

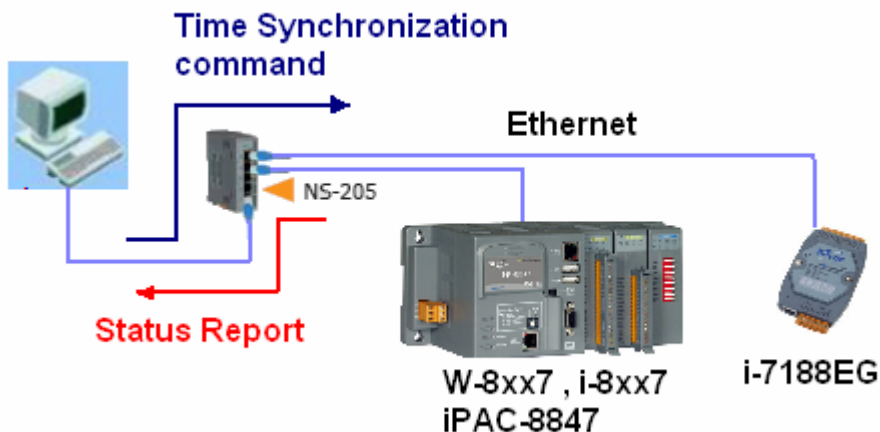
# 如何 自動對多台 ISaGRAF PAC 進行時間校正 與 記錄運作狀態 ？

by chun@icpdas.com

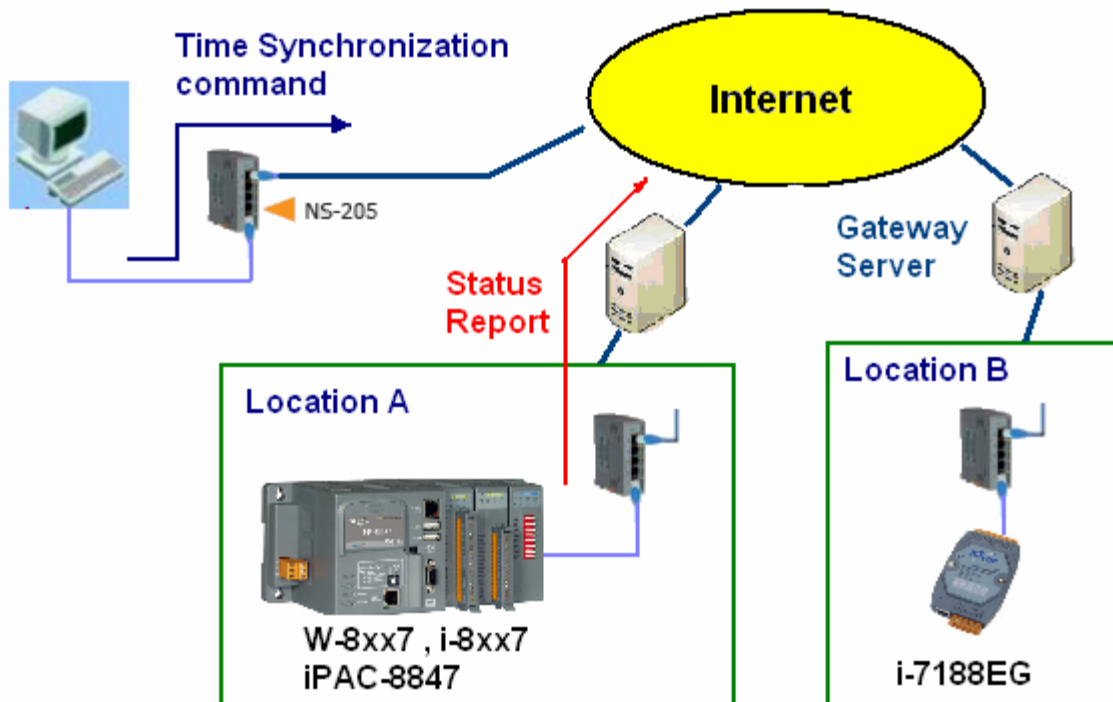
## 1. 基本介紹

本文件所使用的技術與[www.icpdas.com](http://www.icpdas.com) – FAQ – Software – ISaGRAF – 065 所描述的相同. 由 1 台 PC /Server 來接收 1 台或多台 ISaGRAF PAC (i-7188EG, i-8xx7, iPAC-8x47, W-8xx7)用UDP傳過來的狀態回報命令, 之後該PC /Server可適時對每台ISaGRAF PAC進行時間校正.

本範例程式採用一台 PC, IP = 10.0.0.91 , Mask = 255.255.255.0 在同一個區域網路內連接 2 台 ISaGRAF PAC (可選用 W-8xx7, i-8x37, iPAC-8447 / 8847, i-7188EG 的任意 2 台) 來展示 .  
PAC 1 IP = 10.0.0.103 , Mask = 255.255.255.0 , PAC 2 IP = 10.0.0.105 , Mask = 255.255.255.0



本例若要使用在 Internet 上, 此時所用的 PC / Server 必需申請到一個固定的 Internet IP. 位於各地區的 ISaGRAF PAC 必需要能連上網路(一般是透過 ISP 公司的 Gateway Server). 然後每台 ISaGRAF PAC (在本例稱呼為 Local controller) 要設定好 它所使用的 Gateway IP address.



## 2. 安裝測試軟體與硬體

建議將 Controller 的 ISaGRAF driver 更新為以下版本, 才能正確運行本範例.

<http://www.icpdas.com/products/PAC/i-8000/isagraf-link.htm>

i-7188EG:	2.19 版或更高版本
i-8437 / 8837:	3.21 版或更高版本
W-8xx7:	3.38 版或更高版本

請先至 [www.icpdas.com](http://www.icpdas.com) – FAQ – Software – ISaGRAF – 070 下載文件與範例程式.

若要瞭解本demo所使用的UDP通訊規約, 請參考第4節.

本範例Controller 所用的ISaGRAF程式為

PAC 1 : wdmo\_64a.pia (請設好該 PAC 的 IP 為 10.0.0.103 , Mask = 255.255.255.0)

PAC 2 : wdmo\_64b.pia (請設好該 PAC 的 IP 為 10.0.0.105 , Mask = 255.255.255.0)

**注意:** 真正在應用時, PC / Server可能是擺在Internet上, 則Local controller需另外指定 Gateway IP. 此 "Gateway IP" 需指定的值 可在一台與Local controller放在同網域的PC上查到. 方法為把那台PC的IP設為 DHCP (自動取得IP), 之後在它的windows上開啓一個 Command Prompt (命令列視窗), 輸入 ipconfig 如下, 就可查到 該local 網域所用的 Gateway 設定.



```
C:\Documents and Settings\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter 區域連線:

    Connection-specific DNS Suffix  . : banchiao.icpdas.com
    IP Address. . . . .                : 10.0.0.91
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 10.0.0.254

C:\Documents and Settings\Administrator>
```

若本例的 PC 要使用在 Internet 上, 此時所用的 PC 必需申請到一個固定的 Internet IP. 且 ISaGRAF 程式 wdmo\_64a 與 wdmo\_64b 內的 "IP\_correct\_PC" 變數的初值宣告 與 IO connection 內 udp\_ip 內的 "to\_ip1" 的值也要改成那個 Internet IP. 然後要再 Compile 一遍, 才能使用.

接下來請將 wdemo\_64a 下載到 PAC 1， wdemo\_64b 下載到 PAC 2。會看到 ISaGRAF 會顯示如下。

Name	Value	Comment
Year1	2007	
Month1	5	
Day1	30	
Hour1	13	
Minute1	8	
Second1	17	
state1		receiving state information
T1	t#59s374ms	timer to show the time elapse
Report_interval	t#1m	interval to report data to PC / Server, init as 1 minute
Timeout_interval	t#15s	interval that PC/Server must reply, init as 15 seconds
msg1	1001,1863154825,1,2007,5,30,13,8,5,1,999990,99	the sending message
ID_No	1863154825	modified before every sending, init as -1
msg2		the coming message
ip_port	0	UDP_IP port No. of the sender
msg_ip_addr		ip addr of the sender (string format)
R_Command	0	Command in the coming data
<end of list>		

Local Controller的日期, 時間

定期回報的Interval設定 與 時間進度

Msg1 為 Local Controller 傳給 PC / Server 的 Message.  
Msg2 為 PC / Server 回覆給 Local Controller 的 Message  
Msg\_ip\_addr 與 ip\_port 為此 Msg2 的來源 IP 地址與 UDP port 編號, 通常是 PC / Server 的 IP. 若不是 表示有其它人想傳資料 (或攻擊) 給 Local Controller.  
R\_Command 為 PC / Server 回覆給 local controller 的 Command (本範例為 2 或 4)

之後請在 PC 上運行 VB 6.0 demo\_8 程式 (請參考第 3 節)。

### 3. 測試VB 6.0展示程式

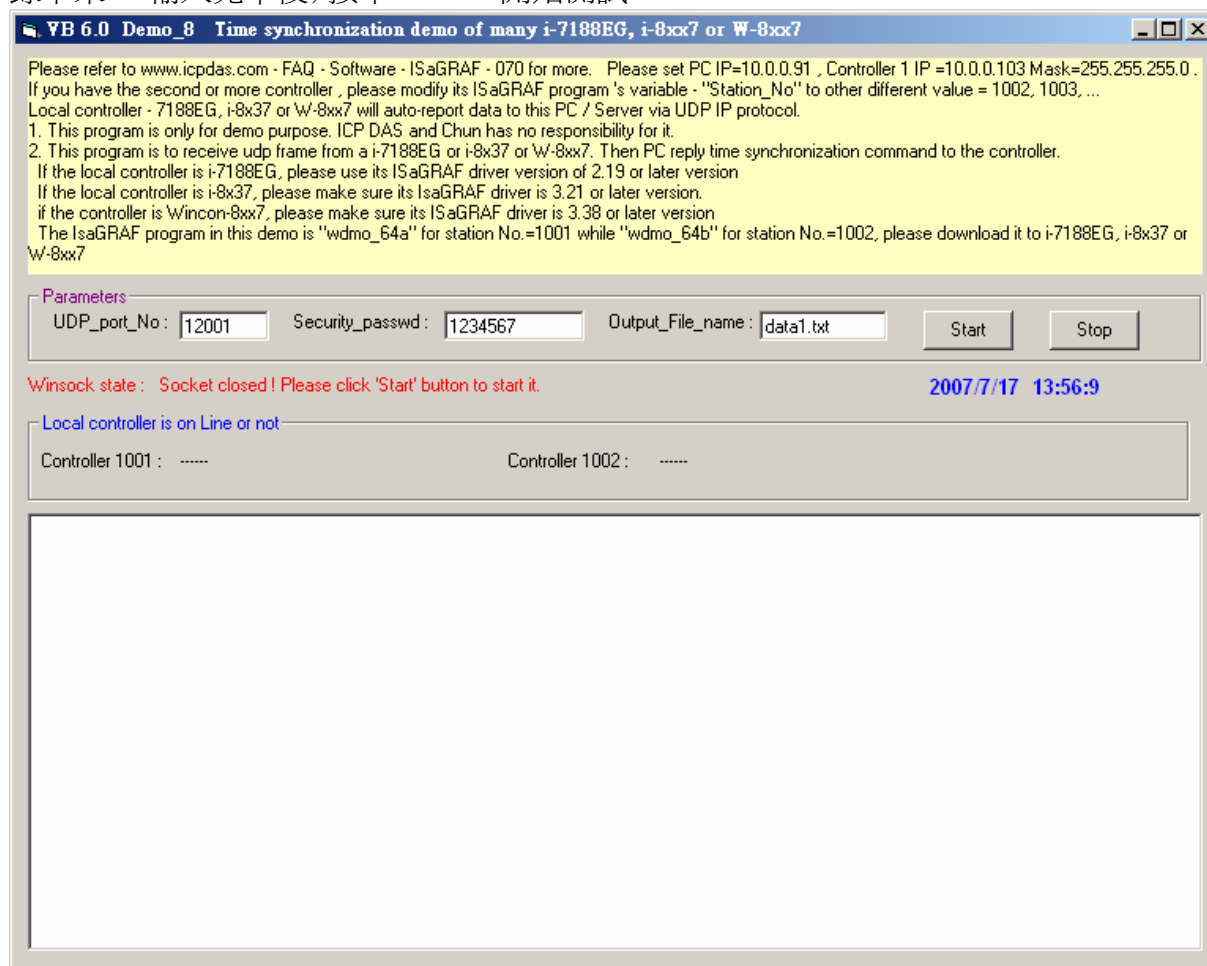
請先完成第2節的動作, 再操作本節的步驟

請將您的測試PC的IP設為Fixed IP = 10.0.0.91 , Mask = 255.255.255.0 才可正確測試本demo程式.  
(因為 Local controller 1 與 2 內Run 的ISaGRAF demo 程式 “wdmo\_64a” 與 “wdmo\_64b” 是將 UDP message 送到 10.0.0.91的那台PC的 UDP port No. = 12001上)

本VB 6.0 測試程式為 demo\_8.exe , 放於 .\vb6\_demo\demo\_8\ 內  
(由[www.icpdas.com](http://www.icpdas.com) – FAQ – Software – ISaGRAF – 070 下載 來的)  
Source code 請用VB 6.0軟體開啓 .\vb6\_demo\demo\_8\demo\_8.vbp

此demo\_8.exe 需在PC內 windows 2000, XP 或相容的OS內來 運行它.  
運行起來後會顯示如下視窗.

“UDP\_port\_No” 為要開啓那個UDP port來接收資料 (可以是1001 ~ 65535), 本demo使用12001  
“Security\_passwd” 為資料的“安全密碼”, 可以是0, 1 ~ 2147483647或-2147483647 ~ -1間的1個值.  
本demo使用1234567  
“Output\_File\_name” 為選項, 可以不指定. 若有指定一個 file name 則會建立一個新file, 把資料記錄下來. 輸入完畢後, 按下 “Start” 開始測試.

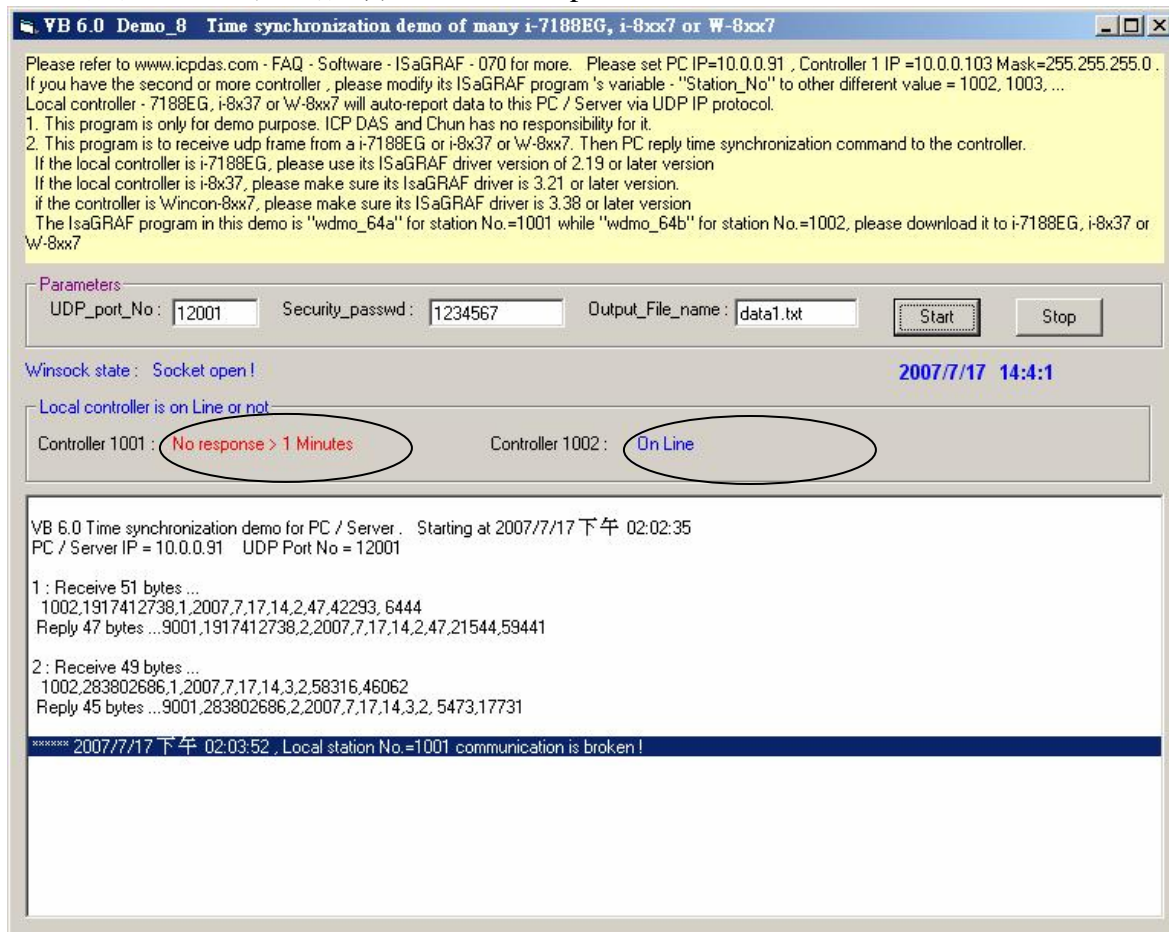


如何測試？

本demo在以下狀況發生時，Local controller會傳送資料到 PC / Server

1. PAC 1 或 PAC 2開機後 過了15秒，各會傳送一次。(這個只會傳一次)
2. 開機後 每經過 1 分鐘會傳送一次。(這個會週期性的一直傳)

A. demo\_8.exe 運行起來後，觀察 2 分鐘. 若 PAC 1 與 PAC 2 連線正常，會顯示 “On Line”，超過 1 分鐘以上沒有回報 會顯示 “No response ...”



B. 請調整這台 PC / Server 的時間，比如往後調 2 個小時，等約 1 分鐘後，會發現這 2 台有連上線的 PAC 會跟著把時間調整為跟 PC / Server 一樣的時間。每當 PAC 送資料給 PC 時，PC 會比對時間差，若時間差超過 20 秒，就會下達時間校正的命令給 PAC。如果本應用是放在區域網路內，可以將這個容許的時間差調小，比如由 20 秒調整為 5 秒，方法為把 VB 6.0 demo\_8 的程式內的  
If Temp > 20 Or Temp < -20 Then 那行改為  
If Temp > 5 Or Temp < -5 Then

C. 請觀察是否每經過一分鐘都會收到一個 Message.

## 4. 本範例所使用的UDP通訊規約說明

本規約適用於 ISaGRAF demo 程式 - wdm0\_64a , 與 wdm0\_64b 與PC上的 VB 6.0 – demo\_8 程式

1. Local Controller 為UDP Client , PC / Server 為 UDP Server. 只有Local Controller 會主動傳送資料給 PC / Server (ISaGRAF 程式 wdm0\_64a 與 wdm0\_64b 內的 Message 變數 “IP\_correct\_PC” 與 Integer 變數 “Port\_correct\_PC” 就是定義要傳到那個IP的 PC / Server 的那個 UDP Port, 還有 IO connection 內 “udp\_ip” 內也有定義).
2. PC 在收到 Controller 傳來的一筆資料後, 必需在15秒內回覆 <Command> = 2 或4給 Controller. 正確的回覆資料內的 <ID No.> 需跟 收到的資料內的 <ID No.> 一樣. 若不一樣, Controller 會認定該回覆資料的格式是錯的. 若 Controller 等待超過15秒沒收到PC / Server 的正確回覆資料, 會再傳送一次, 之後若等待超過15秒沒收到回覆, 會再傳一次, ... (ISaGRAF 程式 wdm0\_64a 與 wdm0\_64b 內的 Timer 變數 “Timeout\_interval” 就是定義這個 Timeout 時間)
3. 本demo 在以下狀況發生時, Local controller 會傳送資料到 PC / Server
  - A. Local controller 開機後 過了15秒, 會傳送一次. (這個只會傳一次)
  - B. 開機後 每經過 1 分鐘會傳送一次. (這個會週期性的一直傳, ISaGRAF 程式 wdm0\_64a 與 wdm0\_64b 內的 Timer 變數 “Report\_interval” 就是定義這個週期時間)
4. Local Controller 傳送給 PC / Server 的資料格式定義

Security\_passwd: 需在 ISaGRAF IO connection – “udp\_ip” 內定義 及 PC 的 VB demo 程式內也需指定成相同值才能正確通信. 值可是 0: 表示傳遞的資料不加密(不安全), 或 1 ~ 2147483647 或 -2147483647 ~ -1 間的1個值 (非0值, 較安全), 表示傳遞的資料要經過加密手續

設為非0值, 加密演算法請參考 VB 6.0 demo\_8 內的 “convert\_to\_udp\_deliver\_buf( )”, “convert\_back\_udp\_deliver\_buf( )” 與 “udp\_ip\_crc( )”

若設 Security\_passwd 為0, 每個傳遞的UDP Message 最多不可超過255個byte.

若設 Security\_passwd 為非0, 每個傳遞的UDP Message 最多不可超過259個byte. 最後那4個byte 為 <4-byte-Checksum >, 是用 “udp\_ip\_crc( )” 算出來的.

Local Controller 傳送給 PC / Server 的資料格式

Security\_passwd 為0: (最後方不需加 4-byte-Checksum)

<Station\_No of local controller>, <ID No.>, <Command>,  
<Year>, <Month>, <Day>, <Hour>, <Minute>, <second>,  
<User-defined CRC>



例如:

1001,850334470,1,2007,5,30,17,31,51,46677,18632

表示:

<Station\_No of local controller> 爲 1001

<ID No.> 爲 850334470

<Command> 爲 1

Controller的時間爲 2007/5/30, 17:31:51

< User-defined CRC > 爲 46677,18632

Security\_passwd 不爲0: (最後方 要加 4-byte-Checksum)

<Station\_No of local controller>,<ID No.>,<Command>,  
<Year>,<Month>,<Day>,<Hour>,<Minute>,<second>,  
<User-defined CRC><4-byte-Checksum>

<Command> 的定義:

1 : Local Controller傳送資料給 PC / Server

<User-defined CRC> 的定義:

可由User自行設計 演算法. 本demo採用以下的演算法  
(真正應用時, 爲了安全, 請 自行設計 不同的演算法)

值固定爲11個字 (Character), 包含2個0到65535的值, 中間加一個逗號 “,”

例如:

value_1	value_2		值固定爲11個字 (Character)
0	0	:	' 0, 0' ('0'前面有4個 Space字元)
1	1	:	' 1, 1' ('1'前面有4個 Space字元)
21	21	:	' 21, 21' ('2'前面有3個 Space字元)
321	321	:	' 321, 321' ('3'前面有2個 Space字元)
4321	4321	:	' 4321, 4321' ('4'前面有1個 Space字元)
54321	65535	:	'54321,65535' (沒有Space字元)

本例, value 1的算法如步驟 (a) 到 (d), 步驟 (e) 爲value 2的算法  
(真正應用時, 爲了安全, 請 自行設計 不同的演算法)

(a) 將收到的UDP Message刪除 <User-defined CRC> 11個byte 與 <4-byte-Checksum> 4個byte, 然後存成N個byte的Array (爲了方便表示, 稱呼此byte Array爲 user\_buf[ ])

(b) 取代 user\_buf[3] 爲 user\_buf[3] xor 100

用c語言來算 爲 user\_buf[3] = user\_buf[3] ^ (unsigned char)100 ;

(真正應用時, 爲了安全, 請 自行設計 不同的演算法)

- (c) 取代 user\_buf[7] 為 user\_buf[7] xor 200  
用c語言來算 為 user\_buf[7] = user\_buf[7] ^ (unsigned char)200 ;  
(真正應用時, 為了安全, 請 自行設計 不同的演算法)
- (d) 用CRC-16演算法, 算出user\_buf[0] ~ user\_buf[N-1] 的 <CRC\_Hi><CRC\_Lo> 值  
如此得到value\_1 = 256\*<CRC\_Hi> + <CRC\_Lo>. 它是一個0 ~ 65535 間的值.
- (e) 使用不同的演算法來求出value\_2  
做步驟(a), 然後做步驟(b) 但改爲 user\_buf[4] = user\_buf[4] ^ (unsigned char)48 ,  
做步驟(c) 但改爲 user\_buf[6] = user\_buf[6] ^ (unsigned char)197, 最後做步驟(d).  
如此得到value\_2 = 256\*<CRC\_Hi> + <CRC\_Lo>. 它是一個0 ~ 65535 間的值.

## 5. PC / Server回覆給Local Controller的資料格式定義

Security\_passwd: 與前一條 4. 的定義相同.

PC / Server回覆給Local Controller的資料格式

Security\_passwd 為0: (最後方 不需加 4-byte-Checksum)

<Station\_No of PC/Server>,<Same ID No. from the local controller>,<Command>,  
<Year>,<Month>,<Day>,<Hour>,<Minute>,<second>,  
<User-defined CRC>

例如:

9001,519805546,2,2007,5,30,18,59,53, 6830,42679

表示:

< Station\_No of PC/Server > 為 9001

<ID No.> 為 519805546

<Command> 為 2

PC/Server的時間為 2007/5/30 , 18:59:53

< User-defined CRC > 為 6830,42679 (最前方那個 '6' 前面有一個 Space字元)

Security\_passwd 不為0: (最後方 要加 4-byte-Checksum)

<Station\_No of PC/Server>,<Same ID No. from the local controller>,<Command>,  
<Year>,<Month>,<Day>,<Hour>,<Minute>,<second>,  
<User-defined CRC><4-byte-Checksum>

<Command> 的定義:

2: 告知 controller, PC已收到Controller傳來的正確資料

4: 告知Local Controller, 它的時間與 PC的時間相差超過20秒, 請controller校對時間  
之後請再重傳資料一次

<User-defined CRC> 的定義: 與前一條 4. 的定義相同.



## 5. Controller 網路安全防護

### 5.1 : Modbus TCP/IP 安全防護

有幾種方式可以經由以太網路來存取Wincon-8xx7內的資料.

1. 使用Modbus TCP通訊規約, Port編號502. (ISaGRAF軟件與SCADA / HMI就是這樣連的)
2. 使用ftp (比如在PC上執行Internet Explorer, 鍵盤輸入“ftp://10.0.0.103”)
3. 使用telnet (比如在PC上開啓一個“Command”視窗, 鍵盤輸入“telnet 10.0.0.103”)
4. 使用Web server (Wincon的Web HMI功能使用的方式)

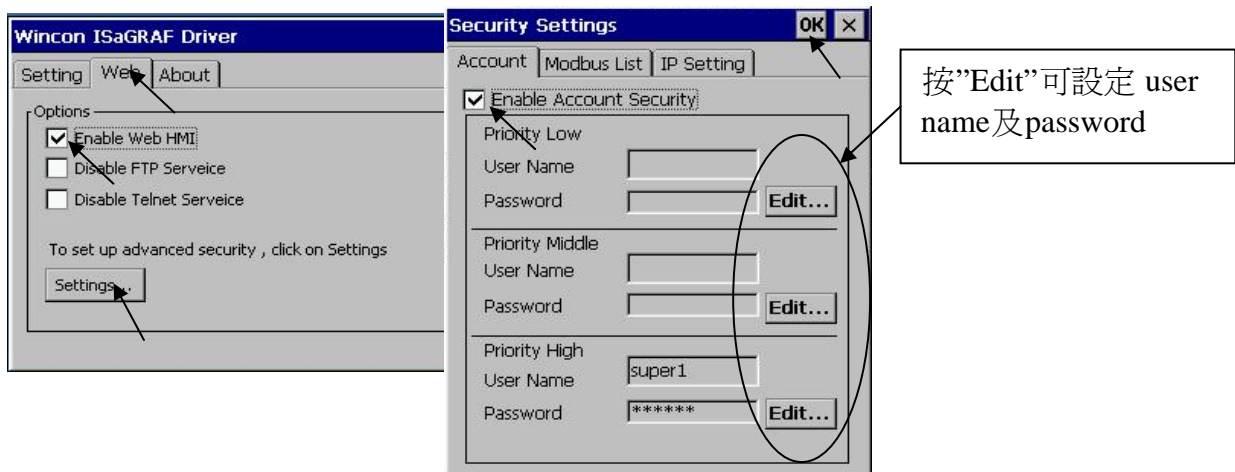
注意:

1. 若是使用I-8xx7與I-7188EG, 只有方式1可使用.
2. 若是使用W-8047 / 8347 / 8747 / 8046 / 8346 / 8746, 要使用“ftp”, “telnet”, “Web HMI”與“Modbus TCP/IP”, 請連您的PC/HMI到其上的LAN1網口, 並且請使用ICP DAS的Industrial Ethernet Switch產品“NS-205”或“NS-208”.

為了安全, 您可以開啓Wincon驅動程式的對話框, 關閉第2及第3項功能, 如下.

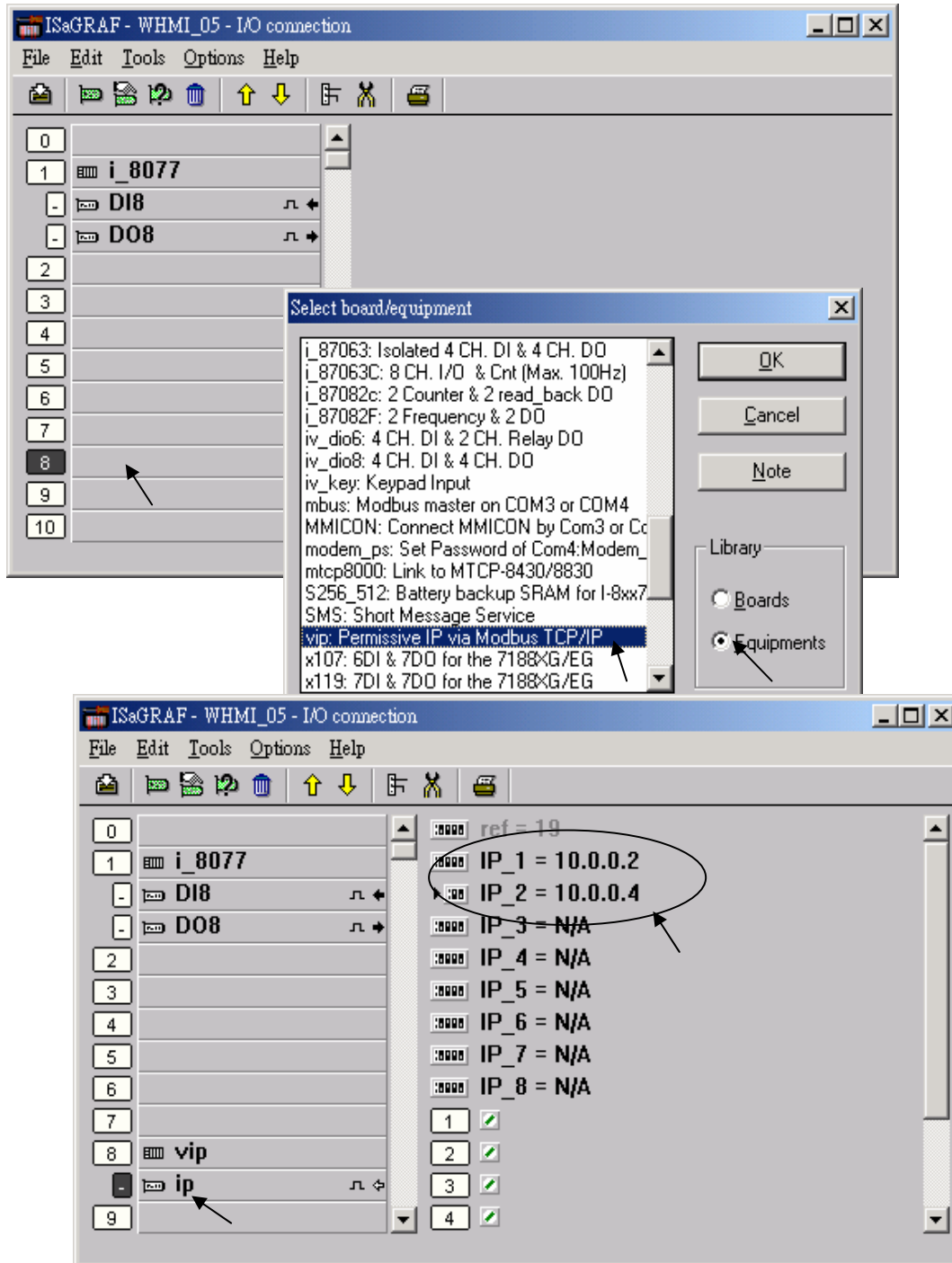


關於第4項, 請設好必要的User name及Password來保護.



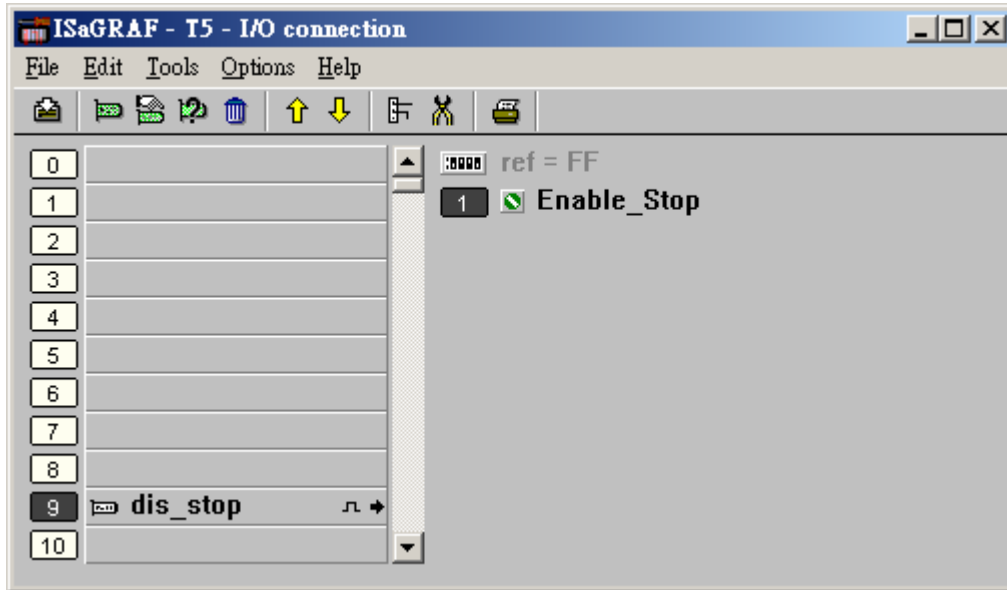
關於第一項 Modbus TCP/IP 的保護, 使用者可以在 i-7188EG, i-8x37與W-8xx7等控制器上設定最多只開放到8組PC / SCADA / HMI 的IP可允許連進來, 方法如下.

請在 ISaGRAF I/O連結視窗內 使用“vip” 虛擬板卡. 最多可設立8組IP允許用Modbus TCP/IP 通訊規約連進來.若控制器內沒有使用“vip”,那表示, 任何IP都允許用 Modbus TCP/IP 連進來. 如果使用了“vip” 但都設為“N/A” 將沒有任何 IP 允許用 Modbus TCP/IP 連進來. (包含 ISaGRAF也連不進來)



## 5.2 : 使用 dis\_stop 虛卡 來 關閉 / 開啓 ISaGRAF Download 程式功能

有時當 i-7188EG , I-8x37 與 W-8xx7 程式開發完, 爲了預防 被人誤用 或故意 使用ISaGRAF 從 Local 或Internet來將 Program Stop, 可以連接 Dis\_stop 虛卡, 將該輸出點的 初值 設爲TRUE, 就可防止被人使用 ISaGRAF 將程式 Stop.



若是需要再啓用它, 請先用原來的 ISaGRAF 程式 連上 controller後, 將 該輸出點 設爲 False. 如此就可 download 修改後的 ISaGRAF程式進去.