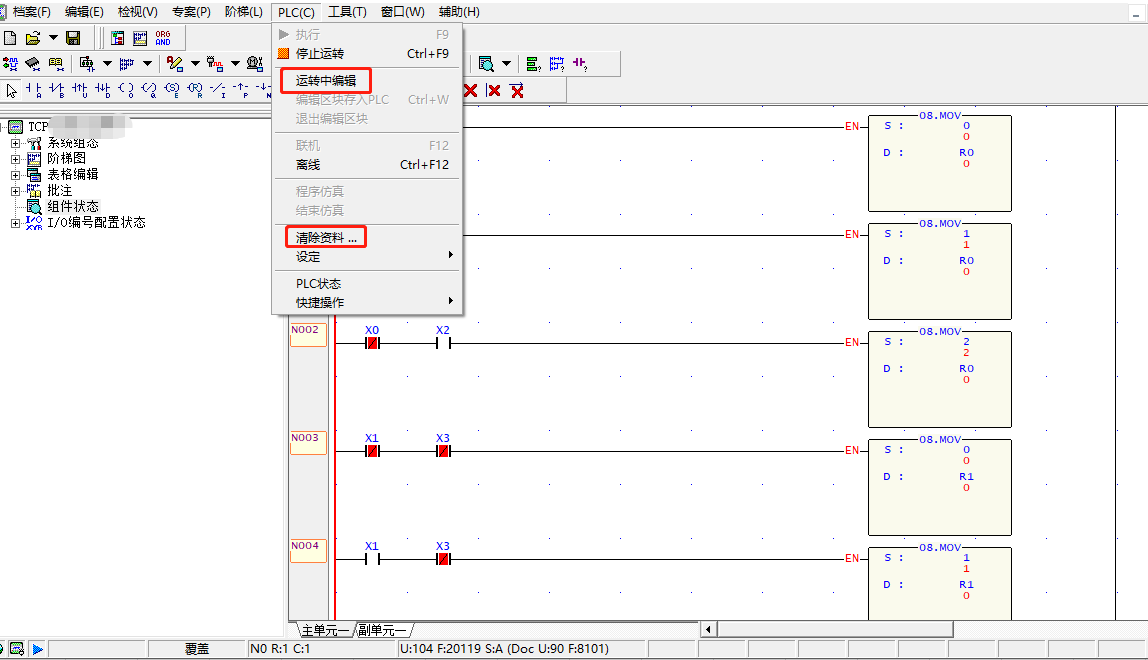
根据对永宏PLC的研究实验，永宏PLC在未设置程序密码的情况下，任何人均可通过其编程软件WinProladder连接其IP地址，进行联机操作，下载修改PLC梯形图信息，清除资料等，如图所示。

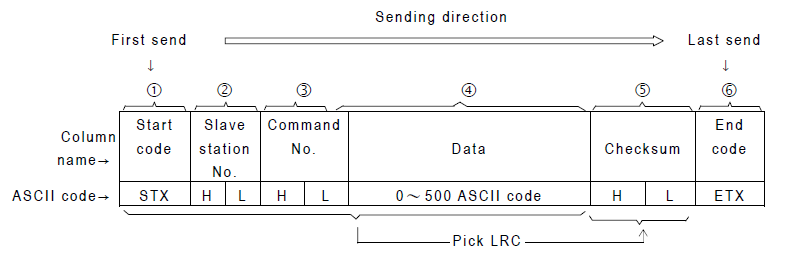


该协议包含站号字段，目标PLC可以设置是否对站号是否严格校验，如果严格校验，只有站号一致的指令才会被目标PLC所接受；如果不严格校验，那么无论站号多少，只要协议格式正确，目标PLC均接受。

目前提取出的关机指令载荷为023031314130303503，该载荷由编程软件WinProladder与永宏FBs-10MC通信流量中得来。经验证，只要目标PLC处于运行状态，无论是否设置密码，只要发送该载荷到目标端口，均可让其停止运转（站号正确的情况下）。

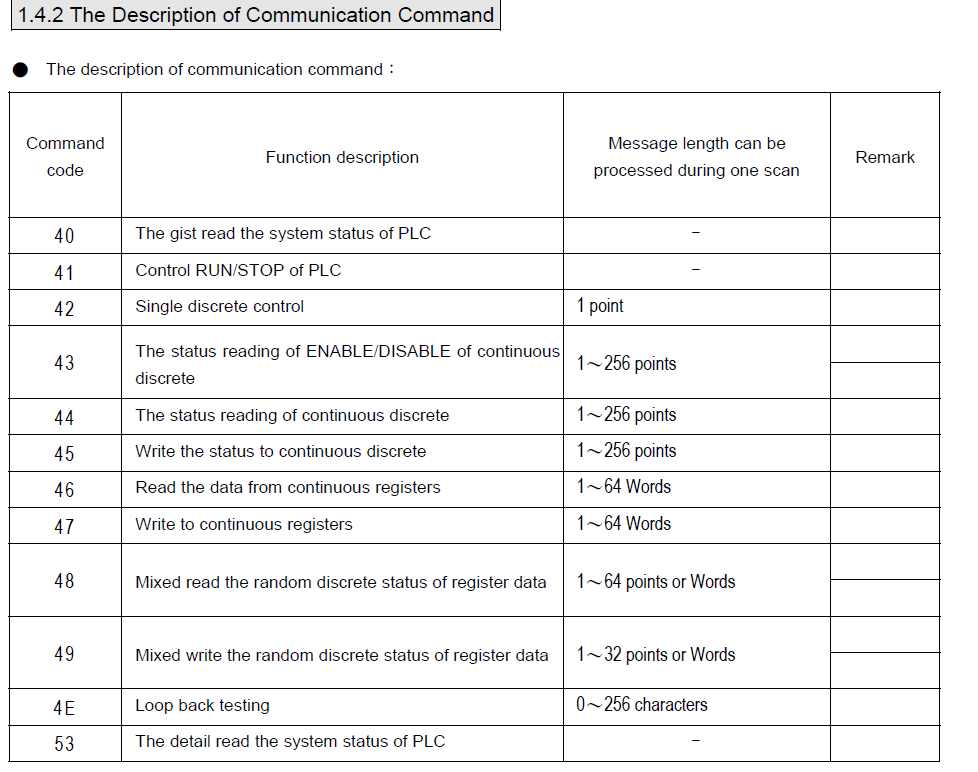
从载荷可见命令号为0x1A，在公开的永宏协议文档中未发现对该指令的描述。另外在公开的永宏通信文档中，0x41为永宏PLC的启停指令，对于该指令的启停效果暂未验证。

永宏FATEK通信协议在网络上可以找到公开的描述文档，这里介绍一下其协议格式，如图所示：



StartCode和Endcode作为协议的首尾部分，分别为固定值0x02和0x03，Slave station No为站号，如站号为1，则Slave station No值为0x30，0x31，即字符“01”的十六进制值，Command No为命令号，后面的Data为传输文本，Checksum为LRC校验码。

目前公开的命令号如下：



据逆向分析研究发现2.6~4.0版本的识别过程与4.0~5.x版本的识别过程存在较大差异，下表为未公开的命令号的含义推测：

|  |  |
| --- | --- |
| **命令号** | **命令含义** |
| 0x2A | 获取目标系统版本 |
| 0x02 | 获取系统信息（OS版本为2.6~4.0） |
| 0x30 | 获取点数信息（OS版本为2.6~4.0） |
| 0x00 | 获取系统信息（OS版本为4.0~5.x） |