屏人機 Modbus TCP教程

目的：透過Modbus TCP取得人機的變數值

兩種方式：

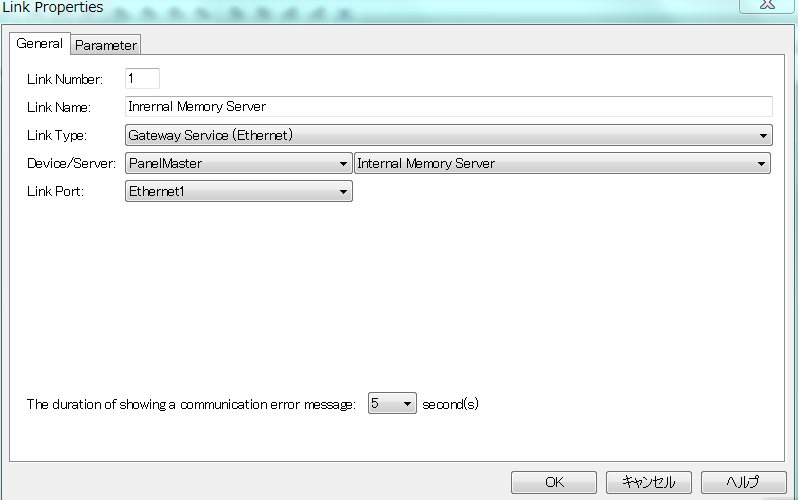
一：兩台人機，一台作為Internal memory server，一台作為Internal memory的client。

二：一台人機作為internal memory server，一台電腦或手機作為client，透過Modbus TCP讀取internal memory server的變數，整合用的。

方式一：兩台人機

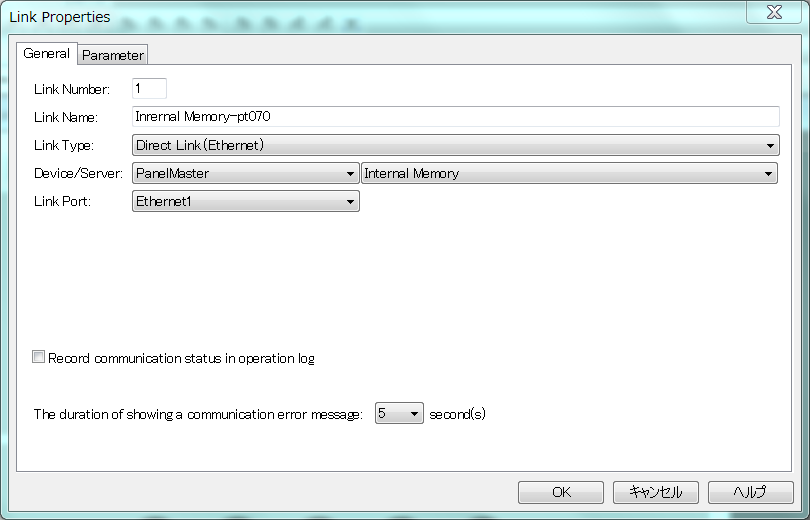
人機設定：

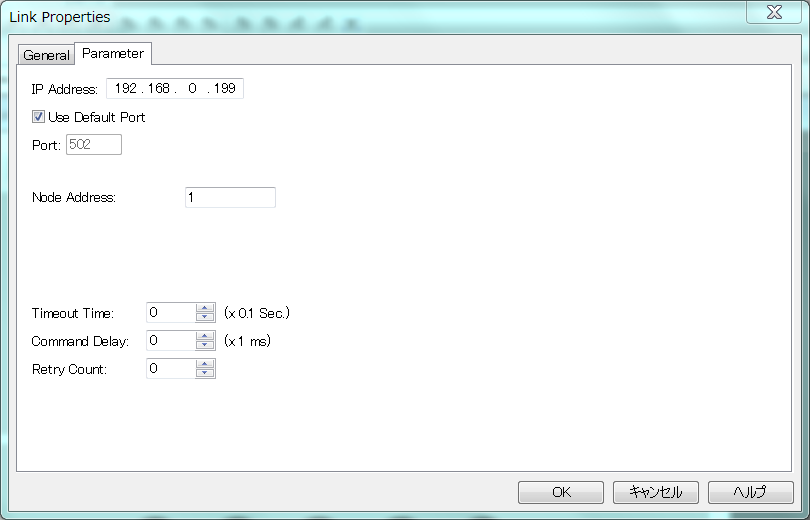
1：Modbus TCP 的Server：在link設定如下：



Server的IP是在開機設定畫面裡面設的。我們設為192.168.0.199

2：Modbus TCP的client：在link的設定如下：





作為client要設定讀取內部變數的server IP位置，也就是192.168.0.199

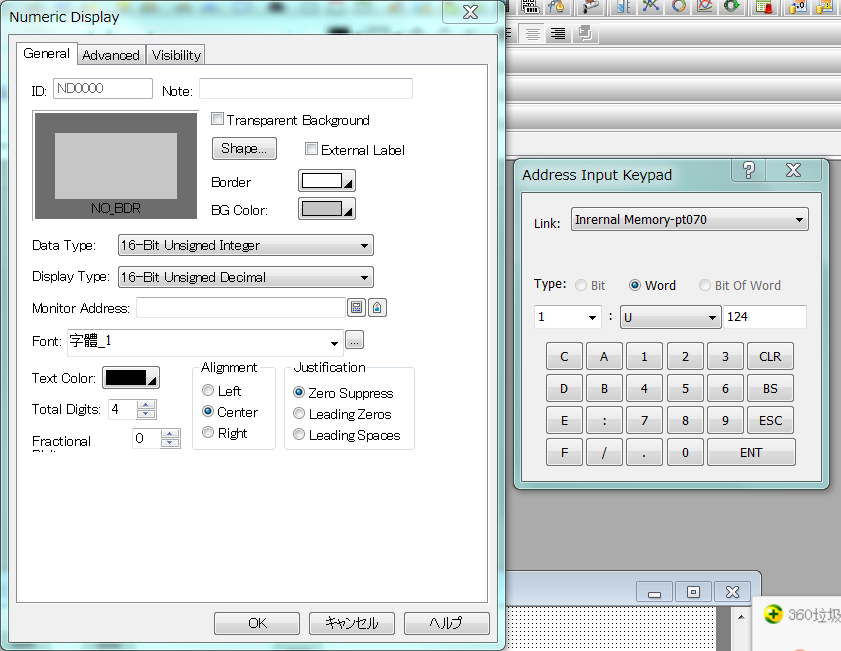
Client當然也要設IP，就設192.168.0.198

設定之後，我們來讀取server的變數。

範例：

Client要讀取server變數 $U124，在client做一個numeric display,如下：

注意：Data Type要和server的變數一樣，還有，link要選internal memory



然後compile，刷人機。Client端就可以讀取server的$U124變數值了

方式二：人機 Internal memory server +電腦

發送modbus 命令 ： **00 00 00 00 00 0a 01** **14 07 00 00 00 00 00 7A 00 02**

說明如下：

1： 紅色粗體字是 MBAP

第一和第二個bytes 0001是Transfer ID，，兩個bytes，我們設為00 00

第三和第四個bytes 0000是Protocol ID ，，兩個bytes，預設為00 00

第五和第六個bytes 000a是Data length（00 0a就是 10個bytes），如果只取一個group，就固定是00 0a。詳細說明看注一

第七個byte是slave address , 我們設為 01

以上就是MBAP header的部分，共7個bytes。接下來就是function code和data

2 function code和data （9個bytes），就是黑色粗體字部分

第一個byte 是function code 20，就是16進位的14

第二個就是第二個byte之後還有幾個bytes，如果只取一個group，就固定是07

第三個是first group的reference type ，我們要取的U變數，是在refernece type 0，所以是 00 ，reference type看注二（在PM Master的help就有此說明）

第四到第七個bytes是reference number，共四個bytes。一樣看注二

第八，九個byte是 word counts，我們取兩個值，所以是 00 02

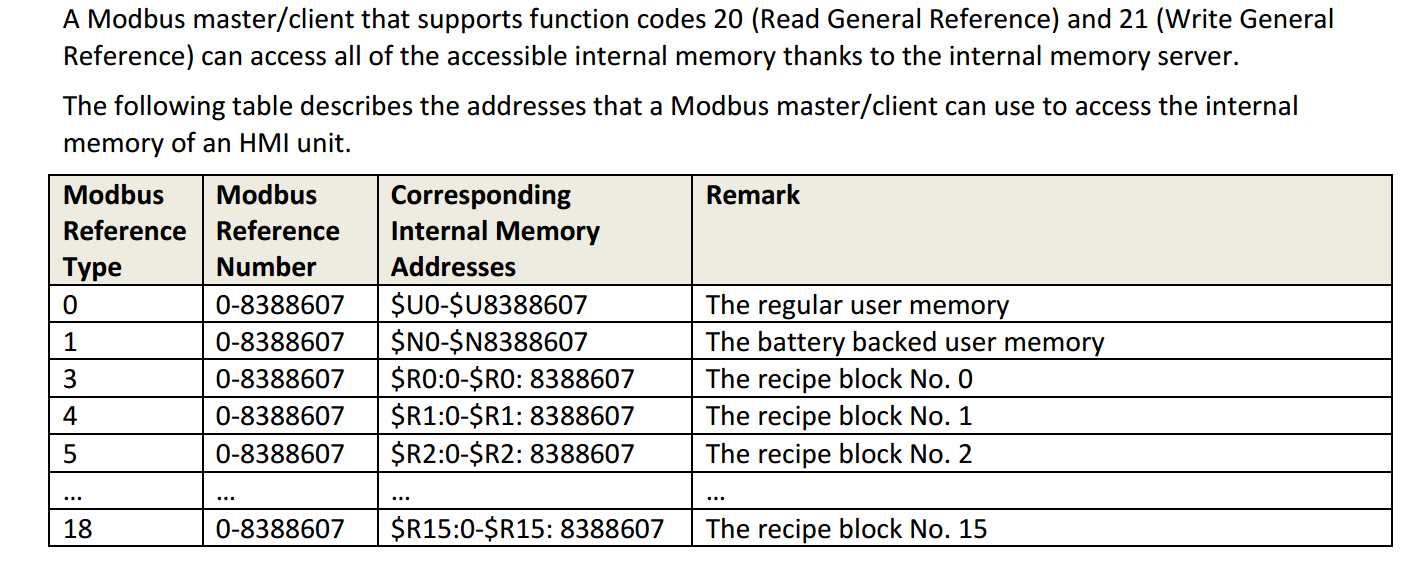
以上共9個bytes

所以發送的modbus TCP控制碼，共16個Bytes

注1：

第五和第六個bytes 000a是Data length（00 0a就是 10個bytes），，兩個bytes，內容是以下這幾個bytes總數相加： Slave address（一個byte 01h），function code（一個byte 14h），byte count (一個byte, byte count 之後的資料長度，7個。所以這個byte的值是07)，Reference Type（一個byte，人機U變數的reference type是00），Reference address（四個byte，就是變數的編號，本範例是取U124，所以值是 00 00 00 7C）, Word count （兩個bytes，我們取兩個word，所以是00 02）

注二：



范例一： 9226 ACCU2取测试区，预热区，预冷区的PV值，SV值

变数名称和资料长度如下：

PV值（2个words，4个bytes）：测试区 $U602, 预热区 $U604, 预冷区 $U606

SV值（1个words，2个bytes）：测试区 $U610, 预热区 $U923, 预冷区 $U924

取三区的PV值：

Modbus TCP 发送： 00000000000a011407000000**025a0006**

红色粗体字的 025A就是取值的开始位置，也就是变数名称 $U602 ,602转换成 hex就是025A、

红色粗体字的 0006，表示从开始取值的位置取6个words，因为每个值是2个words，取3个值就是6个words

Modbus TCP的response：00 00 00 00 00 10 01 14 0D 00 **00 A9 00 00 00 A9 00 00 00 A2 00 00**

红色粗体字共12个bytes，也就是6个words，每两个words是一个值，所以是3个区的PV值，解析如下：

00 A9 00 00 ，其实只用前面2个bytes， 00A9换算成十进位就是 169，除以10就是测试区温度 16.9度C

00 A2 00 00 ，也只用前面两个bytes，00A2换算成10进位就是162 ，除以10，就是预冷区温度16.2度C

參考資料：

1：<http://irtfweb.ifa.hawaii.edu/~smokey/software/about/sixnet/modbus/Modbus_TCP_Standard.doc>

2：wireshark 抓包軟體