第六章：使用 Modbus 注意要项

1　善用检核表及 Utility 程序做通信异常确认

由于通信系统是包括双方甚至多方的设备及系统都要配合得当，才能建立完成。于通信系统建立之初或者某种设备异动故障时，常常为了找出其通信不通的关键点，需要耗费许多时间。本章节提供一个检核表（Check List），让使用者由硬件、配线、设备的设定系数、操作系统、应用程序等各种方向，做一一的检查，希望以标准的程序为每次通信系统建立时，提供一个最快速便捷的方法。

检查项目	说明	结果纪录
1. 串行式硬件		
1.1 硬件接口	RS232、422、485 等。	
1.2 Baud Rate	1200、2400、4800、9600、19200、38400、57600、115200 等双方设定是否一至。	
1.3 Parity	None、Odd、Even 等双方设定是否一至。	
1.4 Data Bits	7、8 等双方设定是否一至。 注意 Modbus 设定于 RTU Format 时一定要使用 8 bits。 设定于 ASCII Format 时大部份设备使用 7 bits，但是有时会用 8 bits。	
1.5 Stop Bits	1、2 等双方设定是否一至。	
1.6 RS232 Flow Control	RTS/CTS、Xon/Xoff、Modem、None 等数种信号流程的控制。与 Pin Assignment 有很大的关系，见后面 Pin Assign 图标。	
1.7 RS232 Pin Assign	详见 Pin Assignment 图标及配线安排。	
1.8 RS422 Pin Assign	同上	
1.9 RS485 Pin Assign	同上	
通信线	是否有连接。 RS232 连接线是否超过 15 米，此种情形容易受噪声影响。	
1.10 RS232 电压准位	联机双方的电压准位，如果某一方过低，将无法辨别 0、1 信号而通信不良。 有些控制设备对此规格要求甚严。 一般 PC 所输出的信号都可符合规定。	
1.11 RS485 干扰	信号隔离效果，如果未有效隔离，容易产生噪声而有 CRC Check error。	
2. Ethernet 系统		

2.1 IP Address 对应	所要连接的 Modbus 设备 IP Address 是否对应无误。也就是 Modbus Slave 设备本身的 IP Address 与 Modbus Master Driver 所设定的 Remote IP Address。	
2.2 IP Address 重复	于网络上相同 IP Address 是否重复设定。	
2.3 NetMask	联机双方的 NetMask 是否一至。	
2.4 TCP Port No.	Modbus Default TCP Port No.为 502。	
2.5 Ethernet Cable	是否有连接。再检查 Pin 脚跳线或不跳线。	
2.6 Hub or Switch	是否连接完成。	
2.7 同一网域	网域设定检查。	
2.8 系统权限	是否有权限进入 Remote Modbus Slave 系统。	
2.9 是否防火墙的影响	是否被防火墙挡住。	
2.10 Ping check	执行 Ping 程序，检查基本网络联机是否无问题。	
3. Modbus 基本设定		
3.1 Modbus Address 范围	同一 RS485 网络上的每个 Modbus 设备的 Address（ID No.）必须唯一的。 其范围为 1 – 247。	
3.2 Modbus Address 重复设定	是否有重复设定。	
3.3 Relay/Register Type	一般 Modbus 信号点有 Output Coil、Input Status、Input Register、Holding Register 等四种。使用 Modbus Protocol Function Code：1、2、3、4、5、6、15、16 等。	
3.4 特殊 Relay/Register Type	较特殊者会提供 Gerenal Reference Register，使用 Modbus Protocol Function Code：20、21 等。	
3.5 Relay/Register Address 超出系统范围	控制设备对于每种信号点范围都有规定。当设定 Modbus Master Driver 的取入信号地址必须遵循此规格。	
3.6 Relay/Register Address、Type 的一至性	联机双方所设定的信号点必须匹配。也就是 Modbus Master 所要求的信号点，必须 Modbus Slave 可以提供的。 例如：有些电流表只提供 Holding Register 而且只有数点。 所以必须详读该设备的 Modbus 点数规定。	

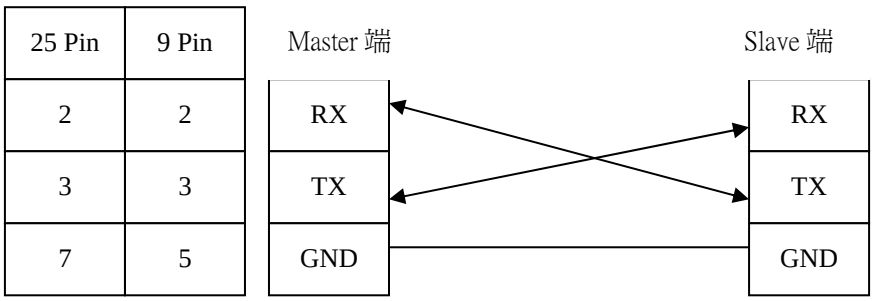
3.7 一次通信点数	Modbus 规定一次通信 Message 为 256 bytes。所以于两种通信 Format 最大通信点数大约如下规定： ASCII Format：Relay 960 点、Register 60 点。 RTU Format：Relay 1920 点、Register 120 点。 如果某些控制设备有其它规格时，必须遵循此规格。不过不能超过以上最大点数规定。	
3.8 连续点的利用	如果相同 Type 数点信号并不连续，但是 Address 很接近，此时最好规划为同一个 Unit 通信一次，而不要每一点通信一次。两者间总通信时间会相差数倍。	
3.9 Exception Code 研判	当 Modbus Slave 接到 Command message 后，如果检查内容不符合，会回传 Exception Code，请检查 code 内容。	
3.10 ASCII LRC error	当通信受到噪声干扰时，Modbus Slave 接到后计算 LRC 不对，不会响应任何讯息。	
3.11 RTU CRC error	当通信受到噪声干扰时，Modbus Slave 接到后计算 CRC 不对，不会响应任何讯息。	
3.12 RTU Message 结束的断定	依据 Modbus 规定，断定 RTU Message 是未接到下一个字符的时间超过 3.5 字符的通信时间。 有些 Modbus Driver 提供 RTU char. Timeout 系数，供使用者设定以调整联机双方的配合。	
4. 其它事项		
4.1 COM Port 被使用	COM Port 已经被其它程序所占用。	
4.2 Cable 断线	因为 Pin 脚接点焊接不够结实，造成有时通或不通的状况。 因为过热或被雷击稍有脱落现象。	
4.3 电源未接	被联机的设备，位于工厂某个角落，常常因为电源未接上或被拔掉造成通信不通。 RS232/422/485 信号转换器或者信号加强器等。 Ethernet 使用的 Hub or Switch 等未接电源。	
4.4 Polling Time	此为 Modbus Master 主动通信的时间间隔，例如为 10 millsecond，表示此时间就会通信一次。此时间必须调整，时间过短会造成通	

	信堵塞现象。	
4.5 Timeout check	此为 Modbus Master 端传送 Command 后，等待 Modbus Slave 端的回传 Respnse 的最大时间。如果逾时，表示 Slave 设备不在联机网络上。 有些 Modbus Slave 因为 Processor 处理速度过慢，造成反应时间超过 Modbus Master 端 Timeout 值，就必须调整此值因应。此种现象常发生在一些较低阶 Modbus 设备上，因为使用速度较慢的硬设备。	
5. Utility Program Check	见下面图标说明	

图(6-1)：Modbus 通信检核表

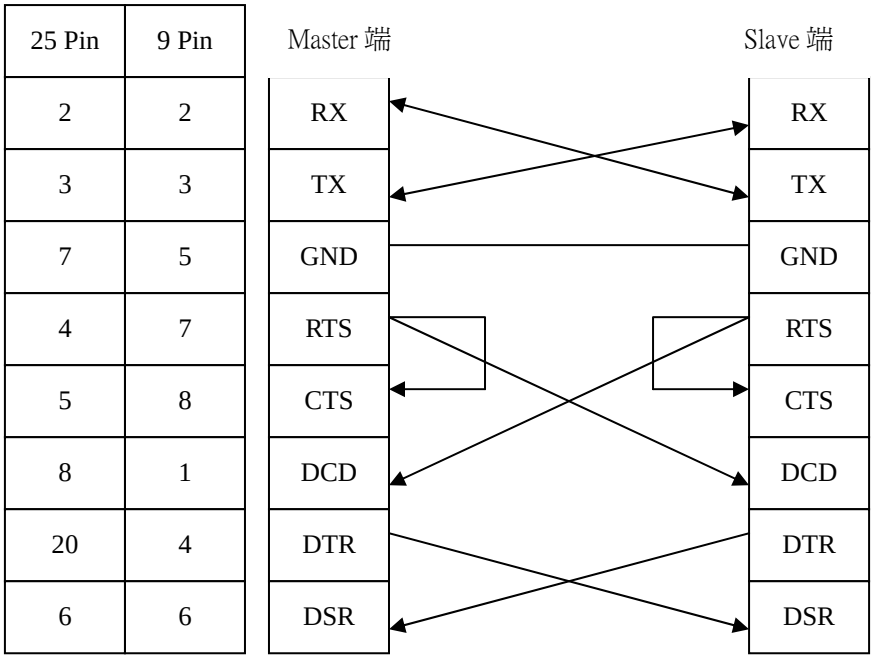
1.1 串行式 Pin 脚须知

RS232 Pin 接线方式(1)：只用 RX、TX、GND 等三个 Pin。适用于不做任何 Flow Control 的场合。

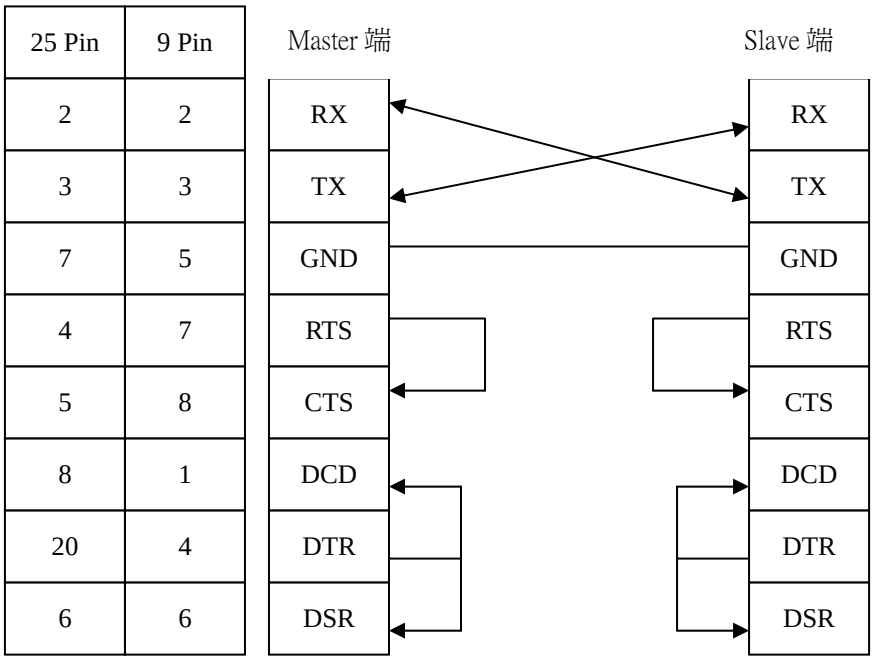


图(6-2)：RS232C Pin 联机图(1)

RS232 Pin 接线方式(2)：除了 RX、TX、GND 等 Pin 外，再加上硬件信号检查的 Flow Control 的场合。一般来说绝大部份是以下的两种方式接法：第一种将 RTS 与 CTS 等两点对接，然后 DTR、DSR、DCD 等三点连接，如果是联机双方互相连接就是标准接法。第二种将以上的 Pin 脚自行与自己的 Pin 脚互接的短路接法，表示自行发出的检查信号，回到自己另一 Pin 脚，确认通信状态良好。

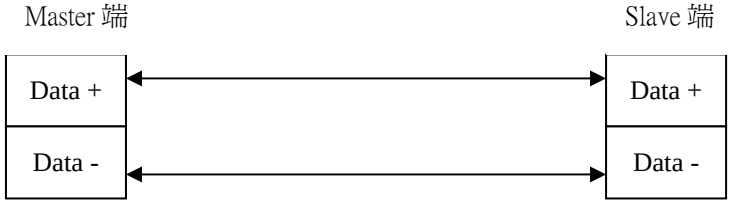


图(6-3)：RS232C Pin 联机图(2)



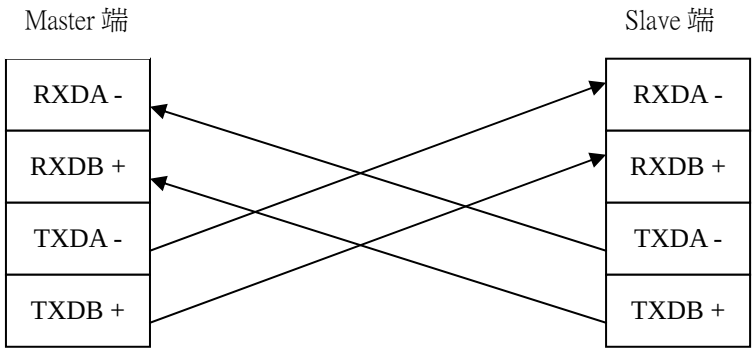
图(6-4)：RS232C Pin 联机图(3)

RS485 接线法：Pin 脚号码未标准化，依据各项设备的规格而定



图(6-5)：RS485 Pin 联机图

RS422 接线法：Pin 脚号码未标准化，依据各项设备的规格而定



图(6-6)：RS422 Pin 联机图

1.2 以 Utility 程序测试 Modbus 联机架构

联机系统的建立，是必须两个端点的设备及系统完全配合，才能成功的。所以测试联机系统排除障碍点的步骤，就是要以 Utility 分开测试 Modbus Master 及 Slave 的设备，然后再将两端联机做整合测试。所要测试确定的三大部份为

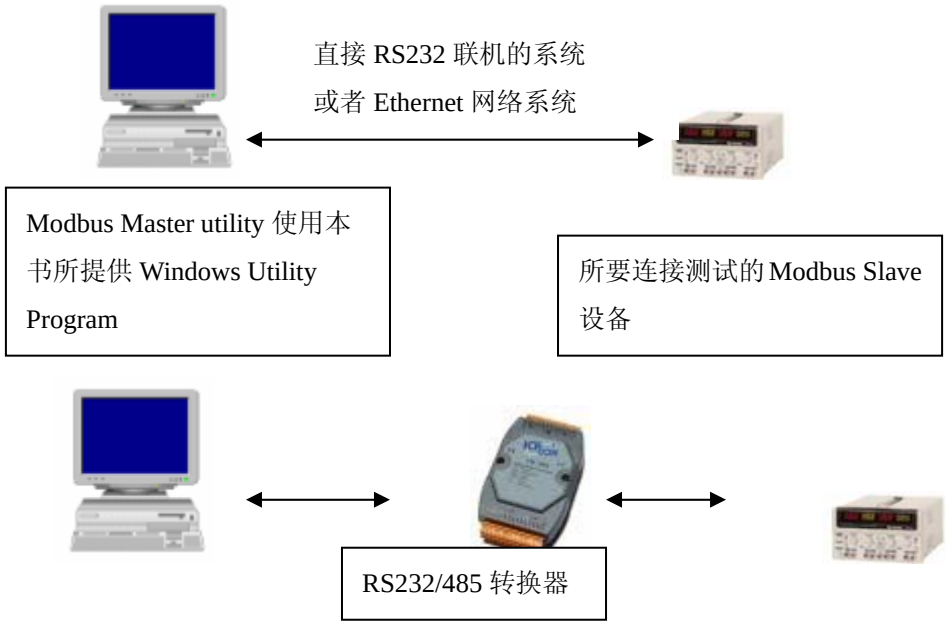
Modbus Master 端：通信 Driver 的通信系数、Modbus Relay/Register 设定、通信硬件建立等是否正确。

Modbus Slave 端：通信 Driver 的通信系数、Modbus Relay/Register 设定、通信硬件建立等是否正确。

两端联机设备的确定：通信线、转换器、Hub、Switch 等。

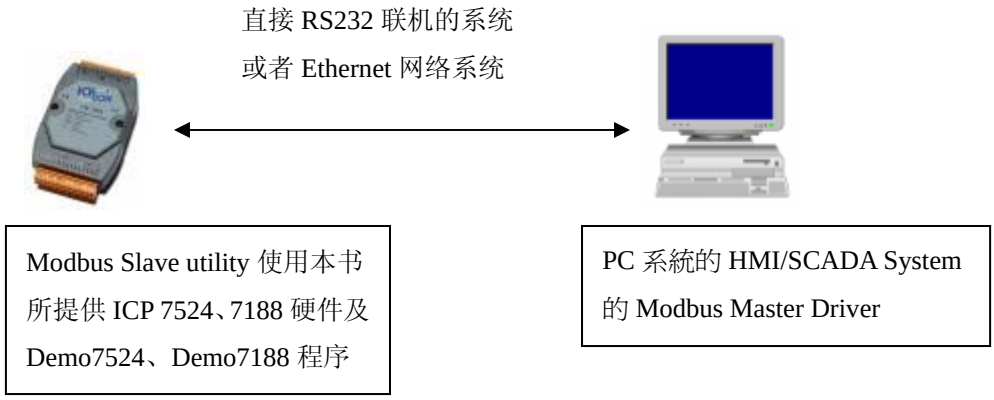
使用 Utility 程序测试系统架构如下各图：

测试 Modbus Slave 设备：例如电表、PLC、PID 控制器等。



图(6-7)：测试架构图(1)

测试 Modbus Master 系统：例如监控系统 Modbus Driver。



图(6-8)：测试架构图(2)

RS485 最后要点：有许多电流表、PID 控制器、温度计、分析仪器…等等以 Modbus 通信协议提供联机资料的设备。都使用 RS485 方式，提供同一网络上多台联机架构，但是其 RS485 的隔离并不十分有效而常常产生 CRC check error。建议使用 RS232/485 转换器，此设备都会提供较佳的隔离效果，然后 Modbus Master 端以 RS232C Port 与此转换器相接，以排除此干扰现象。

2 一些 Modbus 特殊用法

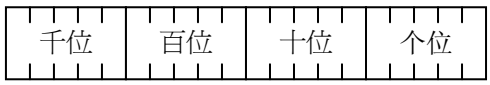
- float、long integer 资料型态：Modbus Protocol 内对于 Register 的数值，是以 16 bits integer 为一个数值的表示，也就是为 32767 ~ －32768 的范围。但是有些时必须使用 float、long integer 等资料型态时，就无法满足需求，例如：PID 控制器所计算的结果大都超出 16 bits integer 数值范围。由 float、long integer 来看都需要使用 32 bits（4 bytes）的资料长度。所以这些控制器就规定一种方式来表达此需求。对于每一个 Register 都是 4 bytes，其 Register Address 都是奇数编号，因为偶数编号已经被占用。举例说明如下：有一种 PID Controller 提供 Register Address 如下表（Modbus Slave Type）

项目	Regsiter Address	Protocol Offset	Data Type
Process Value (PV)	40001	0	float
Set Point (SV)	40003	2	float
Manipulator Value (MV)	40005	4	float
Control Interval (TM)	40007	6	float
:			
etc.			

图(6-9)：Data Type 对照表

Modbus Master Driver 要取入资料，就要奇数开头的 Register Address，如果取入 4 个 Register 就是 16 bytes 资料。然后每 4 bytes 对应一个 Register。

- word swap 要点：另一个 16 bits integer 的使用要点是，Modbus Protocol 规定传送顺序必须将 High Byte 先传，然后再传送 Low Byte。但是有些控制器因为使用 Processor 的不同，可能将 integer 做相反顺序的处理，此时 Modbus Master Driver 就要提供 word swap 的选项功能，将此顺序再转回来。如果此 Register 又是上一点所提到的 4 bytes float、long integer 的资料，更要提供 Byte swap 的功能。
- BCD Code：如果将一个 16 bits integer 内，每 4 bits 都当作一个十进制数，因此总共有四个 4 bits，可以表示至千位数，也就是 0 ~ 9999 的数值，此种方式为 BCD Code。



图(6-10)：BCD Data Type 资料图

3 Modbus 网站

下列三个网站非常重要的 Modbus Protocol 相关网站。

- 因为 Modbus Protocol 已经被许多控制系统当作对外通信的标准通信协议，有一个协会专门制定此标准。

http://www.modbus.org.com/default.htm

- Modbus Protocol 是由 Modicon PLC 所提出的通信标准，此 PLC 厂商网站，当然也非常的重要。

http://www.schneider-electric.com

- OPC 的标准规格，也是由一个 OPC 协会所制定的

http://www.opcfoundation.org

4 Sample Program 目录一览表

存放于光盘片各 Demo Program 的目录如下表：

\Cbuilder50\Modbus_Tool\SRC	Modbus Utility sample program source
\Cbuilder50\Modbus_Tool\Install	Modbus Utility Intsall disk
\Cbuilder50\MB_SUB\SRC	MB_SUB.DLL program source
\ICP\Demo7524	ICP 7524 Modbus sample program source
\ICP\Demo7188	ICP 7188 Modbus sample program source
\ICP\MST7524A	ICP 7524 Modbus ASCII Master/Slave sample program source
\ICP\MST7524R	ICP 7524 Modbus RTU Master/Slave sample program source
\ICP\MST7188	ICP 7188 Modbus TCP Master/Slave sample program source
\OPC\Trial_Modbus	Modbus OPC Trial Version install disk
\OPC\Trial_ModbusTCP	ModbusTCP OPC Trial Version install disk
\VB6\OPCClient_Demo	OPC Client sample program source

图(6-11)：Sample Program 一览表