

学习工控通讯思路分享（工控交流Q群：207149229 / 852232516）

以下为经验浅谈，用语可能不严谨，旨在帮助刚接触通信的朋友快速确定主要方向，欢迎大家指正。

通讯是信息交互的基础，掌握它有助于理解更多的系统。

通讯（或通信）至少有两步：一是建立连接（数据传输）；二是协议解析（数据分析），如果是安全通信，还有加密和解密两步，这里不讨论。

打个比方来说：通信就像两个人对话，先要双方能清晰听到对方说的话；然后就是双方有通用的语言（如中文或英文）。如果要加密解密，就得有暗号或密码本之类的。

下面分两步简单说一下：

一、通讯连接方式：

1. 串口：常用的接口有TTL、232、485、总线等，使用相应的串口软件就能收发数据，一般要注意接线顺序，通过监控两端数据是否收发一致即可确定连接是否正常，若有问题就需要检查双方的通讯参数和线序，甚至更换串口设备（技巧：可通过短接串口收发线后测试当前设备收发是否正常）。注：串口通信一般容易被干扰，需要使用校验码（例如CRC）来确认数据的准确性。

2. 网络：含无线网，先使用Ping或Telnet等命令确认双方指定端口连接正常；然后通过网络测试小工具确认收发数据一致，若有问题，主要检查端口号、防火墙、路由设置等。注：网络通信一般已具备数据核验功能，但要注意数据头部增加通讯编号。

3. 使用数据网关在多种接口间传输数据：一样的先确认双方连接正常并收发数据一致，具体以产品使用说明为准。

二、协议解析：

目前常用的协议有Profibus/Profinet、Modbus（RTU/ASCII或TCP）、EtherCAT等。

对于不熟悉的通信协议，一定要先使用通用的调试工具来进行测试确认，再进行后续开发。

用Modbus协议来举例，你要开发服务端（也叫从站Slave），就使用ModbusPoll或ModScan等客户端来配合测试；你若要开发客户端（或叫主站Master），就使用ModbusSlave或ModSim等服务端来配合测试，这样你就能高效的判断出自己的思路是否正确，提高开发效率。

刚接触通讯开发的难点一般在于理解：通讯参数（串口的数据位和校验等、网口的网段和端口等）、协议参数（含设备识别码、功能码、数据长度等）、数据类型及长度（各种Bit、整数、浮点数）、数据Byte排序（正反传输）、数据地址偏移（从0或1开始）等。

完成以上简单的一对一通讯后，再去深入了解多数据和多机通讯的轮询机制（考虑硬件特性），以及数据加密解密等。

总结：必须先确认数据连接正常，再研究数据解析；在使用中不断理解各种协议通讯的时效性与数据量和硬件特性的关系，有利于自己开发其它非标通讯协议。