第一章　SCADA 系统

1.1. SCADA 系统的意义

SCADA 是 Supervisory ControI And Data AcquiSition System 的缩写，是对分布距离远，生产单位分散的生产系统的一种数据采集、监视和控制系统。

了解生产情况是实施科学生产的基础，如果生产过程分布很近，可以采用就近控制的办法，就地接线，就地监视，就地控制，对于复杂的过程生产采用 DCS 系统控制的比较多，也有采用 PLC 的或者专业控制器。而对于生产各个环节分布距离非常远的，比如几公里，几十公里，几百公里甚至几千公里的，如变电站，天然气管线，油田，自来水管网，随着技术的发展，人们慢慢发展出远程采集监视控制系统，称为 SCADA 系统。

SCADA 系统与其他系统的区别在于：

分布区域广泛

主站与控制对象距离远

监控终端的工作条件苛刻

通讯系统复杂多变

通讯系统不保证可靠传输

1.2. SCADA 系统的构成

SCADA 系统主要包括三部分组成，主站端，通讯系统和远程终端单元

主站一般采用先进的计算机，有着良好的图形支持，现在采用 PC 计算机和 WINDOWS 系统居多，在历史上，曾经有很多系统采用 UNIX 系统和 XWINDOWS 图形界面。一个主站可能的分站数量从几十到几百、几千个不等。

通讯系统就非常复杂了，有线的包括音频电缆、载波电缆、光纤、电力载波等，无线的包括电台、卫星、微波等。

远程终端单元(RTU or TeleControl)的品种也很多，大的系统由很多机柜组成，小的系统可能就是一个小盒子。

1.3. SCADA 的主站系统

SCADA 系统的主站过去由很多著名的系统是基于 UNIX 操作系统家族和 XWINDOW 图形界面的。

随着计算机系统的发展，特别是 PC 机的发展，PC 机和 PC 机上运行的操作系统在扮演着越来越重要的角色。

庞大的主站系统一般包括如下内容：

通讯前置系统，主要负责解析各种不同的规约，完成通讯接口数据处理，包括数据转发。包括前置计算机，串口池或者 MODEM 池，机架，防雷措施和网络接口。

实时数据库系统，主要包括运行实时数据库的服务器。

工程师工作站，负责系统的组态、画面制作和系统的各种维护。

生产调度工作站，是监控系统的主要用户，显示画面，画面浏览，实现各种报警等。

各种监控工作站，主要用于特别庞大的系统，几个人已经无法监控的情况，这时会根据需要，设立各种的监控工作站，每个工作站有人员工作。

历史数据库服务器，是 SCADA 系统保存历史数据的服务器。

WEB 服务器，是现在 SCADA 主站系统的一个流行趋势，只要用户装有浏览器软件，得到相应的

授权，就可以访问相应的他关心的数据。

上层应用工作站，主要用于实时数据和历史数据的挖掘工作。在电力系统比如潮流分析，负荷预测，事故追忆，电网稳定性分析，能量管理 等等。在自来水行业包括管网压力损耗分析，管网经济性分析，管网漏失分析等。在采油工程上，包括示功图显示，示功图分析，泵况分析，功图计产等等。

作为 SCADA 主站系统，大的系统可能有几十个上百个工作站，多个服务器。为了保证系统的可靠性，采用双前置系统，多服务器系统，两个网络。但是对于简单的 SCADA 主站系统可能就只有一台计算机，运行一套软件。

各种不同应用的 SCADA 系统，可以说大部分是相同的或者类似的。但是各个行业有各个行业的特点，每个行业所关心的东西不一样。比如电力行业非常关心每个线路电压电流功率，而对于自来水行业就不是特别关心这些数据，而关心管道的压力流量等。这样就形成了不同行业的系统。也有通用的人机界面使用，但是这种界面一般无法满足各个行业的特殊需要。

1.4. SCADA 的通讯系统

SCADA 通讯系统是最丰富多彩的，有很多通讯方式是很多人都没有听说过的。一般分类大体可以分为两类，有线和无线，但是随着通讯技术的发展，基于各种网络的通讯方式也发展很快，这种通讯方式很难归结到有线或者无线的范畴，所以也单独作为一类。

有线方式比较多：音频电缆，架空明线，载波电缆，同轴电缆，光纤，电力载波等。在有线上传输大体分为基带传输和调制传输，基带传输是在介质上传输的是数字信号，可能也要经过信号变化。调制解调传输要经过模拟数字变换的传输。很多介质既可以作为基带传输也可以作为调制传输。

无线方式主要包括: 电台、微波、卫星、光线、声波等手段。

网络方式是通讯系统架构在一个计算机网络之上，比如帧中继，ATM.，IP 网，这种通讯方式可能是有线的也可能是无线的，甚至多次跨越无线和有线。其性能也明显区分于有线和无线系统。比如不用考虑误码，不用考虑报文的大小，不考虑系统的拓扑结构，但是网络的时延可能比较大。通过 GPRS 网络或者 CDMA 传输 SCADA 系统数据就是典型的例子。

1.5. SCADA 的远方终端单元

SCADA 系统远程终端单元有一个专门的词汇 RTU。现在术语中称为 TeleControl。

RTU 一般包括通讯处理单元、开关量采集单元、脉冲量采集单元、模拟量采集单元、模拟量输出单元，开关量输出单元和脉冲量输出单元等构成。还有一些其他的接口方式，比如电力变压器的分接头，气象的格雷码接口，水文的 BCD 码接口等等。

远方的通讯一般和 RTU 安装在一起，这样便于接线。

现在的 RTU 出来完成本身的数据采集工作和协议处理之外，还要完成和各种 IED 设备的接口和协议转换工作。而且 RTU 的通讯处理单元的能力越来越强大，而相应的采集工作却在逐渐的弱化，由各种 IED 设备代替了。

RTU 在中国电力系统的最大发展就是用交流采样算法直接计算线路的电压、电流、有功功、无功功率、功率因数、频率、谐波等，取代了传统的电力变送器，降低了成本，降低了接线复杂度，减少了误差环节，提高了精度。而今综合了保护、远动、计量的设备已经出现了，而传统的远动已经基本退出了历史舞台。

在其他行业的发展限于作者的知识范围，无法多写。

SCADA 主站系统

2.1. 概述

主站一般采用先进的计算机，有着良好的图形支持，现在采用 PC 计算机和 WINDOWS 系统居多，在历史上，曾经有很多系统采用 UNIX 系统和 XWINDOWS 图形界面。一个主站可能的分站数量从几十到几百、几千个不等。

SCADA 主站系统主要包括计算机硬件和计算机软件构成。

作为 SCADA 主站系统，大的系统可能有几十个上百个工作站，多个服务器。为了保证系统的可靠性，采用双前置系统，多服务器系统，两个网络。但是对于简单的 SCADA 主站系统可能就只有一台计算机，运行一套软件。

软件主要包括如下模块：

1 规约接口模块
2 实时数据库软件
3 图形界面
4 制图软件
5 历史数据软件
6 上层应用软件
7 报警模块

2.2. 系统硬件构成

庞大的主站系统一般包括如下硬件内容：

通讯前置系统，主要负责解析各种不同的规约，完成通讯接口数据处理，包括数据转发。包括前置计算机、串口池或者 MODEM 池，机架，防雷措施和网络接口。根据系统的规模可能有一个，两个甚至多个前置计算机。串口池是多个串口构成的集合，有两种方式，一种是插在计算机上的多串口卡，一种是以太网接口的多串口服务器。MODEM 池是多个 MODEM 的集合，可以采用多个 MODEM 或者采用 DSP 技术的集成式 MODEM（一个接口可以提供 30 个 MODEM）。

各种数据网关把各种不同的协议进行解析，转换成统一的数据存储于实时数据库中。某种意义上前置系统是一种特殊的网关设备。

实时数据库系统，主要包括运行实时数据库的服务器。

工程师工作站，负责系统的组态、画面制作和系统的各种维护。

生产调度工作站，是监控系统的主要用户，显示画面，画面浏览，实现各种报警等。

各种监控工作站，主要用于特别庞大的系统，几个人已经无法监控的情况，这时会根据需要，设立各种的监控工作站，每个工作站有人员工作。

历史数据库服务器，是 SCADA 系统保存历史数据的服务器。

WEB 服务器，是现在 SCADA 主站系统的一个流行趋势，只要用户装有浏览器软件，得到相应的授权，就可以访问相应的他关心的数据。

上层应用工作站，主要用于实时数据和历史数据的挖掘工作。在电力系统比如潮流分析，负荷预测，事故追忆，

电网稳定性分析，能量管理等等。在自来水行业包括管网压力损耗分析，管网经济性分析，管网漏失分析等。在采油工程上，包括示功图显示，示功图分析，泵况分析，功图计产等等。

支撑硬件：

因为 SCADA 系统要求 365D×24H 连续工作，电源系统要求比较苛刻，除了双回供电，还要求有保证系统供电的 UPS 系统，甚至柴油发电机。

用于系统输出的打印机系统

方便用户了解工作状态的模拟屏系统，这是因为有时整个 SCADA 系统的画面过于庞杂，而调度人员可能关心的数据没有那么多，而且在计算机的屏幕上无法全面显示，为了调度人员了解全局，需要一个 N 平方米的模拟屏显示，而且有些操作可以在模拟屏上演练。

大型投影装置，主要方式有背投，投影仪，电视墙等，其原因基本与模拟屏类似，可以降低调度人员的劳动强度。

安装机柜和布线

空调系统，为了系统可靠工作和人员的舒适性，需要空调系统，而且这样的空调系统不同于家庭空调，可能要求 24 小时工作。

2.3. 系统软件构成

系统软件庞大而复杂，其软件划分有时候类似于盲人摸象，怎么看都有其道理。软件划分的目的是为了软件的编制和维护。一个好的软件架构超过一堆程序员的辛苦努力。软件划分的方法一般分为模块方法，把软件划成很多的模块，软件通过模块通讯的方法进行耦合，对于简单的程序一般采用模块法。模块间的接口只要定义清楚，修改一个模块不会影响到其它模块的功能。

还有一种划分方法是层次法，把软件分为很多层，软件是按照层次关系进行操作，比如对于操作系统就必须按照层次进行分析，层次法的好处对于某一层不满意，只有层间的关系划分得很合理，就可以重新编写一个层替换原来的层，而不需要修改其它代码。

而实际上对于复杂的软件系统一般采用的是模块层次的划分方法，既要按照层的概念定义操作的层次关系，又要按照模块的方法划分同层间的模块关系。

监控系统的层次构成如下，但实际为了软件编制的方便和软件的效率，也未必完全按照这个层次模型进行划分和编写，因为完全模块化和层次化后系统的效率可能很低，影响性能，允许跨层次的访问，一般不允许跨模块的访问。

<table>
<tr><td colspan="2">上层应用软件</td><td colspan="2">数据挖掘软件</td><td colspan="2">状态分析软件</td><td colspan="2">WEB 发表</td></tr>
<tr><td colspan="2">图形界面</td><td>图形工具</td><td>报警</td><td colspan="2">历史数据</td><td colspan="2">其它应用</td></tr>
<tr><td colspan="5">实时数据库</td><td colspan="3" rowspan="3">数据库服务器
/GIS 服务器</td></tr>
<tr><td>规约接口</td><td>OPC</td><td>OLE</td><td colspan="2">其它接口</td></tr>
<tr><td colspan="5">操作系统</td></tr>
<tr><td colspan="2">硬件驱动</td><td colspan="2">图形接口</td><td colspan="2">文件系统</td><td colspan="2">网络系统</td></tr>
</table>

2.3.1. 规约接口模块

从软件划分的角度看规约接口模块是整个监控软件直接和控制设备打交道的，从监控系统的数据来源来看它是最底层的数据提供者，它所服务的对象是实时数据库。它是系统数据的来源，也是系统操作执行的输出模块。

一般按照规约不同，进行模块的划分，不同的规约采用不同的模块实现，OPC 和 OLE 由专门的模块实现，不同的 OPC 和 OLE 采用不同的模块实现。

规约的实现有的是没有层次的，很多也是有层次的。具有层次的规约好处在于在一种通讯模式下的规约很容易在其它通讯模式下实现。规约的调度可以采用单线程或者多线程的方式，单线程实现简单，容易管理，但是效率低。多线程的优点在于效率高，缺点是编写复杂管理复杂。

所有的规约都可以用有限状态机模型进行描述，采用状态机，画出状态转移图后，编写程序时，可以非常清楚状态间的转移和转移条件，避免进入死状态或者出现饿死的状态。

其实规约很多都是有其层次结构的，一般包括物理层、链路层和应用层（不可能采用七层模型，那样太复杂效率太低，软件编写业太复杂），实现时也按照层次实现。协议的分层是指协议报文的头和内容的关系，下层一般把上层的数据作为载荷使用。

规约接口模块可以由软件在前置系统实现，也可以通过硬件（网关设备）实现。所有的数据都写入实时数据库。

现在 SCADA 系统的规约很多，关于规约的问题在其它章节阐述。

2.3.2. 实时数据库

先进的监控组态软件都有一个实时数据库作为整个系统数据处理、数据组织和管理的核心。也有人称其为数据词典。实时数据库与基于传统数据库技术的数据库（如：关系数据库）在原理、实现技术、功能和系统性能方面有很大的不同。集成了实时数据库功能的组态软件的应用范围更为广阔，尤其是在时间关键型应用中。

但实时数据库并不是数据库技术和实时系统两者的简单结合，它在概念、理论、技术、方法和机制方面具备自身特点。如：数据库的结构与组织；数据处理的优先级控制、调度和并发控制协议与算法；数据和事务特性的语义及其与一致性、正确性的关系；数据查询/事务处理算法与优化；I/O 调度、恢复、通信的协议与算法，等等，这些问题之间彼此高度相关。

实时数据库无缝地集成了数据库与定时性，在对数据库能力和实时处理技术两者均有要求的各种领域有着极其广泛的应用前景，集成了实时数据库的监控组态软件，对多种工程或过程及时间关键型应用更是必要而迫切的，为国家的现代化尤其是自动化建设及国民经济的发展提供有力的、必不可少的支持，在信息技术、信息高速公路及信息产业的建设中起到重大作用。

利用实时数据库可以完成以下应用：

1. 记录实时过程的历史数据，用于过程存档、历史数据查询、事故分析、系统建模等。

2. 连接各种类型的自控设备（如：DCS、PLC、智能模块、板卡、智能仪表、控制器、变频器等），配以监控界面，实现自动监控。

3. 通过数据库网络通讯功能构建分布式应用系统。

4. 运行在控制系统（包括 DCS 大型控制系统或其它中小控制系统）的上位机中，在数据库上运行先进控制软件、优化控制软件和其它用户应用程序，在客户机上运行各种界面监控软件，快捷方便地实现可扩展的先进控制或优化控制的目标。

5. 连接多种控制系统和设备，实现车间级、分厂级及总厂级实时数据综合利用和管理。

6. 配合关系数据库管理系统，构建生产指挥调度系统及其它管控一体化系统。

7. 通过数据的 Web 功能，利用 Internet/Intranet 资源，在浏览器上访问生产过程数据。

8. 完全的开放功能，以实时数据库为平台进行再次开发。

2.3.3. 图形界面

指将采集的数据，用各种计算机图形技术展示给使用者而提供给使用者的界面。

主要包括图和动画连接。图指展示给用户的图形，动画链接是指让图随着数据的改变而发生变化。比如在图上存在一个指示灯，与实时数据库内的一个离散变量 X 进行动画连接，那么当 X=0 时至少灯为绿色，X=1 时指示灯为红色。不同的软件对动画连接的叫法不一样，动画连接的词最早见于组态软件。

为了方便用户根据需要产生各种方便的图形，一般主站软件给用户提供了很多类型的图元供用户使用。图元大体可以分为：

基本图元如点、线、矩形、圆形、文字等，这些图元的形状、颜色、填充、文字等在动画连接后可以随着变量的改变而改变。

复杂图元可以是综合了很多基本图元而生成的图元，它的属性更多，更为复杂，比如 X-Y 曲线，圆饼图，指示仪表。

对象图元更为复杂，也更利于用户的使用，比如可以把一个炉子定义成一个对象图元，把一个管道定义为对象图元。

结合 GIS 系统，可以对数据进行多个层面多维度的展现。在很多的 SCADA 系统中需要了解采集控制对象和地理分布的关系，这就需要强大的 GIS 系统的支持。目前的主站软件把这二者结合的不是很多。

2.3.4. 图形工具

提供给开发工程师的工具。

因为一个软件即使功能再强大，提供的图元再多也有不能满足用户要求的时候。这时需要提供一种可以开发复杂图元和对象图元的工具。用户可以根据自己的需要开发图元。

提供这样的工具可以把原来需要软件提供商做的工作交给用户做，如果存在很好的交流和利益分配机制，可以把用户变成开发者，这样对于发展客户和提高软件的功能很有益处。

2.3.5. 报警

报警模块主要用于提示操作人员，主要包括如下类型的报警信息.

开关量输入状态变化报警，指开关量输入信号的状态发生改变，如断路器的位置从合变为分，阀的状态由通变为断等待。这种状态的变化可能直接导致严重的事故或者对系统的运行有巨大的影响。

模拟量超限报警，指模拟量超过或者低于设定的限值，比如管道温度高于设定值，这种状态的可能会导致产品质量下降或者造成人身安全事故。模拟量报警一般包括上上限、上限、下限、下下限等，有时用颜色加以区分。

报警模块从实时数据库读取数据，进行处理，产生报警事件。报警事件写入历史报警记录。

事故追忆(SOE),有时为了分析系统出现故障时系统的状态，便于找出事故原因，需要知道各个重要点数据和时间。这就需要 SOE。SOE 事件记录的产生是在 RTU 内部产生并存储，实质是具有时标的信息（也就是把信息上打上时间标签），主站端需要把这些数据读出来并显示，存入历史报警数据库中。SOE 系统需要整个系统的时钟同步，而且要求同步精度很高（1mS），所以对整个系统要求很高。过去很难有一种办法解决这个问题，现在的网络时钟同步和 GPS 可以很好的解决。

2.3.6. 历史数据

历史数据是整个 SCADA 系统的财富。历史数据是按照时间或者其它规则把实时数据库内容转成历史记录。

历史数据的记录很庞大，一年的记录数据可能就有几个 GB 甚至几十个 GB 的数据量。所以对历史数据库服务器的内存和存储以及 CPU 的速度要求比较高。因为在数据挖掘的时候，需要大量的遍历历史数据。

2.3.7. 网络发布

为了满足信息化建设的要求，避免建设成为信息化孤岛，现在主流的主站软件都有网络发布功能或者模块。

网络发布包括很多种形式，目前最流行的是 WEB 发布，这是因为随着互联网的发展，WEB 浏览器成为目前个人计算机的主要软件配置，而且浏览器软件大多数是免费的，功能相当的强大，用户数量众多。这样通过 WEB 进行发布不需要安装软件，不需要培训客户，用户也习惯这样获得数据。缺点：安全性差和速度慢

网络发布的另外的形式是需要客户安装客户端软件，客户端软件是收费的，所以这种方式不太受欢迎。但是其优点也很明显，安全性高，速度也快，而且甚至不需要借助于网络，通过电话线、RS485、RS232 接口都可以。

网络发布的另外一种形式是通过实时数据库和历史数据库发布，这种发布一般不是给人看的，是应用软件间的一种数据传递方式。

其它的方式如基于网络的 OPC，COBRA 等等。

2.3.8. 主站系统的工作阶段划分

主站系统按照工作阶段可以分为系统开发阶段和系统运行阶段。

系统开发阶段：是设计工程师为实施其控制方案，在主站软件的支持下进行应用程序的系统生成工作所必须依赖的工作环境。通过建立一系列用户数据文件，生成最终的图形目标应用系统,供系统运行环境运行时使用。

系统开发环境由若干个组态程序组成，如图形界面组态程序、实时数据库组态程序等。

其主要使用者是开发工程师和工艺工程师。

系统运行阶段：在系统运行环境下，目标应用程序被装入计算机内存并投入实时运行。系统运行环境由若干个运行程序组成，如图形界面运行程序、实时数据库运行程序等。

主站软件支持在线组态技术，即在不退出系统运行环境的情况下可以直接进入开发环境并修改工程内容，使修改后的工程直接生效。

设计工程师最先接触的一定是系统开发环境，通过一定工作量的系统组态和调试，最终将目标应用程序在系统运行环境投入实时运行，完成一个工程项目。

2.4. SCADA 软件的上层应用

SCADA 系统的上层应用比较复杂，种类繁多，应用五花八门，也就是不同 SCADA 系统区别的本质所在。因为各种 SCADA 系统应用 85%都是一样的，差异很小。而差异主要在上层应用和传感器。

应用太多种类，限于笔者的经历和知识，只能进行一些简单举例。

路灯监控的开灯时间计算是室外照明应用的一个重要的模块，是要根据控制地点的经纬度计算每天的开灯关灯时

间，下置给 RTU 设备进行开关灯控制，这个模块不需要历史数据，仅仅需要当地的经纬度。

电力系统的短期负荷预报，需要利用去年的历史数据和当前几天的历史数据以及天气预报情况，根据数据模型，可以进行短期的负荷预报，可以指导调度和发电。

油井监控的示功图分析和示功图计产，需要根据每口井的示功图数据进行泵况的分析和泵效的分析，给修井、开井和停井提供数据依据。在地形复杂（山地、丘陵、高原），无法设置计量间的地区，可以根据示功图进行产量的估计，虽然有误差，但误差可以忍受，而且就是有误差的数据也比没有误差好。

供热管网的管效分析，根据管网出口的压力和温度，各个测压测温点的数据，取一个时间断面，可以分析管网的效率，分析供热的经济性，甚至为增设和修改管网走向，提供数据依据。

水文监控的洪水预警，根据各个 RTU 采集的降水信息、水位信息等，结合河流流域地区的地貌特征，建立数学模型，可以估计河流的干流和支流的流量，估算水位，发布洪水预告，找出危险地段等等。这种应用关系到人民群众的生产生活，关系到生命和财产的安全。

上层应用只能根据行业进行单独的开发，不可能一个软件满足各行各业的要求。

第三章 SCADA 通讯系统

2.5. 概述

SCADA 中通讯系统显得非常的重要，可以看成 SCADA 系统的神经系统。而通讯实际是单独的一门学科，想在这里用一个章节讲清楚基本是不太可能的。这里只能给出一个粗略的说明，详细内容可以参考有关通讯系统和原理的书籍。

通信系统的基本模型见图 3-1。图 31-1 中发送端的信息源把消息 m 转换成信号 g(t)。为了使信号适合于在信道中传送，由发送设备将它变换为 s(t)后再送人信道。信道是指传输信号的通道。图 3-1 中噪声源是信道中的噪声以及通信系统中其它各处噪声的集中表示。由于噪声的干扰，接收端收到的信号 r(t)可能不同于 s(t)。接收设备把以 r(t)转换为输出信号 g'(t)，它是 g(t)的近似或估计值，最后受信者将 g'(t)转换成对应的消息 m'(t)。

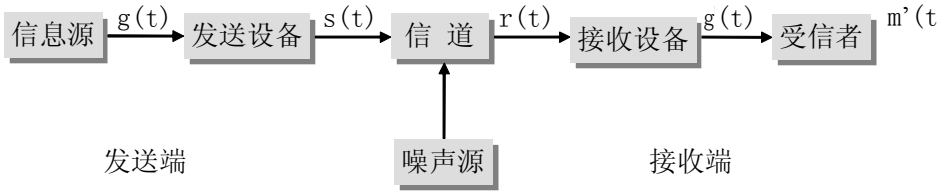


图 3-1　　通信系统的基本模型

由 g(t)到 s(t)称为信道编码，一般调制方式有 ASK,FSK,PSK,QAM,TCM 等等。信道编码经常用在有线和无线通信。随着 DSP 计算能力的提高，AD、DA 速度和精度的提高，以及数学方法的发展，现在信道编码的能力越来越接近香农信息论的理论值，在电话线上，香农信息论的理论值在 64K 以下，而实际的调制解调器可以达到 33.6K 甚至 56K 的速度。

正弦振荡的载波信号可以用 Asin(2*π*ω*t+φ), 各种调制方式可以用下面的数学公式加以描述。

ASK　信号　s(t)= Asin(2*π*ω*t+φ)　g(t)=1
　　s(t)= 0　　g(t)=0

FSK　信号　s(t)= Asin(2*π*ω1*t+φ)　g(t)=1
　　s(t)=Asin(2*π*ω2*t+φ)　g(t)=0

PSK　信号　s(t)=Asin(2*π*ω1*t+π)　g(t)=1
　　s(t)=Asin(2*π*ω1*t+0)　g(t)=0

PSK 和 FSK 还有很多变型的方式，如 DPSK, MSK 等。

QAM 和 TCM 过于复杂，在这里不便赘述，请参考有关书籍。

由于通讯过程中存在噪声干扰，就有可能出现差错，那么就要进行差错控制，差错控制的方法就是编码。通讯编码的数学理论基础是《近世代数》，里面研究群环域的概念，详细内容可以参考相关书籍，而编码解码、检错和纠错是通信与编码学科研究的范畴，国内典型的教材是西安电子科技大学 王新梅老师编写的教材，其缺点过于深奥，不太好懂。

而在 SCADA 系统中经常用的是检错，纠错除了特殊的场合很少使用，检错主要是两种编码方式校验和和 CRC 校验。

和校验原理非常简单，就是对信息进行加法运算或者模 2 加法运算，接收后对信息进行同样的运算，比较运算结果和传输来的校验是否一致，如果一致认为是正确的，否则认为错误。这个算法实现起来非常简单，也得到了广泛的应用，但是其基本原理存在着出现差错检不出的可能，适合于信道质量比较好的场合。

CRC 校验方法可以检出的错误远远超过了和校验，适合比较恶劣的通讯场合。

CRC 校验比较复杂一些，它有一个生成多项式 g(x),信息可以看成一个 i(x)，设校验位为 16 位，则校验多项式 r(x)=x↑16 *i(x) / g(x)。则整个发送序列多项式为 t(x)= x↑16 *i(x) / g(x) + r(x)。接收时，如果没有差错则用 t(x)/g(x)=0, 如果有差错就不是 0。这样就可以知道差错了。人们已经找到很多的标准生成多项式，比如

CRC-16　　g(x)= x↑16+ x↑15+ x↑2+1

CRC –CCITT　　g(x)= x↑16+ x↑12+ x↑5+1

而 CRC 的计算需要进行移位和模 2 加运算，计算机除非有专门的硬件设备，否则计算起来很慢，为了提高计算速度，一般采用查表计算的方法，把运算转换成查表和字节运算，这样使得运算速度大大提高。下面的一段程序 是 MODBUS CRC 校验的计算方法，体现了上述的思想。

```
const unsigned char auchCRCHi[] = {
0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81,0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1,
0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0,0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40,
0x01,0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41,0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0,
0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81,0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41,
0x01, 0xC0,0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01,0xC0, 0x80, 0x41, 0x00, 0xC1,
0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40,0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41,
0x00, 0xC1, 0x81,0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0,0x80, 0x41, 0x01, 0xC0,
0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01,0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40,
0x01, 0xC0, 0x80, 0x41,0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81,0x40, 0x01, 0xC0,
0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40,0x01,0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40,
0x01, 0xC0, 0x80, 0x41, 0x01,0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81, 0x40, 0x00, 0xC1, 0x81, 0x40, 0x01, 0xC0, 0x80, 0x41,0x00, 0xC1,
0x81, 0x40, 0x01, 0xC0, 0x80, 0x41, 0x01, 0xC0, 0x80, 0x41, 0x00, 0xC1, 0x81,0x40
} ;
const unsigned  char auchCRCLo[] = {
0x00, 0xC0, 0xC1, 0x01, 0xC3, 0x03, 0x02, 0xC2, 0xC6, 0x06, 0x07, 0xC7, 0x05, 0xC5, 0xC4,0x04, 0xCC, 0x0C, 0x0D, 0xCD, 0x0F,
0xCF, 0xCE, 0x0E, 0x0A, 0xCA, 0xCB, 0x0B, 0xC9, 0x09,0x08, 0xC8, 0xD8, 0x18, 0x19, 0xD9, 0x1B, 0xDB, 0xDA, 0x1A, 0x1E,
0xDE, 0xDF, 0x1F, 0xDD,0x1D, 0x1C, 0xDC, 0x14, 0xD4, 0xD5, 0x15, 0xD7, 0x17, 0x16, 0xD6, 0xD2, 0x12, 0x13, 0xD3,0x11, 0xD1,
0xD0, 0x10, 0xF0, 0x30, 0x31, 0xF1, 0x33, 0xF3, 0xF2, 0x32, 0x36, 0xF6, 0xF7,0x37, 0xF5, 0x35, 0x34, 0xF4, 0x3C, 0xFC, 0xFD,
0x3D, 0xFF, 0x3F, 0x3E, 0xFE, 0xFA, 0x3A,0x3B, 0xFB, 0x39, 0xF9, 0xF8, 0x38, 0x28, 0xE8, 0xE9, 0x29, 0xEB, 0x2B, 0x2A, 0xEA,
```

```
0xEE,0x2E, 0x2F, 0xEF, 0x2D, 0xED, 0xEC, 0x2C, 0xE4, 0x24, 0x25, 0xE5, 0x27, 0xE7, 0xE6, 0x26,0x22, 0xE2, 0xE3, 0x23, 0xE1,
0x21, 0x20, 0xE0, 0xA0, 0x60, 0x61, 0xA1, 0x63, 0xA3, 0xA2,0x62, 0x66, 0xA6, 0xA7, 0x67, 0xA5, 0x65, 0x64, 0xA4, 0x6C, 0xAC,
0xAD, 0x6D, 0xAF, 0x6F,0x6E, 0xAE, 0xAA, 0x6A, 0x6B, 0xAB, 0x69, 0xA9, 0xA8, 0x68, 0x78, 0xB8, 0xB9, 0x79, 0xBB,0x7B, 0x7A,
0xBA, 0xBE, 0x7E, 0x7F, 0xBF, 0x7D, 0xBD, 0xBC, 0x7C, 0xB4, 0x74, 0x75, 0xB5,0x77, 0xB7, 0xB6, 0x76, 0x72, 0xB2, 0xB3, 0x73,
0xB1, 0x71, 0x70, 0xB0, 0x50, 0x90, 0x91,0x51, 0x93, 0x53, 0x52, 0x92, 0x96, 0x56, 0x57, 0x97, 0x55, 0x95, 0x94, 0x54, 0x9C,
0x5C,0x5D, 0x9D, 0x5F, 0x9F, 0x9E, 0x5E, 0x5A, 0x9A, 0x9B, 0x5B, 0x99, 0x59, 0x58, 0x98, 0x88,0x48, 0x49, 0x89, 0x4B, 0x8B,
0x8A, 0x4A, 0x4E, 0x8E, 0x8F, 0x4F, 0x8D, 0x4D, 0x4C, 0x8C,0x44, 0x84, 0x85, 0x45, 0x87, 0x47, 0x46, 0x86, 0x82, 0x42, 0x43,
0x83, 0x41, 0x81, 0x80,0x40
} ;

unsigned short crc(unsigned char *puchMsg , unsigned short usDataLen)
    {
      unsigned char uchCRCHi = 0xFF ; /* high byte of CRC initialized */
      unsigned char uchCRCLo = 0xFF ; /* low byte of CRC initialized */
      unsigned uIndex ; /* will index into CRC lookup table */
       while (usDataLen--)/* pass through message buffer */
       {
          uIndex = uchCRCHi ^ *puchMsg++ ; /* calculate the CRC */
          uchCRCHi = uchCRCLo ^ auchCRCHi[uIndex];
          uchCRCLo = auchCRCLo[uIndex] ;
       }
      return (uchCRCHi << 8 | uchCRCLo) ;
    }
```

当然，还可以用编码解码的方法纠正错误，但是实现起来比较复杂，一般只有在信道非常昂贵的时候才使用如卫星通道和深空通讯。在 SCADA 系统中采用可以纠错的编码的极少。

通讯由于介质的不同大体可以分为如下的三种类型：

有线、无线和网络。单独把网络拿出来是因为这些年网络技术发展很快，目前网络成了传输 SCADA 信息的一个很重要的方式。

信道分类也可以分为半双工和全双工的信道，但是有时即使信道是全双工的，而协议是半双工的，系统也工作在半双工状态。

2.6. 有线系统

有线的范畴很广，常用的包括电话线、音频电缆、电力载波、同轴电缆、光纤等待，我们这里的有线指的是要有介质连接而且不经过网络协议而直接进行 SCADA 协议的通讯方式。

在有线信道中，除了载波信道，普遍来看传输的速度要高于无线信道，误码率低于无线信道，时延也小，可靠性高于无线信道。其缺点是建设投资大，周期长，而且在有些特殊场合根本无法建设有线的通讯方式。

有线信道中有的是直接传输的数字信号，比如在双绞线上走 RS485/RS422 信号，在双绞线上通过长线驱动设备进项传输，在光纤上直接传输的都是数字信号。RS485 可以在 100KBPS 的速度上传输 1.2 千米，长线驱动器可以到 19.2KBPS 的速度，光纤可以到几百 K 甚至几百兆的速度，传输距离可以在几百米到几十千米。。

有线信道很多要用到调制解调设备，如电话线、音频电缆、载波通道，其信道容量肯定小于香农信息论容量。电话线中的调制解调器可以达到 33.6kbps 的速度，而载波通道有的只能到 300bps 的速度。

2.7. 无线系统

无线信道常用的包括无线电台、微波通讯和卫星通讯等。GPRS/CDMA 通讯方式列入网络通讯的范畴。

无线电台由于收到带宽的限值，其信道一般为 25KHZ，无线电管理委员会专门划出几个频段用于无线数据传输，主要包括 150MHZ 频段，230MHZ 频段和 470MHZ 频段。目前的调制解调技术可以做到的速度从 600bps 到 19200bps 不等。目前一般都是采用调制解调器和无线电台做在一起的数传电台。

采用无线电台中心站要复杂一些，为了系统能够更好的通讯，需要建设一个很高的全向天线，有的是安装在楼顶，有的是建设专门的铁塔。实施前要进行频点干扰测试、遮挡测试、场强测试等。无线电台受到地形和建筑的影响相当严重，有时会出现本来通讯很好，在中间出现一个高层建筑导致无法通讯。无线电台有时不适宜于城市应用，也不适宜于山区、高原、丘陵地带使用。适合于平原农村和水面应用。

无线电台是一个典型的半双工轮询系统，系统如果点数很多，轮询一遍所花的时间可能会长达几分钟甚至更长。

另外必须区分无线电台的接口速率和空中速率，这二者是独立的没有关系的两个概念。空中速率指的是电台在无线信道的实际数据速率，这个速度越快，说明电台的性能越好，而且单位时间传输的数据越多。接口速率是电台 与 RTU 设备的速率，这个速率只要不小于空中速率和通讯速度没有太大关系。

无线电台可能会受到干扰的影响，严重影响通信性能，甚至完全无法使用。主要干扰有：同频干扰、高压输电线路电晕干扰、其它射频设备等。一般不受天文情况的影响，如太阳黑子，太阳磁暴，电离层等。

微波通讯只有在特别重要的场合才实施，其投资巨大，而且要每大约 50KM 就要有一个中继站，对于地形复杂的场合，可能为了视距原因可能很近就要有一个中继站。一般的单位是没有财力建设微波系统的。国内的电力企业当年倒是有一套从各个大区到中央的微波通讯系统。微波通讯还是会收到降水和雾的影响的。

卫星通讯更是万不得已才使用，首先其功率太大，一个小型的卫星基站要上百瓦的功率，需要一个 1M 口径的抛物天线，需要专门昂贵的设备（通讯设备要人民币几万块），而且通讯费用非常高昂，一个报文，可以承载 256BYTE 的数据需要 0.5 圆人民币，只有海上，沙漠等实在无法借助其它通讯手段的时候才采用。

卫星通讯相当可靠，除了太阳耀斑、太阳磁暴、暴雨等情况，一般都不会出现通讯中断现象。

太阳耀斑、太阳磁暴会影响卫星的通信，还存在所谓的星蚀效应，就是通信卫星和太阳在同一个方向上，由于太阳是一个很大的干扰源，导致卫星通信中断。不过中断时间只有几分钟的时间。

2.8. 网络系统

网络通讯方式在无线方式上常用的包括 GPRS/CDMA, ZIGBEE, 无线以太网等。有线方式常用的包括以太网、ADSL、CABLE MODEM 等。

网络通讯方式的优点在于借用现有的网络资源，真正打破了地域的限制，可以构架分布全球的 SCADA 系统，对于很多全球生产的企业非常有利。

由于网络构建于公共网络之上，在出现突发事件时而且要求 SCADA 系统在突发事件进行应急处理时，这样的方式可能会因为公众通讯的信息量大增，导致通讯设备瘫痪或者阻塞，而无法应对这样的应用。这种通讯阻塞的情况完全有可能出现，所以在构建 SCADA 系统的时候，一定要评估这个风险，否则就是一套在紧急情况下不能使用的系统，这个系统可能就没有建设的必要。对于这种系统一定要采用生存能力强的独立系统，比如无线电台。

在网络通讯上，由于 GPRS/CDMA，ADSL 等设备都是构建在 PPP 协议或者 PPPOE 协议之上的，其地址分配可能是动态的，也可能是静态的。而主站的地址可能是静态的也可能是动态的，所以二者可能存在互不知道 IP 地址的可

能，如果没有专门的机制是无法通讯的。为了保证 RTU 能和主站通讯就需要做专门的处理。

就 TCP/IP 通讯而言，双方必须知道对方 IP 地址和端口号才能通信，而且一般的通讯模型是客户机/服务器模型，而且一般主站作为服务器使用，所以主站系统不能放在防火墙的后面，如果放在防火期后面，防火墙至少要开放几个端口，而且把主机的 IP 地址通过 NAT 的方式映射到公网上，否则 RTU 不可能和主站通讯。如果主站地址是静态的，RTU 端设置通讯设备时，把主站的 IP 地址设为主机 IP 地址。这样上电后，RTU 的通讯设备 DTU 就可以根据设定的 IP 地址和端口号及通讯方式（TCP/UDP）找到主站进行通讯。

如果主站是动态地址（比如采用电话拨号上网或者 ADSL 拨号上网），由于主机地址是动态的，RTU 的通讯设备 DTU 的 IP 地址也是动态的，双方不可能直接找到对方。

就需要申请一个动态域名解析业务以区别于静态域名解析服务，比如动态域名为 WWW.JUYINGELE.COM.CN，在主站端安装动态域名解析软件，主站只要开机就登陆到动态域名服务器，比如花生壳，注册自己的 IP 地址，告知 WWW.JUYINGELE.COM.CN 的地址是 XX.XX.XX.XX。RTU 端的 DTU 设备设置时其通讯的主机不能设为 IP 地址，而应该设为 WWW.JUYINGELE.COM.CN，在 DTU 设备上电后，首先向 DNS 服务器请求解析 WWW.JUYINGELE.COM.CN 的 IP 地址，DNS 服务器根据动态域名解析软件注册的 IP 地址，告诉 DTU，WWW.JUYINGELE.COM.CN 的 IP 地址是 XX.XX.XX.XX，这样 DTU 知道了主站的 IP 地址和双方约定的端口号和通讯方式(TCP/UDP)就可以通讯了。

另外，由于通讯是 TCP/IP 通讯，主站和 RTU 端的端口号和通讯方式（TCP/UDP）要设成一致。

GPRS/CDMA 的应用是无线通讯，几乎没有数传电台的缺点，其构架于无线通讯运营商的网络之上，只要手机能够通话就能工作，缺点是按照流量收费，费用可能略微嫌高。另外收到网络能力限制，同时能够发起的认证连接数和同时能够维持的连接数有限，对于大规模的应用可能是一个相当大的制约。一般来看 CDMA 的通讯速度要高于 GPRS，而实际应用中，SCADA 系统应用的速度要远远低于其标称速率。GPRS/CDMA 还有一个重要的问题是网络延时问题，从用户发出一个报文到收到响应报文，可能需要 3 秒甚至更长的时间，对于有些苛刻的应用无法满足。

无线以太网是一个非常有前途的通讯方式，其价格越来越便宜，而且带宽很宽，最高可以到 54M，可以在上面承载语言业务、图形监控业务和 SCADA 业务，非常有发展潜力。而且可以在无线以太网上构建自组织网络（MASH 网），这样无论网络是固定的还是移动的，都能正常通信；即使出现个别设备的损坏，都能通过网络的再组织，保证正常的通信。无线以太网采用全向天线时，其通讯距离受到很大的限制，只有几百米，而采用定向高增益天线，距离可以到几到几十公里。

ADSL/CABLE MODEM 都是大家耳目能详的日常上网方式，其优点缺点想必大家都很清楚，值得一提的是很少有 RTU 设备可以直接支持 PPPOE 协议，这可能需要进行配置或者增加网络设备实现，倒是一个限制。

第四章 远程终端单元（RTU）

2.9. 概述

按照国标 GB/T 14429-93 《远动设备及系统 术语》中的定义，远动（tele control）指应用通信技术，完成遥测、遥信、遥控和遥调等功能的总称。简称“四遥”。

远程测量指应用通信技术，传输被测变量的测量值，同义词：遥测。

远程信号指应用通信技术，完成对设备状态信息的监视，如告警状态或开关位置、阀门位置等；同义词：遥信。

远程命令指应用通信技术，完成改变运行设备状态的命令；同义词：遥控 。

远程调节指应用通信技术，完成对具有两个以上状态的运行设备的控制；同义词：遥调。

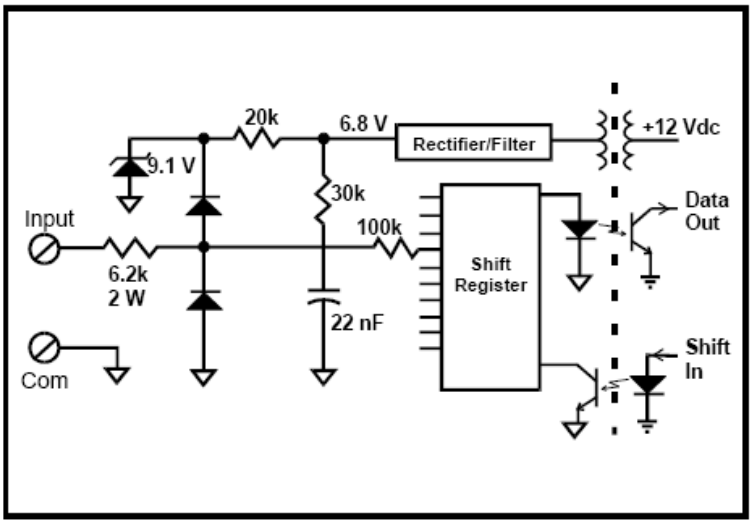
本章节只想对测量技术做一个粗略的介绍，让读者有一个概括性的了解，而不会深入到技术细节去讨论某个功能怎么实现。

2.10. 远程信号

远程信号的实质是开关量状态的采集和传输。

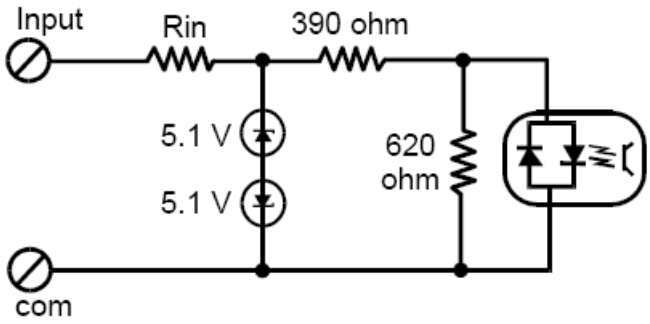
开关量的采集现在一般都采用光电耦合器进行隔离，过去也有其它的方法。

下图是一个型号的遥信输入电路：



其优点是节省光耦的数量，其缺点是扫描的速度和可靠性不好。

这是另外一种型号的开关量输入电路



这是大多数 RTU 和 PLC 以及 DCS 系统典型的开关量输入电路，但是其电阻值未必是典型的。

其原理是当开关量输入状态接上电源后，光耦的发光二极管发光，被光敏三极管接收，光敏三极管导通；平常发光二极管不发光，光敏三极管截至。作为计算机系统扫描输入的 IO 口，或者扩展的数字输入，就能得到开关量的状态。

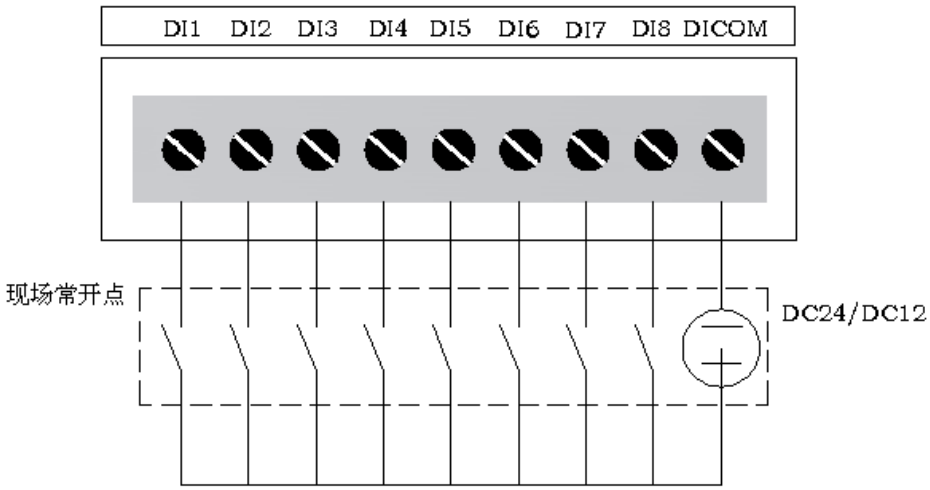
如果扫描速度够快，就能发现开关量输入状态的变化，可以用于低频的计数，有时称为遥脉。

一组开关量输入，如果每位的权重不一样，组合起来，又称之为数字量输入，在水位编码信息，变压器分接头位置上有着广泛的应用。

有时为了研究事件发生的顺序，需要记下开关量状态发生变化的时刻，这种信息称为带时标的开关量，称为 SOE。

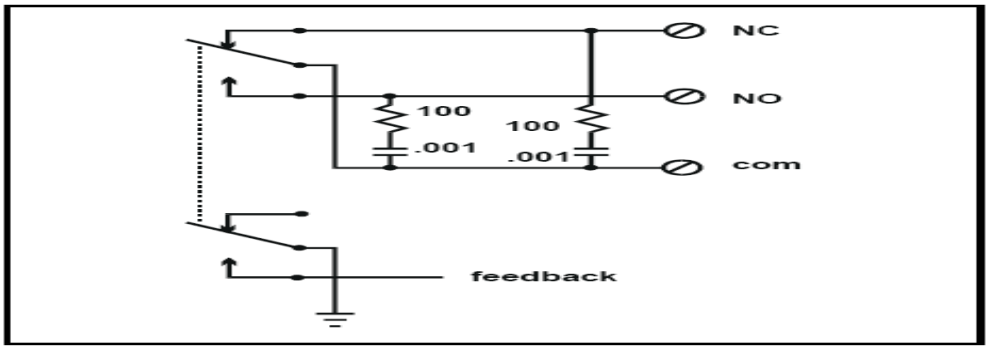
光耦的耐压一般在 3500V 以下，也有特殊的型号耐压可以超出这个数字，所以不能用光耦隔离共模电压很高的场合。

现场接线可以参考下图，但是最主要的是参考厂家的使用说明书



2.11. 远程命令

远程命令的实质是开关量输出，下图是一个典型的继电器输出：



图中采用了双刀双掷的继电器，一组用于输出，一组用于状态的回馈。这种设计指应用于要求非常高的场合，普通的应用，一般不需要回馈。

图中的电阻和电容，是用于火花吸收的，可以在感性负载下，可以降低触点间的过电压和火花，大大提高触点的寿命。

继电器输出形式在可靠性，抗负载复杂性上性能很好，但是其动作速度慢，不能控制非常小的信号（如毫伏、微安级信号），寿命有限，并不能适合所有场合。

开关量输出还有晶体管和固态继电器的形式，其负载能力比较差，对于过电压耐受能力比较差；可以快速动作，可以控制非常微弱的信号。

2.12. 远程测量

远程测量也就是模拟量输入，一般通过 AD 转换和多路模拟量开关进行多路切换测量。现在的 AD 价格已经很便宜了，有的 AD 甚至把多路模拟开关直接做到了片内。目前 12 位的 AD 已经很普遍使用，16 位的 AD，甚至 24 位的 AD 也得到了广泛的使用。

远程测量肯定离不开变送器和传感器，变送器是把物理信号转换成标准电信号的设备。传感器是把物理信号变为可电测量信号的设备。

最简单的例子就是温度测量，传感器采用 PT100，PT100 传感器是一个热敏电阻传感器，其在 0 摄氏度的电阻值是 100 欧，每增加一摄氏度，其电阻增加 0.3875 欧姆。而温度变送器是把这个电阻信号转变成标准的二线制 4～20mA 信号。如果变送器的范围是 0～100 摄氏度，在 0 摄氏度时，变送器输出 4mA 电流，在 100 摄氏度，输出 20mA 电流，如果电流是 12mA,传感器安装环境的温度就是 50 摄氏度。

模拟量输入由于历史原因，其信号非常复杂，一般包括如下的几种信号 0～10V,0～5V，0～20mA，4～20mA 几种量程。以 4～20mA 信号最为常用，一般的变送器都变送成 4～20mA 的信号输出。

4～20mA 信号又很多优点，比如可以方便的判断开路，可以方便的采用 2 线制供电，传输距离长（因为是恒流的），不容易受到干扰等等。但是 AD 转换一般都是电压输入的，需要通过电阻变成电压信号才能采集，另外由于是 2 线制的，一个仪表给 2 个采集装置非常困难，只有通过专门的设备才能实现。

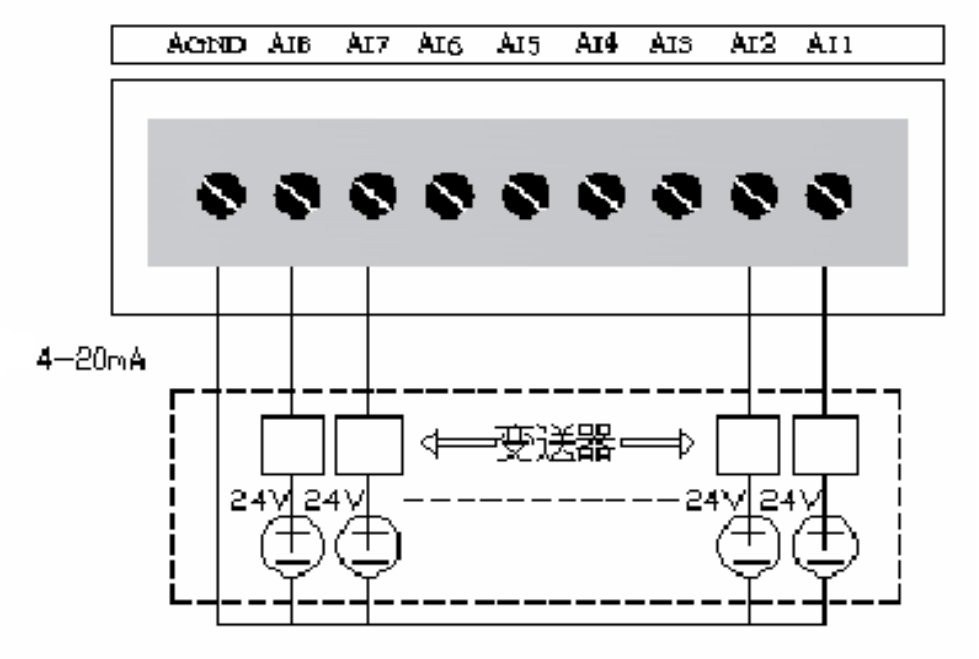
模拟开关可以是电子开关，最为简单的是 CMOS 的 CD4066 型号，价钱才几块钱，也有复杂的如 ADG508，一片要几十块钱。为了提高通道间的隔离度，有人采用光电模拟开关进行多路的选择，这样的固态继电器的耐压可以到 400V，而电子开关的耐压才几伏，几十伏。很多厂家宣称其通道间耐压能达到 400V，具体怎么实现，却作为技术秘密，从来不透露。实际上各家的电路设计都大同小异。

12 位 AD 转换在国内应用中典型的芯片是 AD574，现在已经停产了，换成了 AD1674 了。16 位的 SAR AD 非常昂贵，现在用的 16 位/24 位的 AD 大多数是 Delta-Sigma 类型的 AD，片内集成 PGA，性能非常优越。

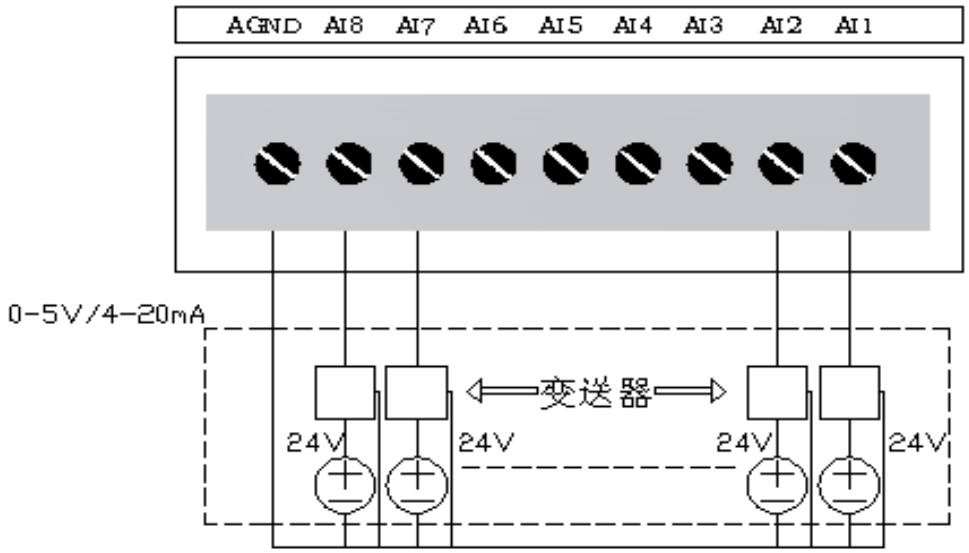
对于一些典型的应用，如电力远动，已经把电量变送器和 RTU 设备合为一体的，称为交流采样技术，这样省去了误差环节，提高了系统的精度、可靠性，降低了系统的成本和安装复杂度。

目前有一种把测量和变送器合在一起的趋势，特别是对于典型的传感器，如热电阻、热电偶、应变片等。

二线制变送器接线



三线电流型变送器接线



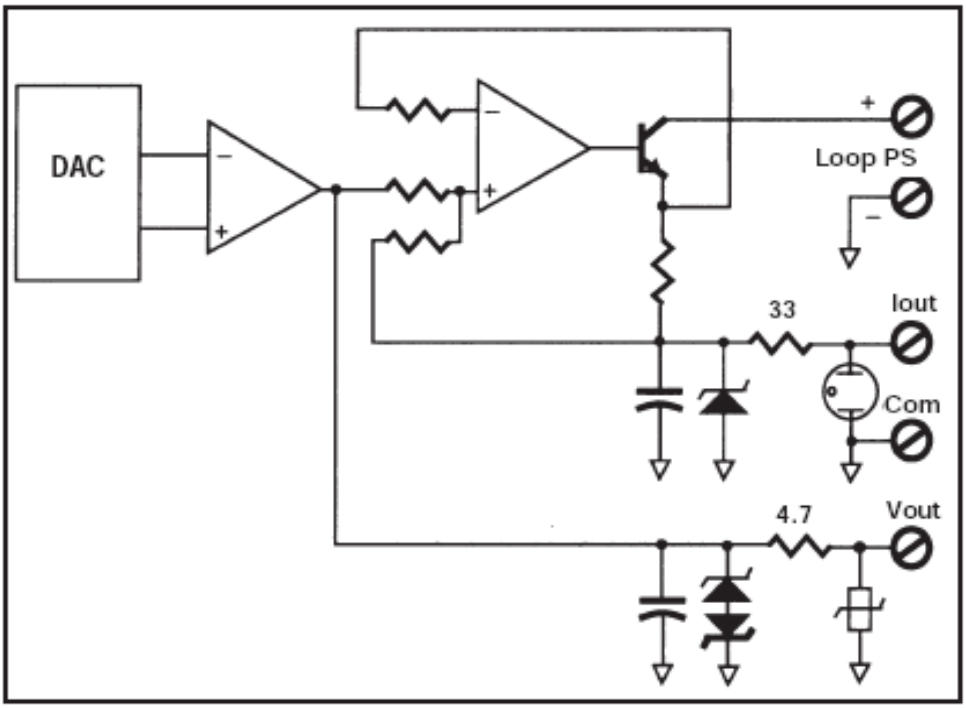
2.13. 远程调节

远程调节主要是模拟量输出，但是也有开关量输出的。

模拟量输出主要形式是通过 DA 转换和相应的电路把输出信号转换成标准的模拟信号，如 4～20mA，0～10V 等。比如把这个信号输出给变频器，使之输出频率改变而改变电动机的转速，从而控制压力，控制转速等。

远程调节的开关量形式也有，比如，通过给阀门的电机通电，让阀门转动，通过时间的控制来控制阀门的开度。正方向开关量给电时间越长，阀门开度就越大，反方向，开关量给电时间越长，阀门开度就越小。这种控制一般不是线性的。

典型的模拟量输出模块框图



这个框图同时给出了电压输出和电流输出的两种形式。该电路设计了不少的保护元件，提高系统的可靠性。