FATEK[®]

永宏 Binary 通訊手冊

編輯歷史

版本	韌體版本	修改日期	人員	描述
V_1.0		2024/12/06	Eric	初版

目錄

主僕定位與通訊互動關係	4
永宏 PLC 通訊訊息格式	5
命令碼	.10
命令碼 40 PLC 狀態讀取	.10
命令碼 41 PLC RUN/STOP	
命令碼 42 單一個單點運作控制	.19
命令碼 43 多個連續單點之抑/致能狀態讀取	.24
命令碼 44 多個連續單點狀態(Data)讀取	
命令碼 45 多個連續單點狀態(Data)寫入	
命令碼 46 多個連續暫存器資料(Data)讀取	
命令碼 47 多個連續暫存器資料(Data)寫入	.49
命令碼 48 多個任意單點狀態或暫存器資料(Data)混合讀取	
命令碼 49 多個任意單點狀態或暫存器資料(Data)混合寫入	
命令碼 4E 測試回傳	.72
表格	

主僕定位與通訊互動關係

本通訊協定是建立在任何設備只要可以符合其通訊訊息格式,並使用相同的通訊參數溝通,任何設備皆可與 M 系列 PLC 通訊, M 系列 PLC 會作為僕系統與主系統通訊。

通訊時將為主系統向 M 系列 PLC 傳送命令,如果符合訊息格式 PLC 將會回覆訊息。如下圖:



M 系列通訊孔支援 Type C 、COM1 與 COM2,及 TCP/IP 通訊。

永宏 PLC 通訊訊息格式

● 其中使用時主站發送的命令訊息格式如下:

命令訊	開頭字	有效封	訊息長	訊息內	偵誤值		結尾字元	
息段落	元	包編號	度	容	(Checksum)			
訊息內	0x51	0x10 ,	N(基於	M(基於	將"訊息	息長度"	0x55+	
容		固定給	訊息長	所下達	與訊息	内容作	0xAA	
		Binary	度而有	的命令	CRC16-I	Modbus		
		通訊協	所不同)	及其內	校驗計	算後產		
		定使用		容而不	生的校	驗碼,		
		的		同。)下	依序產	生。		
				個小節	Hight	Low		
				將會解	byte	byte		
				釋訊息				
				結構。				
訊息長	1	1	2	М	2		2	
度(單								
位:Byte)		_						
★ 依序發送 ★								

開頭字元: 命令與回應訊息的開頭字元不同,命令的開為"0x51"(16 進制), M PLC 將以此為判知傳輸資料之開頭。

> 最後送出

有效封包編號: Binary 通訊協定的編號固定為 0x10。

訊息長度: 以訊息內容的有幾個 Bytes 的長度。

最先發出 一

訊息內容: 通常會包含僕站編號、命令碼與傳送資料,其內容會根據不同指令而 有所變化,可以參考後續指令介紹與範例。 **偵誤值:** M 系列 PLC 使用 CRC 校驗的 CRC16-Modbus 做校驗,將"訊息長度"與"訊息內容"作 CRC16-Modbus 校驗計算後產生的校驗碼,並依序產生 Hight byte +Low byte。

其詳細算法如下:

- 1. 將 crc 計算輸出變數設為 OxFFFF 的初始值 (2bytes)
- 2. 使用愈計算的 1 byte 的資料跟 crc 輸出變數的低位元 byte 進行 xor 運算
- 3. 製作 FOR 迴圈,對 crc 輸出變數的 LSB 做檢查,總共 8 次,當最右的 LSB 為 1 時,將 crc 輸出變數右移一位,並和 0xA001 做 xor 運算;當最右的 LSB 為 0 時,則將 crc 輸出變數右移一位。
- 4. 完成此 byte 的 crc 運算,回到第二步取出下個資料 byte 繼續進行 crc 運算,直到完成所有資料 byte。
- 5. 對調 crc 輸出變數的高低 byte,此即為檢查碼。

結束字元: 命令與回應訊息的結束字元相同,為"0x55" (16 進制)、"0xAA" (16 進制), M PLC 將以此為判知傳輸資料之結束。

● 其中使用時僕站接收到命令後,回覆的訊息格式如下:

命令訊	開頭字	有效封	訊息長	訊息內	CRC 較驗碼	結尾字元	
息段落	元	包編號	度	容			
訊息內	0x52	0x10 ,	N(基於	M(基於	將"訊息長度"	0x55+	
容		固定給	訊息長	所下達	與訊息內容作	0xAA	
		Binary	度而有	的命令	CRC16-Modbus		
		通訊協	所不同)	及其內	較驗計算後產		
		定使用		容而不	生的較驗碼,		
		的		同。) 下	依序產生		
				個小節	Hight byte		
				將會解	+Low byte		
				釋訊息			
				結構。			
訊息長	1	1	2	М	2	2	
度(單							
位:Byte)							
	依序發送						
最先發出							

開頭字元: 命令與回應訊息的開頭字元不同,命令的開為"0x52"(16 進制), M PLC 將以此為判知傳輸資料之開頭。

有效封包編號: Binary 通訊協定的編號固定為 0x10。

訊息長度: 以訊息內容的有幾個 Bytes 的長度。

訊息內容: 通常會包含僕站編號、命令碼與傳送資料,其內容會根據不同指令而 有所變化,可以參考後續指令介紹與範例。 **偵誤值:**M 系列 PLC 使用 CRC 校驗的 CRC16-Modbus 做校驗,將"訊息長度"與"訊息內容"作 CRC16-Modbus 校驗計算後產生的校驗碼,並依序產生 Hight byte +Low byte。

其詳細算法如下:

- 1. 將 crc 計算輸出變數設為 0xFFFF 的初始值 (2bytes)
- 2. 使用愈計算的 1 byte 的資料跟 crc 輸出變數的低位元 byte 進行 xor 運算
- 3. 製作 FOR 迴圈,對 crc 輸出變數的 LSB 做檢查,總共 8 次, 當最右的 LSB 為 1 時,將 crc 輸出變數右移一位,並和 0xA001 做 xor 運 算;

當最右的 LSB 為 O 時,則將 crc 輸出變數右移一位。

- 4. 完成此 byte 的 crc 運算,回到第二步取出下個資料 byte 繼續進行 crc 運算,直到完成所有資料 byte。
- 5. 對調 crc 輸出變數的高低 byte,此即為檢查碼。

結束字元: 命令與回應訊息的結束字元相同,為"0x55" (16 進制)、"0xAA" (16 進制), M PLC 將以此為判知傳輸資料之結束。

● 發送的命令訊息內容與格式如下:

訊息段落	僕站站號	命令碼	傳送資料
訊息內容	N(0x00 為廣	請參考後續指	隨命令而已不
	播,0x01~0xEF	令,編號為	同,將在指令章節
	為有效站號)	0x40~0x4E	介紹。
訊息長度(單位:Byte)	1	1	М

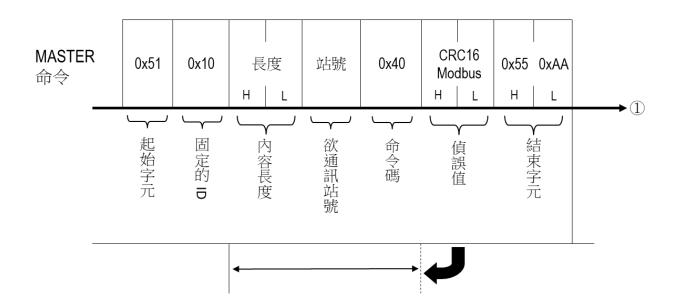
● 接收後發送的回覆訊息內容與格式如下:

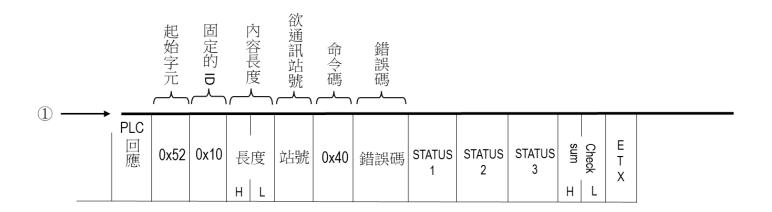
訊息段落	僕站站號	命令碼	錯誤碼	傳送資料
訊息內容	N(0x00 為	請參考後續	可以參考指	隨命令而已不
	廣播,	指令,編號	令章節或頁	同,將在指令章
	0x01~0xEF	為	尾表格	節介紹。
	為有效站號)	0x40~0x4E		
訊息長度(單	1	1	1	M
位:Byte)				

命令碼

命令碼 40 PLC 狀態讀取

如果 PLC 配備記憶卡且設定了 ID,且正常情況下 PLC 狀態為 "RUN"條件下,MASTER 讀取的 PLC 系統狀態如下:(B5、B3、B0 均為 1,其他均為 0 即 STATUS 為 29





● 發送命令如下:

命令訊	開頭	有效封	訊息長	訊息內	7容	CRC 較驗碼	結尾字
息段落	字元	包編號	度				元
訊息內	0x51	0x10 ,	0x00	僕站	命令	將("訊息長	0x55+
容		固定給	+0x02	站號	碼:0x40	度"+"訊息內	0xAA
		Binary				容")做	
		通訊協				CRC16-Modbus	
		定使用				計算依序產生	
		的				的 Hight byte+	
						Low byte	
訊息長	1	1	2	1	1	2	2
度(單							
位:Byte)							
範例:	0x51	0x10	0x00	0x01	0x40	0xA1+0x 84	0x55+
僕站站			+0x02				0xAA
號:01							

● 接收並回覆的訊息如下:

回覆訊	開	有效	訊息	訊息	内容			CRC 較驗碼	結尾
息段落	頭	封包	長度						字元
	字	編號							
	元								
訊息內		0x10 ,	0x00	僕	命令	錯	狀態	將("訊息長	0x55
容	0x5	固定	+0x0	站	碼:0x4	誤	碼	度"+"訊息內	+
	2	給	6	站	0	碼		容")做	0xAA
		Binary		號				CRC16-Modb	
		通訊						us 計算依序	
		協定						產生的 Hight	
		使用						byte+ Low	
		的						byte	
訊息長	1	1	2	1	1	1	3	2	2
度(單									
位:Byt									
e)									
範例:	0x5	0x10	0x00	0x0	0x40	0x0	0x01	0xD5+0x 55	0x55
僕站站	2		+0x0	1		0	+x0x0		+
號:01			6				0		0xAA
							+0x00		

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC, PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

● 狀態碼(3 Byte):

回覆訊息段	狀態碼 1	狀態碼 2	狀態碼 3
落			
訊息內容	B0: RUN	保留	保留
	1;STOP:0		
	B1: Battery		
	Low		
	B2: 階梯圖		
	Check sum 錯		
	誤 1;正常:0		
	B3: 是否插入		
	SD 卡		
	B4: 看門狗超		
	時 1;正常:0		
	B5: ID 為預設		
	1;ID 不為預		
	設:0		
	B6: 緊急停止		
	1;正常:0		

命令碼 41 PLC RUN/STOP

控制 PLC RUN 或 STOP。

● 訊息內容

(1) 發送

STN(1) CMD(1) CTRL(1)

(2) 回覆

STN(1) CMD(1) ERR(1)

參數	描述	值		
CTRL		00H: Stop		
	控制碼	01H: Run		

● 範例

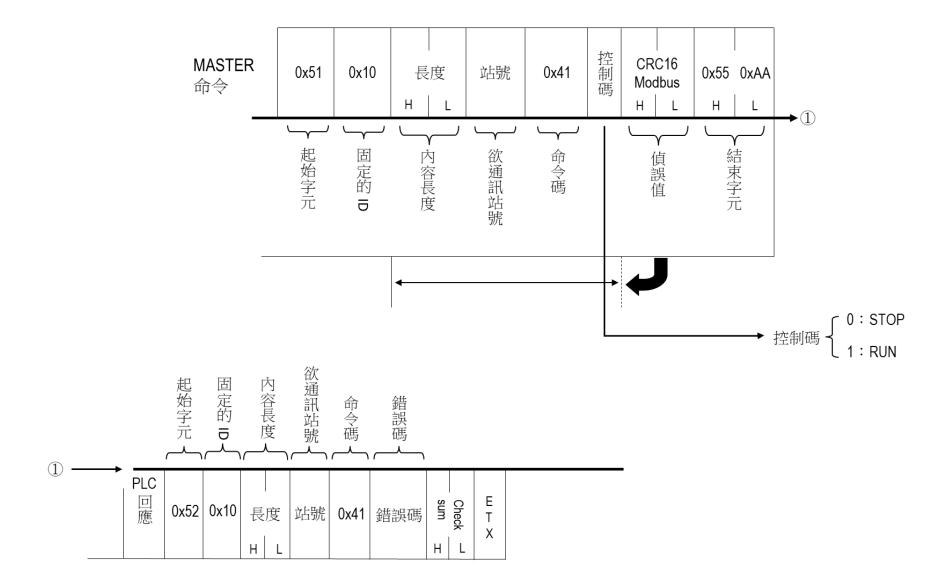
將 PLC 切至 "Run"

(1) 發送

01H 41H 01H

(2) 回覆

01H 41H 00H



● 發送命令如下:

命令訊	開頭	有效封	訊息	訊息区	内容		CRC 較驗碼	結尾
息段落	字元	包編號	長度					字元
訊息內		0x10 ,	0x00	僕	命令	控	將("訊息長	0x55+
容	0x51	固定給	+0x03	站	碼:0x41	制	度"+"訊息內	0xAA
		Binary		站		碼:	容")做	
		通訊協		號			CRC16-Modbus	
		定使用					計算依序產生	
		的					的 Hight byte+	
							Low byte	
訊息長	1	1	2	1	1	1	2	2
度(單								
位:Byte)								
範例:	0x51	0x10	0x00	0x01	0x41	0x00	0x45+0x D4	0x55+
僕站站			+0x03					0xAA
號:01、								
PLC								
STOP								

● 控制碼(1 Byte):

回覆訊息段落	控制碼
訊息內容	0x00 : STOP
	0x01 : RUN

● 接收並回覆的訊息如下:

回覆訊	開	有效封	訊息	訊息	内容		CRC 較驗碼	結尾
息段落	頭	包編號	長度					字元
	字							
	元							
訊息內		0x10 ,	0x00	僕	命令	錯誤	將("訊息長	0x55+
容	0x52	固定給	+0x03	站	碼:0x41	碼	度"+"訊息內	0xAA
		Binary		站			容")做	
		通訊協		號			CRC16-Modbus	
		定使用					計算依序產生	
		的					的 Hight byte+	
							Low byte	
訊息長	1	1	2	1	1	1	2	2
度(單								
位:Byte)								
範例:	0x52	0x10	0x00	0x01	0x41	0x00	0xD4+0x 55	0x55+
僕站站			+0x03					0xAA
號:01、								
PLC								
STOP								

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC, PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

命令碼 42 單一個單點運作控制

此指令可以控制指定的單點做致能、抑能、設定、清除四種運作。

● 訊息內容

(1) 發送

STN(1) CMD(1)	CTRL(1)	TYPE(x)	ADDR(2)
---------------	---------	---------	---------

(2) 回覆

STN(1)	CMD(1)	ERR(1)
J - 1 - 1 (±)	C.V.D(±)	

參數	描述	值
		01H: 抑能
₩₩ 4 .1	控制碼	02H: 致能
控制		03H: 設定
		04H: 清除
類型	資料類型	參考末頁表格 1
地址	資料地址	

● 範例

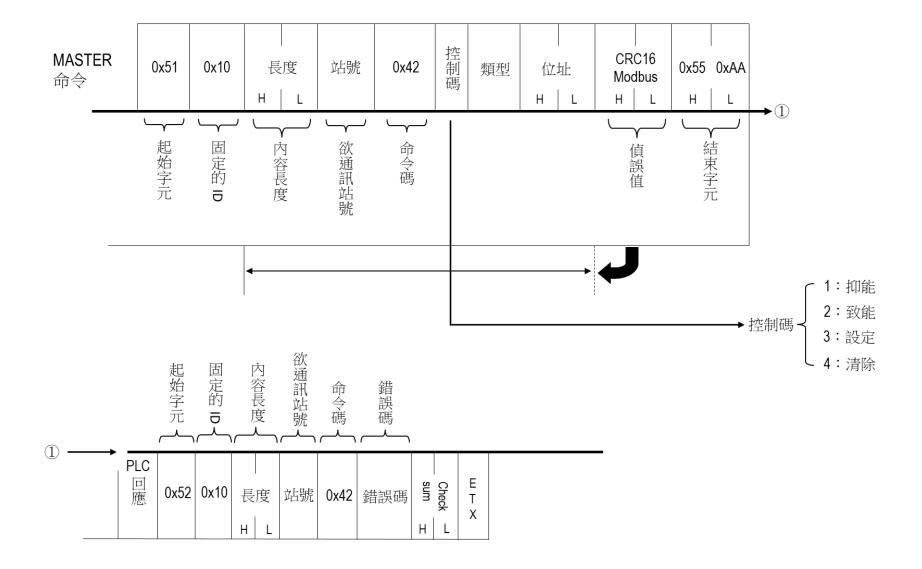
以下是抑能 X16 的通訊格式範例

(1) 發送

01H	42H	01H	58H	00H	10H
				\uparrow	
				X16	

(2) 回覆

01H	42H	00H
-----	-----	-----



● 發送命令如下:

命令	開	有效	訊息	訊息	内容				CRC 較驗碼	結
訊息	頭	封包	長度							尾
段落	字	編號								字
	元									元
訊息		0x10	1+1+	僕	命令	控	類	單	將("訊息長	0x55
內容	0x5	,	1+類	站	碼:0x	制	型	點	度"+"訊息	+
	1	固定	型長	站	42	碼:		的	內容")做	0xA
		給	度+2	號				位	CRC16-Mod	Α
		Binar						址	bus 計算依	
		у 通							序產生的	
		訊協							Hight byte+	
		定使							Low byte	
		用的								
訊息	1	1	2	1	1	1	參	2	2	2
長度							考			
(單							表			
位:Byt							格			
e)										
範例:	0x5	0x10	0x00	0x0	0x42	0x0	0x5	0x00	0x8E	0x55
僕站	1		+0x0	1		3	9	+0x6	+0x69	+
站			6					4		0xA
號:01										Α
•										
Y100:S										
ET										

● 控制碼(1 Byte):

回覆訊息段落	控制碼
訊息內容	0x00:抑能(Disable)
	Ox01: 致能(Enable)
	0x02: 設定(Set)
	0x03:清除(Reset)

● 類型碼(n Byte):

回覆訊息段落	類型碼(單點)	長度
訊息內容	0x58 : X	1
	0x59 : Y	1
	0x4D : M	1
	0x53 : S	1
	0x54 : T	1
	0x43 : C	1

● 接收並回覆的訊息如下:

回覆訊	開	有效封	訊息	訊息区	内容		CRC 較驗碼	結尾
息段落	頭	包編號	長度					字元
	字							
	元							
訊息內		0x10 ,	0x00	僕	命令	錯誤	將("訊息長	0x55+
容	0x52	固定給	+0x03	站	碼:0x42	碼:參	度"+"訊息內	0xAA
		Binary		站		考下	容")做	
		通訊協		號		方表	CRC16-Modbus	
		定使用				格	計算依序產生	
		的					的 Hight byte+	
							Low byte	
訊息長	1	1	2	1	1	1	2	2
度(單								
位:Byte)								
範例:	0x52	0x10	0x00	0x01	0x42	0x00	0x24+0x 55	0x55+
僕站站			+0x03					0xAA
號:01、								
PLC								
STOP								

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC, PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

命令碼 43 多個連續單點之抑/致能狀態讀取

此指令可以控制指定的單點做致能、抑能、設定、清除四種運作。

● 訊息內容

(1) 發送

STN(1) CMD(1)	NUM(1)	TYPE(x)	ADDR(2)
---------------	--------	---------	---------

(2) 回覆

參數	描述	值
數量	連續資料數量	00H: 256 個
数 <u>里</u>		01H~FFH: 1~255 個
型別	資料類型	參考末頁表格 1
地址	資料起始地址	
		n: 資料數量,
狀態	致能/抑能 狀態	00H: 致能
		01H: 抑能

● 範例

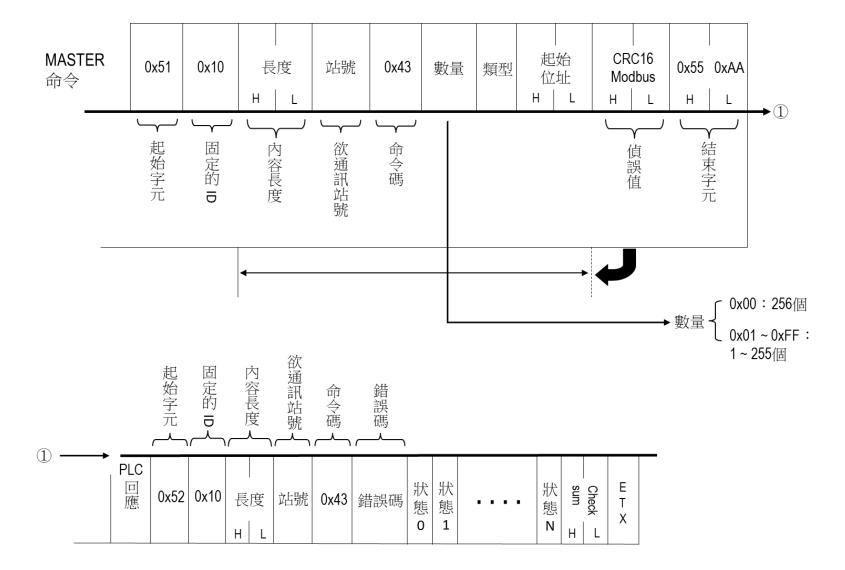
若 Y10~Y16 中, Y10、Y12、Y16 為抑能狀態, 其他的都為致能狀態, 那麼 此命令讀取的回覆狀態如下所示。

(1) 發送

01H 43H 07H 59H 00H	0AH
---------------------	-----

(2) 回覆

01H	43H	00H	01H	00H	01H	00H	00H	00H	01H
			\uparrow	\uparrow	\uparrow	\uparrow	\uparrow		
			Y10	Y11	Y12	Y13	Y14	Y15	Y16



● 發送命令如下:

命令	開	有效	訊息長度	訊息	.內容				CRC 較驗	結
訊息	頭	封包							碼	尾
段落	字	編號								字
	元									元
訊息		0x10	1+1+1+n+	僕	命令	數	類	單	將("訊息	0x5
內容	0x5	,	2,n 與	站	碼:0x	量	型	黑上	長度"+"訊	5+
	1	固定	Type 的長	站	43			的	息內容")	0xA
		給	度有關	號				位	做	Α
		Binar						址	CRC16-Mo	
		у 通							dbus 計算	
		訊協							依序產生	
		定使							的 Hight	
		用的							byte+ Low	
									byte	
訊息	1	1	2	1	1	1	參	2	2	2
長度							考			
(單							表			
位:Byt							格			
e)										
範例:	0x5	0x10	0x00	0x0	0x43	0x0	0x5	0x0	0xE2	0x5
僕站	1		+0x06	1		4	8	0	+0xF6	5+
站								+0x		0xA
號:01								00		Α
,										
Y100:S										
ET										

● 數量(1 Byte):

回覆訊息段落	數量
訊息內容	0x00 :256 個
	0x01~0xFF :1~255 個

● 類型碼(n Byte):

回覆訊息段落	類型碼(單點)	長度
訊息內容	0x58 : X	1
	0x59 : Y	1
	0x4D : M	1
	0x53 : S	1
	0x54 : T	1
	0x43 : C	1

● 位址(2 Byte):

回覆訊息段落	位址
訊息內容	0x00+0x00~0xFF+0xFF :1~65535 個

● 接收並回覆的訊息如下:

回覆	開	有效	訊息	訊息	、內容			CRC 較驗	結
訊息	頭	封包	長度					碼	尾
段落	字	編號							字
	元								元
訊息		0x10	1+1+1	僕	命令	錯	抑能/致能狀態	將("訊息	0x5
內容	0x	,	+n	站	碼:0x	誤	碼*n	長度"+"訊	5+
	52	固定		站	43	碼:		息內容")	0xA
		給		號		參		做	Α
		Bina				考		CRC16-Mo	
		ry				下		dbus 計算	
		通訊				方		依序產生	
		協定				表		的 Hight	
		使用				格		byte+ Low	
		的						byte	
訊息	1	1	2	1	1	1	1*n	2	2
長度									
(單									
位:By									
te)									
範例:	0x	0x10	0x00	0x	0x43	0x	0x01+0x01+0x0	0x49+0x	0x5
僕站	52		+0x07	01		00	1+0x01	55	5+
站									0xA
號:01									Α
`									
Y0~Y									
3 為									
致能									
狀態									

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC, PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

● 抑能/致能狀態碼(1*n Byte):

所指單點之狀態	敘述
STATUS1	0x00:致能
	0x01:抑能
STATUS2	0x00:致能
	0x01:抑能
STATUS3	0x00:致能
	0x01:抑能

.

STATUSn	0x00:致能
	0x01:抑能

命令碼 44 多個連續單點狀態(Data)讀取

此指令可以讀取指定的單點的狀態。

● 訊息內容

(1) 發送

STN(1) CMD(1)	NUM(1)	TYPE(x)	ADDR(2)
---------------	--------	---------	---------

(2) 回覆

I	STN(1)	CMD(1)	ERR(1)	DATA 1(1)	DATA 2(1)	 DATA n(1)
Ш	···(-,	0 (-)	(_,	, , _ (_ ,	, , _ (_ ,	 _,(_,

參數	描述	值
數量	連續資料數量	00H: 256 個
数 里	建 類貝州	01H~FFH: 1~255 個
類型	資料類型	參考末頁表格 1
地址	資料地址	
		n: 連續資料個數,
資料	設定/清除狀態	00H: 清除
		01H: 設定

● 範例

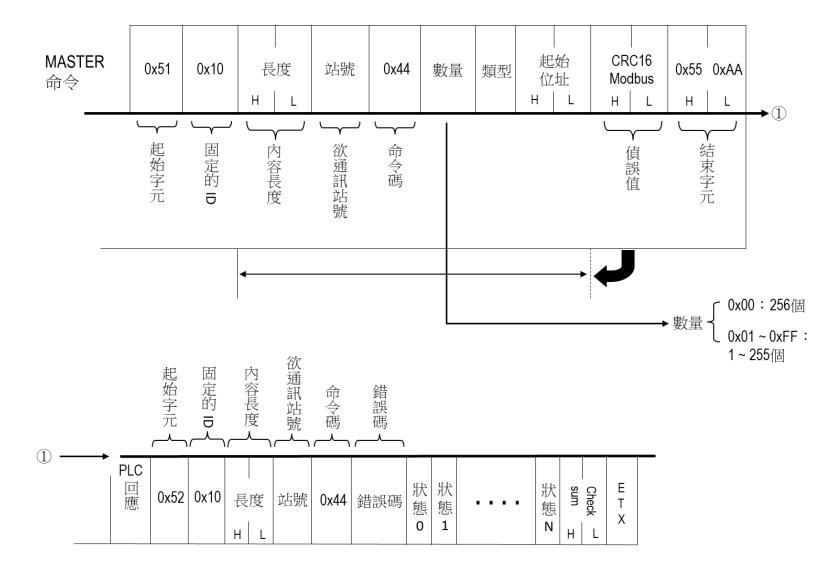
如果 X50、X52、X55 的狀態都是 0,且 X51、X53、X54 的狀態都是 1, 則以下是讀取連續 6 個輸入(X50~X55)的狀態。

(1) Query

01H	44H	06H	58H	00H	32H
-----	-----	-----	-----	-----	-----

(2) Response

01H	44H	00H	00H	01H	00H	01H	01H	00H
			\uparrow	\uparrow	\uparrow	\uparrow	\uparrow	\uparrow
			X50	X51	X52	X53	X54	X55



● 發送命令如下:

命令	開	有效	訊息長度	訊息	内容				CRC較驗碼	結
訊息	頭	封包								尾
段落	字	編號								字
	元									元
訊息		0x10	1+1+1+n+	僕	命令	數	類	單	將("訊息長	0x5
內容	0x5	,	2,n 與	站	碼:0x	量	型	點	度"+"訊息	5+
	1	固定	Type 的長	站	44			的	内容")做	0xA
		給	度有關	號				位	CRC16-Mo	Α
		Binar						址	dbus 計算	
		у 通							依序產生	
		訊協							的 Hight	
		定使							byte+ Low	
		用的							byte	
訊息	1	1	2	1	1	1	參	2	2	2
長度							考			
(單							表			
位:By							格			
te)										
範例:	0x5	0x10	0x00	0x0	0x44	0x0	0x5	0x0	0x04	0x5
僕站	1		+0x06	1		F	9	0	+0xD2	5+
站								+0x		0xA
號:01								0		Α
Y0~Y1										
4										

● 數量(1 Byte):

回覆訊息段落	數量
訊息內容	0x00 :256 個
	0x01~0xFF :1~255 個

● 類型碼(n Byte):

回覆訊息段落	類型碼(單點)	長度
訊息內容	0x58 : X	1
	0x59 : Y	1
	0x4D : M	1
	0x53 : S	1
	0x54 : T	1
	0x43 : C	1

● 位址(2 Byte):

回覆訊息段落	位址
訊息內容	0x00+0x00~0xFF+0xFF :1~65535 個

● 接收並回覆的訊息如下:

回覆	開	有效	訊息	訊息	内容			CRC 較驗碼	結尾
訊息	頭	封包	長度						字元
段落	字	編號							
	元								
訊息	0x5	0x10,	1+1+1	僕	命令	錯	狀態碼	將("訊息長	0x55
內容	2	固定	+n 應	站	碼:0x	誤	*n	度"+"訊息	+
		給	回覆	站	44	碼:		內容")做	0xA
		Binar	狀態	號		參		CRC16-Mod	Α
		у 通	碼總			考		bus 計算依	
		訊協	長度			下		序產生的	
		定使				方		Hight byte+	
		用的				表		Low byte	
						格			
訊息	1	1	2	1	1	1	1*n	2	2
長度									
(單									
位:Byt									
e)									
範例:	0x5	0x10	0x00	0x0	0x44	0x0	(0x00)*	0x89+0x 55	0x55
僕站	2		+0x01	1		0	15		+
站			2						0xA
號:01									Α
,									
Y0~Y1									
4 皆									
Reset									

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC,PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

● 狀態碼(1*n Byte):

所指單點之狀態	敘述	長度(Byte)
STATUS1	0x00:Reset	1
	0x01:Set	
STATUS2	0x00:Reset	1
	0x01:Set	
STATUS3	0x00:Reset	1
	0x01:Set	

.

STATUSn	0x00:Reset	1
	0x01:Set	

命令碼 45 多個連續單點狀態(Data)寫入

此指令可以讀取指定的單點的狀態。

● 訊息內容

(1) 發送

STN(1) CMD(1) NUM(1)	TYPE(x)	ADDR(2)	DATA 1(1)	DATA 2(1)		DATA n(1)
----------------------	---------	---------	-----------	-----------	--	-----------

(2) 回覆

CTNI/4\	CNAD(4)	EDD/41
211/(T)	CMD(1)	FKK(T)

參數	描述	值			
數量	連續資料數量	00H: 256 個			
数里		01H~FFH: 1~255 個			
類型	資料類型	參考末頁表格 1			
地址	資料地址				
		n: 連續資料個數,			
資料	設定/清除狀態	00H: 清除			
		01H: 設定			

● 範例

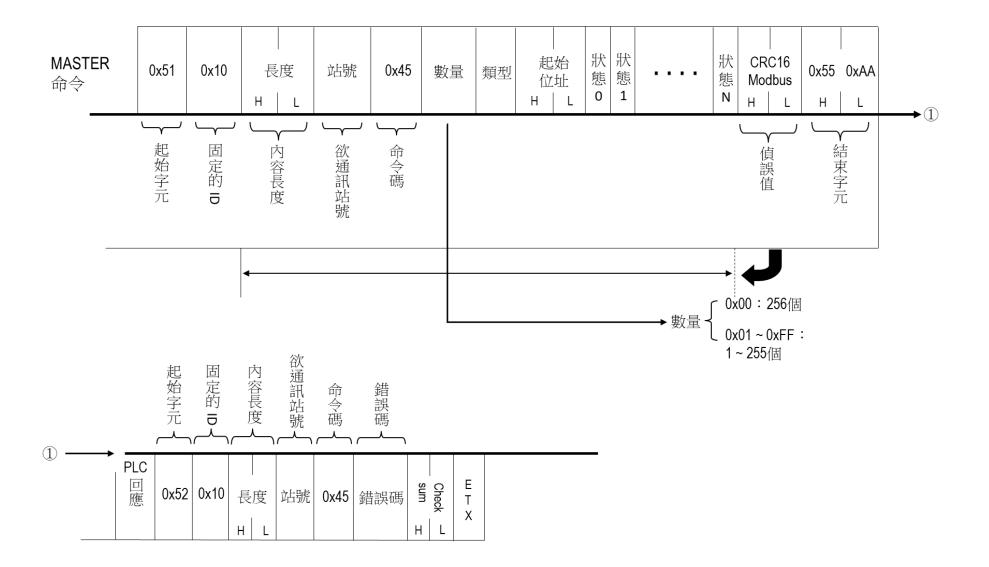
如果 X50、X52、X55 的狀態都是 0,且 X51、X53、X54 的狀態都是 1,則以下是讀取連續 6 個輸入 X50~X55 的狀態。

(1) 發送

01H	45H	04H	59H	00H				01H	
					↑ Y0	\uparrow	\uparrow	\uparrow	
					Y0	Y1	Y2	Y3	

(2) 回覆

01H 45H 00H



● 發送命令如下:

命令 訊息 段落	開頭字元	有效封包編號	訊息長 度	訊息	息内容					CRC 較 驗碼	結尾字元
訊息內容	0x 51	Ox1 Ox1 Ox1 Bin ary通訊協定使用的	1+1+1+n +2+m,n 與 天 與 表 關 與 之 長 關 數 狀 度 關 額 數 狀 度 關 額 數 影 數 長 關 額 數 長 屬	僕站站號	命 令 碼:0 x45	數量	類型	單點的位址	狀態寫 入*數量	將("訊 息度"+"訊 息度"+")做 CRC16- Modbus 計產生 的 Hight byte+ Low byte	0x 55 + 0x AA
訊息 長度 (單 位:Byt e)	1	1	2	1	1	1	n參考表格	2	m	2	2
範例: 僕站 號:01 、Y0、 Y2:RE SET、 Y1:SE T	0x 51	0x1 0	0x00 +0x09	0x 01	0x4 5	0x 03	0x 59	0x 00 +0 x0 0	0x00+0x 01+0x00	0x21 +0x0D	0x 55 + 0x AA

● 數量(1 Byte):

回覆訊息段落	數量
訊息內容	0x00 :256 個
	0x01~0xFF :1~255 個

● 類型碼(n Byte):

回覆訊息段落	類型碼(單點)	長度(Byte)
訊息內容	0x58 : X	1
	0x59 : Y	1
	0x4D : M	1
	0x53 : S	1
	0x54 : T	1
	0x43 : C	1

● 位址(2 Byte):

回覆訊息段落	位址	長度
訊息內容	0x00+0x00~0xFF+0xFF :1~65535 個	2

● 狀態碼寫入(1*n Byte):

所指單點之狀態	敘述	長度
STATUS1	0x00:Reset	1
	0x01:Set	
STATUS2	0x00:Reset	1
	0x01:Set	
STATUS3	0x00:Reset	1
	0x01:Set	

.

STATUSn	0x00:Reset	1
	0x01:Set	

● 接收並回覆的訊息如下:

回覆訊	開	有效	訊息	訊息区	内容		CRC 較驗碼	結尾
息段落	頭	封包	長度					字元
	字	編號						
	元							
訊息內		0x10 ,	0x00	僕	命令	錯誤	將("訊息長	0x55+
容	0x52	固定	+0x03	站	碼:0x45	碼:參	度"+"訊息內	0xAA
		給		站		考下	容")做	
		Binary		號		方表	CRC16-Modbus	
		通訊				格	計算依序產生	
		協定					的 Hight byte+	
		使用					Low byte	
		的						
訊息長	1	1	2	1	1	1	2	2
度(單								
位:Byte)								
範例:	0x52	0x10	0x00	0x01	0x45	0x00	0x14+0x 55	0x55+
僕站站			+0x03					0xAA
號:01								

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC,PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

命令碼 46 多個連續暫存器資料(Data)讀取

此指令可以從指定的暫存器開始連續讀取設定數量的資料。

● 訊息內容

(1) 發送

STN(1) CMD(1)	NUM(1)	TYPE(x)	ADDR(2)
---------------	--------	---------	---------

(2) 回覆

STN(1)	CMD(1)	ERR(1)	DATA 1(y)	DATA 2(y)	 DATA n(y)
· ,	` '	· ,	\ <i>\ , \ ,</i>	() ,	,,

參數	描述	值
數量	連續資料數量	01H~40H: 1~64 個
類型	資料類型	參考末頁表格 1
地址	資料地址	
		n: 連續資料個數,
資料	 暫存器的值	y: 一筆資料的位元組數
貝州	自行命可阻 	y = 2, 16 位元暫存器
		y = 4, 32-位元暫存器

● 範例

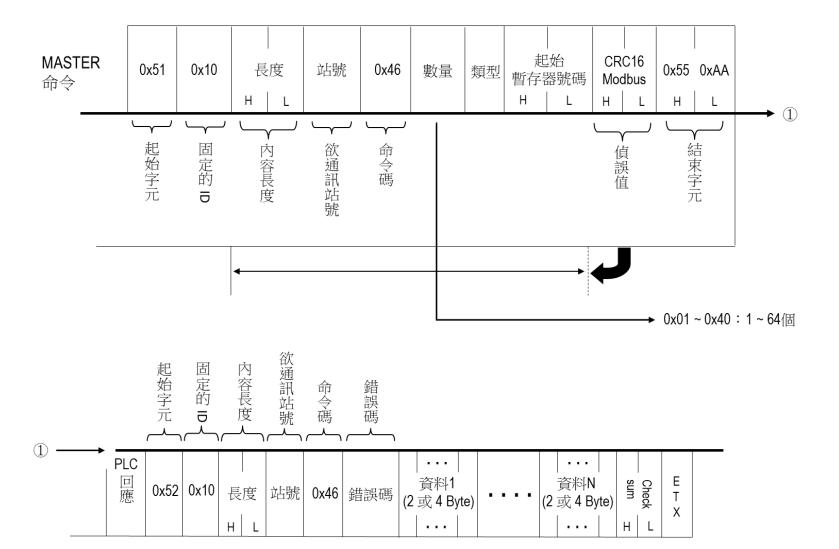
讀取連續的3個16位元暫存器的數據,從R12開始。

(1) 發送

01H	46H	03H	52H	00H	0CH
-----	-----	-----	-----	-----	-----

(2) 回覆

01H	46H	00H	10H	A5H	7FH	C4H	00H	01H
			↑		↑		↑	
			R12		R13		R14	



● 發送命令如下:

命令	開	有效	訊息長度	訊息	 .內容				CRC 較驗	結
訊息	頭	封包						碼	尾	
段落	字	編號								字
	元									元
訊息	0x5	0x10	1+1+1+n+	僕	命令	數	類	暫	將("訊息	0x5
內容	1	,	2,n 與	站	碼:0x	量	型	存	長度"+"訊	5+
		固定	Type 的長	站	46			器	息內容")	0xA
		給	度有關	號				的	做	Α
		Binar						位	CRC16-Mo	
		y 通						址	dbus 計算	
		訊協							依序產生	
		定使							的 Hight	
		用的							byte+ Low	
									byte	
訊息	1	1	2	1	1	1	n	2	2	2
長度							參			
(單							考			
位:By							表			
te)							格			
範例:	0x5	0x10	0x00	0x0	0x46	0x0	0x5	0x0	0x0E	0x5
僕站	1		+0x06	1		2	2	0	+0x7C	5+
站								+0x		0xA
號:01								00		Α
R0~R										
1										

● 數量(1 Byte):

回覆訊息段落	數量
訊息內容	0x01~0x40 :1~64 個

● 類型碼(2 Byte/4 Byte):

回覆訊息段落	類型碼(單點)	長度(Byte)
16 bit 暫存器	0x57+0x58 : WX	2
	0x57+0x59 : WY	2
	0x57+0x4D : WM	2
	0x57+0x53 : WS	2
	0x57+0x54 : WT	2
	0x57+0x43 : WC	2
	0x52+0x54 : RT	2
	0x52+0x43 : RC	2
	0x52 : R	1
	0x44 : D	1
	0x46 : F	1
32 bit 暫存器	0x44+0x57+0x58 : DWX	3
	0x44+0x57+0x59 : DWY	3
	0x44+0x57+0x4D : DWM	3
	0x44+0x57+0x53 : DWS	3
	0x44+0x57+0x54 : DWT	3
	0x44+0x57+0x43 : DWC	3
	0x44+0x52 : DR	2
	0x44+0x44 : DD	2
	0x44+0x46 : DF	2

● 位址(2 Byte):

回覆訊息段落	位址	長度
訊息內容	0x00+0x00~0xFF+0xFF :1~65535 個	2

● 接收並回覆的訊息如下:

回覆訊息	開	有	訊息	訊息	内容	CRC 較驗	結		
段落	頭	效	長度					碼	尾
	字	封							字
	元	包							元
		編							
		號							
訊息內容		0x1	1+1+1	僕	命令	錯	暫存器中的	將("訊息	0x5
	0x	0 ,	+n,n	站	碼:0	誤	數值	長度"+"	5+
	52	固	的數	站	x46	碼:		訊息內	0xA
		定	量與	號		參		容")做	Α
		給	讀取			考		CRC16-M	
		Bina	的暫			下		odbus 計	
		ry	存器			方		算依序產	
		通	數量			表		生的	
		訊	有關			格		Hight	
		協						byte+	
		定						Low byte	
		使							
		用							
		的							
訊息長度	1	1	2	1	1	1	N,依所設數	2	2
(單							量而變		
位:Byte)									
範例:	0x	0x1	0x00	0x	0x46	0x	0xFF+0x55+0	0xB3+0x5	0x5
僕站站	52	0	+0x07	01		00	xFF+0x 4B	5	5+
號:01、									0xA
R0=0xFF+0									Α
x55 `									
R1=0xFF+0									
x4B									

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC,PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

● 暫存器之數值(2*n/4*n Byte):

所指單點之狀態	敘述(16 Bit)	敘述(32 Bit)		
DATA1	0x00+0x00~	0x00+0x00+0x00+0x00~		
	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF		
DATA 2	0x00+0x00~	0x00+0x00+0x00+0x00~		
	0xFF+0xFF	0xFF+0xFF+0xFF		
DATA 3	0x00+0x00~	0x00+0x00+0x00+0x00~		
	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF		

.

DATA n	0x00+0x00~	0x00+0x00+0x00+0x00~
	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF

命令碼 47 多個連續暫存器資料(Data)寫入

此指令可以從指定的暫存器開始連續寫入設定數量的資料。

● 訊息內容

(1) 發送

STN(1) CMD(1) NUM(1) TYPE(x)	ADDR(2)	DATA 1(y)	DATA 2(y)	•••	DATA n(y)
------------------------------	---------	-----------	-----------	-----	-----------

(2) 回覆

STN(1) | CMD(1) | ERR(1)

參數	描述	值
數量	連續資料數量	01H~40H: 1~64 個
類型	資料類型	參考末頁表格 1
地址	資料地址	
		n: 連續資料個數
資料	 暫存器的值	y: 一筆資料的位元組數
貝州	首行命印度 	y = 2, 16 位元暫存器
		y = 4, 32-位元暫存器

● 範例

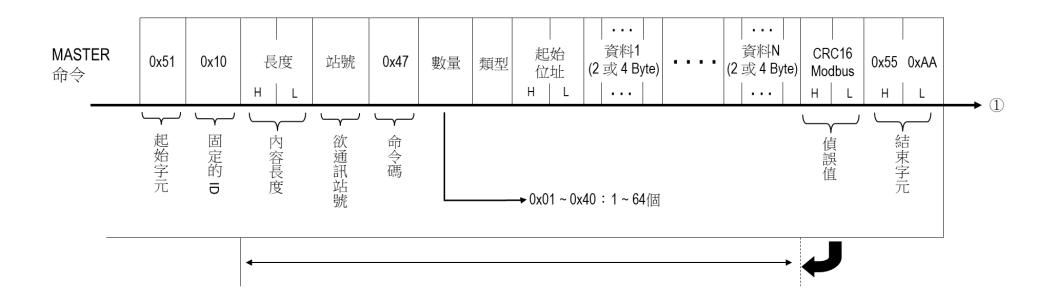
將 AAAAH 輸入到 16 位元暫存器 WY16,並將 5555H 接續輸入到 WY32。

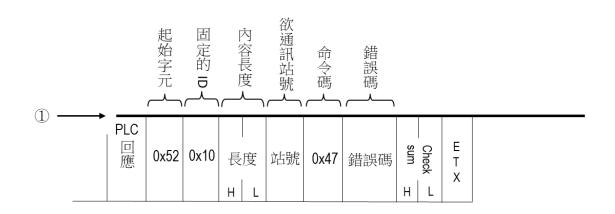
(1) 發送

01H	47H	02H	57H	59H	00H	10H	AAH	AAH	55H	55H
							1	\	\uparrow	
							WY	′16	WY	/32

(2) 回覆

01H 47H 00H





● 發送命令如下:

命令訊息段落	開頭字元	有效封包編號	訊息長 度	訊息	思内容					CRC 較 驗碼	結尾字元
部息内容	0x 51	0x1 0 固定給 Bin ary 通訊協定使用的	1+1+1+ n+m , n 與 長 關 寫 資 度 , 入 料 有	僕站站號	命 令 碼:0 x47	數量	類型	暫存器的位址	欲寫之 器 料	將("訊息度"+"和 高度"+"訊息") 高容")做 CRC16- Modbus 計算在 的 Hight byte+ Low byte	0x 55 + 0x AA
訊息長 度(單 位:Byte)	1	1	2	1	1	1	參考表格	2	m	2	2
範例: 僕站站 號:01、 R0~R2 寫入 (0xFF+0 x55、 0xFF+0x 4B、 0xFF+0x 41)	0x 51	0x1 0	0x00 +0x0C	0x 01	0x4 7	0x 03	0x 52	0x 00 +0x 00	0xFF+0 x55 \ 0xFF+0 x4B \ 0xFF+0 x41	0xC4 +0x16	0x 55 + 0x AA

● 數量(1 Byte):

回覆訊息段落	數量
訊息內容	0x01~0x40 :1~64 個

● 類型碼(2 Byte/4 Byte):

回覆訊息段落	類型碼(單點)	長度(Byte)
16 bit 暫存器	0x57+0x58 : WX	2
	0x57+0x59 : WY	2
	0x57+0x4D : WM	2
	0x57+0x53 : WS	2
	0x57+0x54 : WT	2
	0x57+0x43 : WC	2
	0x52+0x54 : RT	2
	0x52+0x43 : RC	2
	0x52 : R	1
	0x44 : D	1
	0x46 : F	1
32 bit 暫存器	0x44+0x57+0x58 : DWX	3
	0x44+0x57+0x59 : DWY	3
	0x44+0x57+0x4D : DWM	3
	0x44+0x57+0x53 : DWS	3
	0x44+0x57+0x54 : DWT	3
	0x44+0x57+0x43 : DWC	3
	0x44+0x52 : DR	2
	0x44+0x44 : DD	2
	0x44+0x46 : DF	2

● 位址(2 Byte):

回覆訊息段落	位址	長度
訊息內容	0x00+0x00~0xFF+0xFF :1~65535 個	2

● 暫存器之數值(2*n/4*n Byte):

所指單點之狀態	敘述(16 Bit)	敘述(32 Bit)
DATA1	0x00+0x00~	0x00+0x00+0x00+0x00~
	0xFF+0xFF	0xFF+0xFF+0xFF
DATA 2	0x00+0x00~	0x00+0x00+0x00+0x00~
	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF
DATA 3	0x00+0x00~	0x00+0x00+0x00+0x00~
	0xFF+0xFF	0xFF+0xFF+0xFF

:

DATA n	0x00+0x00~	0x00+0x00+0x00+0x00~	
	0xFF+0xFF	0xFF+0xFF+0xFF	

● 接收並回覆的訊息如下:

回覆訊	開	有效	訊息	訊息	内容		CRC 較驗碼	結尾
息段落	頭	封包	長度					字元
	字	編號						
	元							
訊息內		0x10 ,	0x00	僕	命令	錯誤	將("訊息長	0x55+
容	0x52	固定	+0x03	站	碼:0x47	碼:參	度"+"訊息內	0xAA
		給		站		考下	容")做	
		Binary		號		方表	CRC16-Modbus	
		通訊				格	計算依序產生	
		協定					的 Hight byte+	
		使用					Low byte	
		的						
訊息長	1	1	2	1	1	1	2	2
度(單								
位:Byte)								
範例:	0x52	0x10	0x00	0x01	0x47	0x00	0x46+0x 74	0x55+
僕站站			+0x03					0xAA
號:01、								
PLC								

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC,PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

命令碼 48 多個任意單點狀態或暫存器資料(Data)混合讀取

此指令可以依序讀取任意混合順序及任意類型的單點狀態或暫存器資料。

● 訊息內容

(1) 發送

	STN(1)	CMD(1)	NUM(1)	TYPE 1(x)	ADDR 1(2)	TYPE 2(x)	ADDR 2(2)		
--	--------	--------	--------	-----------	-----------	-----------	-----------	--	--

	TYPE n-1(x)	ADDR n-1(2)	TYPE n(x)	ADDR n(2)
--	-------------	-------------	-----------	-----------

(2) 回覆

STN(1)	CMD(1)	ERR(1)	DATA 1(y)	DATA 2(y)		DATA n(y)
--------	--------	--------	-----------	-----------	--	-----------

參數	描述	值
數量	連續資料數量	01H~40H: 1~64 個
類型	資料類型	參考末頁表格 1
地址	資料地址	
		n: 連續資料個數
		y: 一筆資料的位元組數
資料	暫存器的值	y = 1, 單點狀態
		y = 2, 16 位元暫存器
		y = 4, 32-位元暫存器

● 範例

讀取 R1、Y9 和 DWM0(即 M31~M0)的狀態和數據。

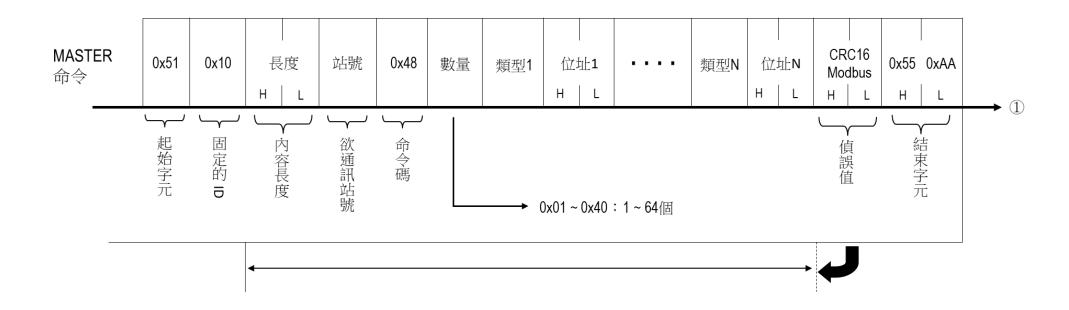
(1) 發送

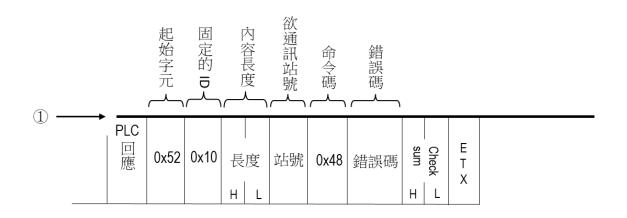
01H	48H	03H	52H	00H	01H	59H	00H	09H	44H	57H	4DH	00H	00H
		Λ			↑			↑					
				R1			Y9			ĺ	DWM0)	

(2) 回覆

01H	48H	00H	5CH	34H	01H	00H	35H	47H	BAH
			1	\			/	٢	

R1	Υ9	DWM0





● 發送命令如下:

命令訊 息段落	開頭	有效	訊息 長度	訊息	息內容							CRC 較 驗碼	結尾
	字	封											字
	元	包											元
		編											
		號											
訊息內	0x5	0x1	1+1+1	僕	命	數	類型	暫		類	暫	將("訊	0x
容	1	0 ,	+(n+2+	站	\Rightarrow	量	n	存		型	存	息長	55
		固	+m+	站	碼:			器		m	器	度"+"	+
		定	2),n、	號	0x4			的			的	訊息內	0x
		給	m與		8			位			位	容")做	AA
		Bin	Туре					址			址	CRC16-	
		ary	的長					n			m	Modbu	
		通	度有									s計算	
		訊	關,且						l			依序產	
		協	n可以									生的	
		定	與 m									Hight	
		使	不同									byte+	
		用	種類									Low	
		的										byte	
訊息長	1	1	2	1	1	1	參考	2		參	2	2	2
度(單							表格			考			
位:Byte										表			
)										格			
範例:	0x5	0x1	0x00	0x	0x4	0x	0x44+	0x52	+0x0	0+0x	0F+	0x48	0x
僕站站	1	0	+0x0A	0	8	0	0x44+	0x00	+0x0	1		+0xB2	55
號:01				1		2							+
`													0x
DR15													AA
、D1													

● 數量(1 Byte):

回覆訊息段落	數量
訊息內容	0x01~0x40 :1~64 個

● 類型碼(1-Byte/2 Byte/4 Byte):

回覆訊息段落	類型碼(單點)	長度(Byte)
単點	0x58 : X	1
	0x59 : Y	1
	0x4D : M	1
	0x53 : S	1
	0x54 : T	1
	0x43 : C	1
16 bit 暫存器	0x57+0x58 : WX	2
	0x57+0x59 : WY	2
	0x57+0x4D : WM	2
	0x57+0x53 : WS	2
	0x57+0x54 : WT	2
	0x57+0x43 : WC	2
	0x52+0x54 : RT	2
	0x52+0x43 : RC	2
	0x52 : R	1
	0x44 : D	1
	0x46 : F	1
32 bit 暫存器	0x44+0x57+0x58 : DWX	3
	0x44+0x57+0x59 : DWY	3
	0x44+0x57+0x4D : DWM	3
	0x44+0x57+0x53 : DWS	3
	0x44+0x57+0x54 : DWT	3
	0x44+0x57+0x43 : DWC	3
	0x44+0x52 : DR	2
	0x44+0x44 : DD	2
	0x44+0x46 : DF	2

● 位址(2 Byte):

回覆訊息段落	位址	長度

訊息內容	0x00+0x00~0xFF+0xFF :1~65535 個	2
------	--------------------------------	---

● 接收並回覆的訊息如下:

回覆 訊息 段落	開頭字元	有效封包編號	訊息長 度	訊息	息内容					CRC 較 驗碼	結尾字元
訊息		0x1	1+1+1+(僕	命	錯誤	暫	•••	暫	將("訊	0x
內容	0x	0,	n++m)	站	\$	碼:參	存		存	息長	55
	52	固		站	碼:0	考下	器		器	度"+"訊	+
		定		號	x48	方表	中		中	息內	0x
		給				格	的		的	容")做	AA
		Bin					數		數	CRC16-	
		ary ः					值 n		值m	Modbus 斗笛法	
		通 訊								計算依 序產生	
		協								的 Hight	
		定								byte+	
		使								Low	
		用								byte	
		的									
訊息	1	1	2	1	1	1	參	•••	參	2	2
長度							考		考		
(單							類		類		
位:By							型		型		
te)							的		的		
							長鹿		長鹿		
							度表		度表		
							格		格		
範例:	0x	0x1	0x00	0x	0x4	0x00+(l .	x99+0x	l .	0xDF+0x	0x
僕站	52	0	+0x09	01	8	(00)+(0x				18	55
站						, ,		•			+
號:01											0x
,											AA
DR15											
=6、											
D1=0											

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC, PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

● 暫存器之數值(1*n/2*n/4*n Byte):

所指單	敘述(單點)	敘述(16 Bit)	敘述(32 Bit)
點之狀			
態			
DATA1	0x00 : OFF	0x00+0x00~	0x00+0x00+0x00+0x00~
	0x01 : ON	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF
DATA 2	0x00 : OFF	0x00+0x00~	0x00+0x00+0x00+0x00~
	0x01 : ON	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF
DATA 3	0x00 : OFF	0x00+0x00~	0x00+0x00+0x00+0x00~
	0x01 : ON	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF

.

DATA n	0x00 : OFF	0x00+0x00~	0x00+0x00+0x00+0x00~
	0x01 : ON	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF

命令碼 49 多個任意單點狀態或暫存器資料(Data)混合寫入

此指令可以依序寫入任意混合順序及任意類型的單點狀態或暫存器資料

● 訊息內容

(1) 發送

STN(1) CMD(1) NUM(1) TYPE 1(x) ADDR 1(2) DATA 1(
--

(2) 回覆

STN(1) CMD(1) ERR(1)

參數	描述	值
數量	連續資料數量	01H~20H: 1~32 個
類型	資料類型	參考末頁表格 1
地址	資料地址	
		n: 連續資料個數
		y: 一筆資料的位元組數
資料	暫存器的值	y = 1, 單點狀態
		y = 2, 16 位元暫存器
		y = 4, 32-位元暫存器

● 範例

將 Y0 的狀態設為 1 , Y1 的狀態設為 0 , 16 位元暫存器 WM8 設為 5555H , 32 位元暫存器 DR2 設為 FFH 。

(1) 發送

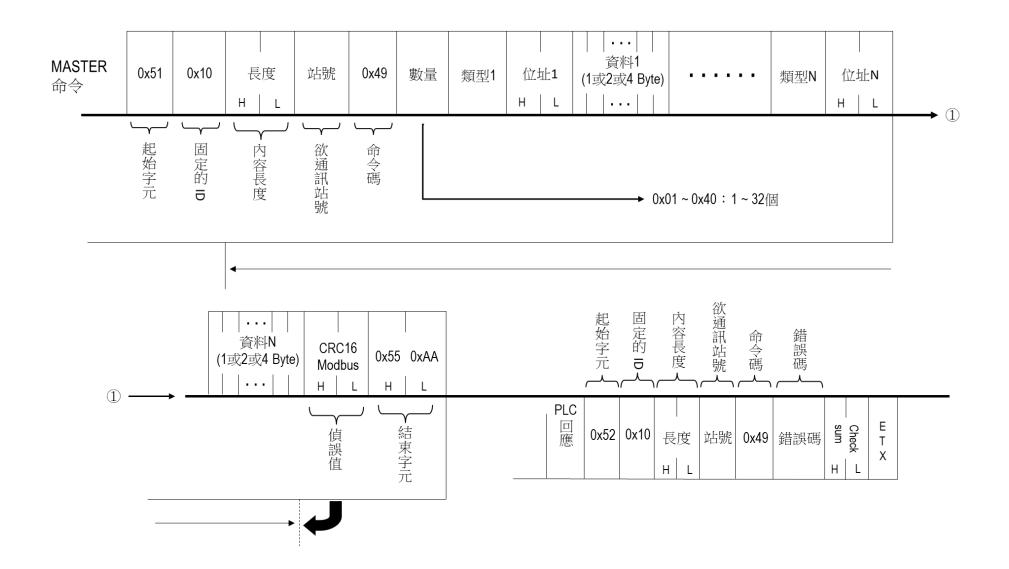
01H	49H	04H	59H	00H	00H	01H	59H	00H	01H	00H
				/	١			/	١	
				Υ	0			Υ	1	

57I	Н	4DH	00H	08H	55H	55H	44H	52H	00H	02H	00H	00H	00H	FFH
	↑									1	`			

WM8	DR2
-----	-----

(2) 回覆

01H 49H 00H



● 發送命令如下:

命	開	有	訊	訊	息內容	容								CRC	結
\$	頭	效	息											較驗	尾
揺	字	封	長											碼	字
息	元	包	度												元
段		編													
落		號													
訊	0	0x	1+1	僕	命	數	類	暫	欲	•••	類	暫	欲	將	0
息	х	10	+1+	站	\rightarrow	量	型	存	寫		型	存	寫	("訊	х
內	5	,	(2+	站	碼		1	器	入		n	器	入	息長	5
容	1	固	· 類	號	:0x			的	之			的	之	度"+"	5
		定	型	4,7 4	49			位	暫			位	暫	訊息	+
		給	碼					址	存			址	存	内	0
		Bi	長					1	器			n	器	容")	х
		na	度+						之				之	做	Α
		ry	暫						資				資	CRC1	Α
		通	存						料				料	6-Mo	
		訊	器						1				n	dbus	
		協	資						-				''	計算	
		定	料)											依序	
		使	, n											產生	
		用用	與											的	
		的													
		пλ	Typ e的											Hight	
														byte+	
			長鹿											Low	
			度											byte	
			有												
学 丑	1	1	弱 2	1	1	1	兹	2	4		4	2	兹	2	2
訊自	1	1		1	1	1	參		參		參	~	參	2	2
息							考		考		考		考		
長							表		類		表		類		
度							格		型		格		型		
(單									長立				長立		
位:									度				度		
Byt									表				表		
e)									格				格		
範	0	0x	0x0	0	0x	0			2+0x0					0x37	0
例:	Х	10	0	Х	49	Х	x00+	0x00	+0x52	+0x00	+0x0F	+0x0(0+0x	+0x8	Х

僕	5	+0x	0	0	OF	9	5
站	1	10	1	2			5
站							+
號:							0
01							х
•							Α
WR							Α
0=1							
5、							
R15							
=25							
5							

● 數量(1 Byte):

回覆訊息段落	數量
訊息內容	0x01~0x40 :1~64 個

● 類型碼(1-Byte/2 Byte/4 Byte):

回覆訊息段落	類型碼(單點)	長度(Byte)
單點	0x58 : X	1
	0x59 : Y	1
	0x4D : M	1
	0x53 : S	1
	0x54 : T	1
	0x43 : C	1
16 bit 暫存器	0x57+0x58 : WX	2
	0x57+0x59 : WY	2
	0x57+0x4D : WM	2
	0x57+0x53 : WS	2
	0x57+0x54 : WT	2
	0x57+0x43 : WC	2
	0x52+0x54 : RT	2
	0x52+0x43 : RC	2
	0x52 : R	1
	0x44 : D	1
	0x46 : F	1
32 bit 暫存器	0x44+0x57+0x58 : DWX	3

0x44+0x57+0x59 : DWY	3
0x44+0x57+0x4D : DWM	3
0x44+0x57+0x53 : DWS	3
0x44+0x57+0x54 : DWT	3
0x44+0x57+0x43 : DWC	3
0x44+0x52 : DR	2
0x44+0x44 : DD	2
0x44+0x46 : DF	2

● 位址(2 Byte):

回覆訊息段落	位址	長度
訊息內容	0x00+0x00~0xFF+0xFF :1~65535 個	2

● 暫存器之數值(1*n/2*n/4*n Byte):

所指單	敘述(單點)	敘述(16 Bit)	敘述(32 Bit)
點之狀			
態			
DATA1	0x00 : OFF	0x00+0x00~	0x00+0x00+0x00+0x00~
	0x01 : ON	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF
DATA 2	0x00 : OFF	0x00+0x00~	0x00+0x00+0x00+0x00~
	0x01 : ON	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF
DATA 3	0x00 : OFF	0x00+0x00~	0x00+0x00+0x00+0x00~
	0x01 : ON	0xFF+0xFF	0xFF+0xFF+0xFF+0xFF

.

 DATA n
 0x00 : OFF
 0x00+0x00~
 0x00+0x00+0x00+0x00+0x00

 0x01 : ON
 0xFF+0xFF
 0xFF+0xFF+0xFF+0xFF

● 接收並回覆的訊息如下:

回覆訊	開	有效	訊息	訊息	內容		CRC 較驗碼	結尾
息段落	頭	封包	長度					字元
	字	編號						
	元							
訊息內		0x10 ,	0x00	僕	命令	錯誤	將("訊息長	0x55+
容	0x52	固定	+0x03	站	碼:0x49	碼:參	度"+"訊息內	0xAA
		給		站		考下	容")做	
		Binary		號		方表	CRC16-Modbus	
		通訊				格	計算依序產生	
		協定					的 Hight byte+	
		使用					Low byte	
		的						
訊息長	1	1	2	1	1	1	2	2
度(單								
位:Byte)								
範例:	0x52	0x10	0x00	0x01	0x49	0x00	0x42+0x 14	0x55+
僕站站			+0x03					0xAA
號:01								

● 錯誤碼(1 Byte):

數值(16 進制)	敘述
0x00	無錯誤發生。
0x02	非法數值。
0x04	非法格式,或通訊格式無法執行。
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。
0x07	無法 RUN PLC,PLC Run 時 PLC 程式語法檢查錯誤。
0x09	無法 RUN PLC,Function 不支援。
0x0A	非法的位址。

命令碼 4E 測試回傳

此指令使 PLC 將所有測試數據回傳給主站。它僅用於測試主站與 PLC 之間的通訊狀況,不影響 PLC 的功能。

● 訊息內容

(1) 發送

STN(1)	CMD(1)	DATA(n)
--------	--------	---------

(2) 回覆

STN(1)	CMD(1)	DATA(n)
--------	--------	---------

參數	描述	值			
資料	測試回傳	n: 資料長度(位元組)			

● 範例

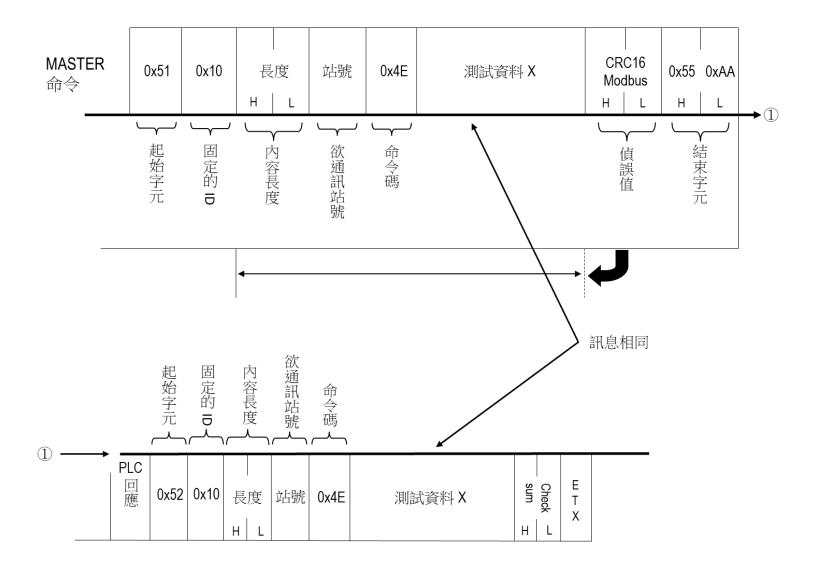
使用此指令將數據 "ABCDEFG" 從主機傳送到 PLC,以測試 PLC 是否正常回應。

(1) 發送

01H 4EH 41H 42H 43H 44H 45H 46H	47H
---------------------------------	-----

(2) 回覆

01H	4EH	41H	42H	43H	44H	45H	46H	47H
-----	-----	-----	-----	-----	-----	-----	-----	-----



● 發送命令如下:

命令訊	開	有效	訊息長	訊息	內容		CRC 較驗碼	結尾
息段落	頭	封包	度					字元
	字	編號						
	元							
訊息內		0x10 ,	1+1+n	僕	命令	測試資	將("訊息長	0x55
容	0x5	固定	,n與	站	碼:0x4	料	度"+"訊息內	+
	1	給	測試資	站	Е		容")做	0xAA
		Binary	料的長	號			CRC16-Modb	
		通訊	度有關				us 計算依序	
		協定					產生的 Hight	
		使用					byte+ Low	
		的					byte	
訊息長	1	1	2	1	1	測試資	2	2
度(單						料長度		
位:Byte)								
範例:	0x5	0x10	0x00	0x0	0x4E	0xFF+0xF	0x91	0x55
僕站站	1		+0x04	1		F	+0x80	+
號:01、								0xAA
測試碼								
0xFF+0x								
FF								

暫存器之數值(n Byte):

所指單點之狀態	敘述(單點)
DATA	測試資料

● 接收並回覆的訊息如下:

回覆訊	開	有效	訊息	訊息	内容		CRC 較驗碼	結尾
息段落	頭	封包	長度					字元
	字	編號						
	元							
訊息內		0x10 ,	0x00	僕	命令	測試資	將("訊息長	0x55
容	0x5	固定	+0x0	站	碼:0x4	料回傳	度"+"訊息內	+
	2	給	3	站	Е		容")做	0xAA
		Binary		號			CRC16-Modb	
		通訊					us 計算依序	
		協定					產生的 Hight	
		使用					byte+ Low	
		的					byte	
訊息長	1	1	2	1	1	測試資	2	2
度(單						料長度		
位:Byte)								
範例:	0x5	0x10	0x00	0x0	0x4E	0xFF+0xF	0x91	0x55
僕站站	2		+0x0	1		F	+0x80	+
號:01、測			4					0xAA
試碼								
0xFF+0xF								
F								

● 暫存器之數值(n Byte):

所指單點之狀態	敘述(單點)
DATA	測試資料

表格

● 類型碼(1-Byte/2 Byte/4 Byte):

回覆訊息段落	類型碼(單點)	長度(Byte)
單點	0x58 : X	1
	0x59 : Y	1
	0x4D : M	1
	0x53 : S	1
	0x54 : T	1
	0x43 : C	1
16 bit 暫存器	0x57+0x58 : WX	2
	0x57+0x59 : WY	2
	0x57+0x4D : WM	2
	0x57+0x53 : WS	2
	0x57+0x54 : WT	2
	0x57+0x43 : WC	2
	0x52+0x54 : RT	2
	0x52+0x43 : RC	2
	0x52 : R	1
	0x44 : D	1
	0x46 : F	1
32 bit 暫存器	0x44+0x57+0x58 : DWX	3
	0x44+0x57+0x59 : DWY	3
	0x44+0x57+0x4D : DWM	3
	0x44+0x57+0x53 : DWS	3
	0x44+0x57+0x54 : DWT	3
	0x44+0x57+0x43 : DWC	3
	0x44+0x52 : DR	2
	0x44+0x44 : DD	2
	0x44+0x46 : DF	2

● 錯誤碼(1 Byte):

數值(16 進制)	敘述	
0x00	無錯誤發生。	
0x02	非法數值。	
0x04	非法格式,或通訊格式無法執行。	
0x05	無法 RUN PLC,PLC Run 時階梯圖 Check sum 錯誤。	
0x06	無法 RUN PLC,PLC Run 時階梯 ID 與 PLC ID 不同。	
0x07	無法 RUN PLC,PLC Run 時 PLC 程式語法檢查錯誤。	
0x09	無法 RUN PLC,Function 不支援。	
0x0A	非法的位址。	

● 命令碼(1 Byte):

數值(16 進	敘述	命令長	控制資料長
制)		度	度
0x40	PLC 狀態查詢	1	-
0x41	PLC RUN/STOP 控制	1	-
0x42	單一個單點運作控制	1	1
0x43	多個連續單點之抑能/致能狀態讀取	1	1~256
0x44	多個連續單點狀態讀取	1	1~256
0x45	多個連續單點狀態寫入	1	1~256
0x46	多個連續暫存器資料讀取	1	1~64
0x47	多個連續暫存器資料寫入	1	1~64
0x48	多個任意單點狀態或暫存器資料混合讀	1	1~64
	取		1 04
0x49	多個任意單點狀態或暫存器資料混合寫	1	1~32
	入		1 32
0x4E	測試回傳	1	0~256