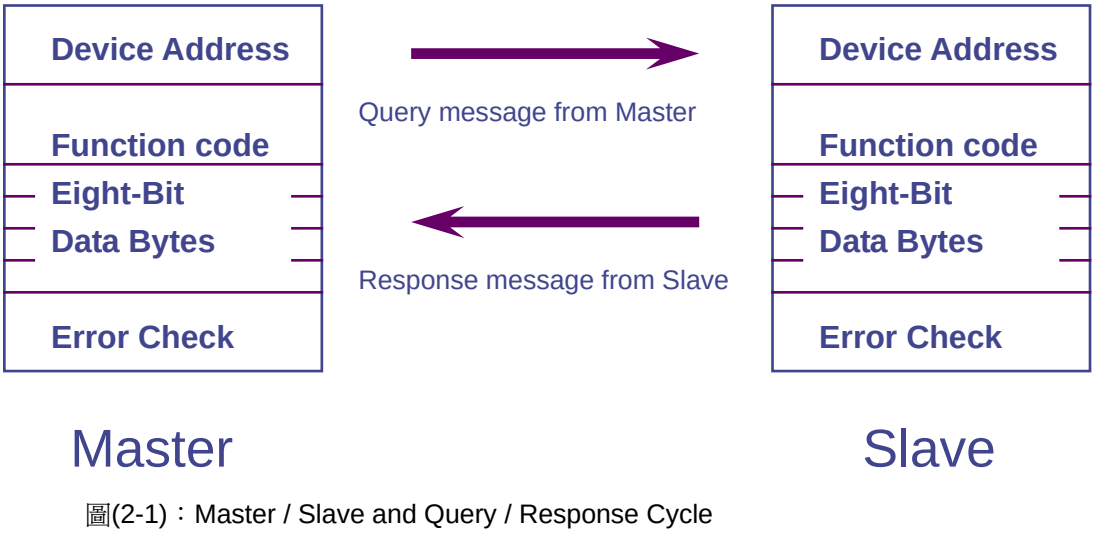
自控界主流通信規約 Modbus 詳解

Modbus 通信規約說明

Modbus 通信規約基本上是遵循 Master and Slave 的通信步驟，有一方扮演 Master 角色採取主動詢問方式，送出 Query Message 給 Slave 方，然後由 Slave 方依據接到的 Query Message 內容準備 Response Message 回傳給 Master。即使目前硬體通信已經可以達到雙方互相主動通信的能力，但是於 Modbus 通信規約的規定，必須一方爲 Master，另一方爲 Slave 不能互換角色。一般使用上，監控系統(HMI)都爲 Master，PLC、電表、儀表等都爲 Slave，HMI 系統一直 Polling Slave 的各種 relay and register 最新數值，然後做顯示及各種邏輯計算及控制調整等處理。

1 共用的通信規約

1.1 Query and Response Cycle



圖(2-1)：Master / Slave and Query / Response Cycle

Device Address：表示該設備的編號，於同一個串列式網路上此爲唯一的號碼。於 TCP/IP 上可以使用 IP Address 區分之，所以該 Device Address 保留此欄位可以使用或不使用。

Function Code：表示要求 Slave 處理各種不同資料或程序的 Command，以不同的 Function Number 來區方之。

Eight-Bit Data Bytes：依據 Function Code 而有不同的詳細資料定義，Slave 設備依據此兩欄位資料，做各種處理。

Error Check：當通信傳送資料時，因考慮信號可能會受外界干擾，所以必須加上 Error Check Code，使得 message 接收方可以就接到的資料再計算一次 Code，如果正確則做正常處理，不正確則不做處理。於串列式通信規定有 CRC and LRC 等兩種方式。於 TCP/IP 通信，因爲通信 Error Check 已經被 TCP/IP 的階層處理掉，所以於 Modbus/TCP 通信規約上不用此欄位。

- TCP/IP 格式：

起始字元組	Device Address	Function Code	Data	Error check	結束規定
6 個起始字元	8 Bits	8 Bits	Number of 8 Bits	不使用	不使用

圖(2-4)：TCP/IP data format

- 起始字元組：於前面再多加 6 個字元，以定義一些 TCP/IP 的需要係數。說明如下：
  Byte 0：本次通信 Message 的編號以 2 bytes 整數（Byte 0、1）表示，此 byte 爲上字元，一般是由 Master 編號之，以區分每次 Message。如果是 Slave 則將 Master 傳來的 Query Message 照轉至 Response Message。
  Byte 1：本次通信 Message 的編號下字元。
  Byte 2：通信規約識別號碼以 2 bytes 整數（Byte 2、3）表示，此 byte 爲上字元，於此處爲零。
  Byte 3：通信規約識別號碼下字元，於此處爲零。
  Byte 4：Message 長度以 2 bytes 整數（Byte 4、5）表示，此 byte 爲上字元（由 Device Address 至 Data 爲止），因爲長度不能超過 256 位元，所以此位元永遠爲零。
  Byte 5：Message 長度下字元（由 Device Address 至 Data 爲止）。
- 由 Device Address 至 Data 內容同 RTU 格式。
- Modbus 規定 IP Port No. 爲 502。

- 舉例說明三種格式：

Function Code-3 讀取 Output Register 數值爲例。Device address：6。Start Address：40123（Modbus 規定 Output Register 由 40001 開始）。通信規約內則將 40001 去除，以 122 表示也就是十六進位 0x007A、讀取點數：3。

Query Message	通信內容 十六進位	ASCII Code	RTU 8-bits field 二進位	TCP 8-bits field 二進位
TCP Byte-0				0000 0000
TCP Byte-1				0000 0001
TCP Byte-2				0000 0000
TCP Byte-3				0000 0000
TCP Byte-4				0000 0000
TCP Byte-5				0000 0110
ASCII 起始字元		:		
Device Address	06	0 6	0000 0110	0000 0110

Function Code	03	0 3	0000 0011	0000 0011
Start Address (Hi byte)	00	0 0	0000 0000	0000 0000
Start Address (Lo byte)	7A	7 A	0111 1010	0111 1010
No. of registers (Hi byte)	00	0 0	0000 0000	0000 0000
No. of register (Lo byte)	03	0 3	0000 0011	0000 0011
Error Check Byte-0				
Error Check Byte-1				
結束字元		<CR><LF>		

圖(2-5)：Example of Query Message

回傳的 3 點 register 數值爲 789、12345、-567 也就是十六進位 0x0315、0x3039、0xFDC9 等

Response Message	通信內容 十六進位	ASCII Code	RTU 8-bits field 二進位	TCP 8-bits field 二進位
TCP Byte-0				0000 0000
TCP Byte-1				0000 0001
TCP Byte-2				0000 0000
TCP Byte-3				0000 0000
TCP Byte-4				0000 0000
TCP Byte-5				0000 1001
ASCII 起始字元		:		
Device Address	06	0 6	0000 0110	0000 0110
Function Code	03	0 3	0000 0011	0000 0011
Byte count	06	0 6	0000 0110	0000 0110
Data-1 (Hi byte)	03	0 3	0000 0011	0000 0011
Data-1 (Lo byte)	15	1 5	0001 0101	0001 0101
Data-2 (Hi byte)	30	3 0	0011 0000	0011 0000
Data-2 (Lo byte)	39	3 9	0011 1001	0011 1001
Data-3 (Hi byte)	FD	F D	1111 1101	1111 1101
Data-3 (Lo byte)	C9	C 9	1100 1001	1100 1001
Error Check Byte-0				
Error Check Byte-1				
結束字元		<CR><LF>		

圖(2-6)：Example of Response Message

1.2 Function Code 說明

Function Code 有二十幾種，但是一般使用上都以 1、2、3、4、5、6、15、16 等八種最爲常用，以及另外特殊使用的 20、21 兩種，此爲 General Reference Register，絕大部份的 Modbus 設備並不會提供此 Register。於 PLC 上主要的控制資料有下列四種型式。此八種 Function Code 就是處理這些控制資料，詳細說明如下各點：

控制資料四種型式：

- DI：Digital Input，以一個 bit 表示 On/Off，用來記錄控制信號的狀態輸入，例如：開關，接觸點，馬達運轉，超限 switch…等等。於 PLC 上被稱爲 Input relay、input coil 等。
- DO：Digital Output，以一個 bit 表示 On/Off，用來輸出控制信號，以啓動或停止馬達，警鈴，燈光…等等。於 PLC 上被稱爲 Output relay、Output coil 等。
- AI：Analog Input，以 16 bits integer 表示一個數值，用來記錄控制信號的數值輸入，例如：溫度、流量、料量、速度、轉速、檔板開度、液位、重量…等等。於 PLC 上被稱爲 Input register。
- AO：Analog Output，以 16 bits integer 表示一個數值，用來輸出控制信號的數值，例如：溫度、流量、速度、轉速、檔板開度、飼料量…等等設定值。於 PLC 上被稱爲 Output register、Holding register。

Modbus Function Code	說明
01	Read Coil Status (output relay)
02	Read Input Status (input relay)
03	Read Holding Registers (output register)
04	Read Input Registers
05	Force Single Coil
06	Preset Single Register
15	Force Multiple Coils
16	Preset Multiple Registers
65 to 72	開放給一般使用者定義
100 to 110	開放給一般使用者定義

圖(2-7)：Modbus Function Code 一覽表

以下說明常用 10 種 Function Code：每種 Function Code 以舉例說明其中間 Message 的格式至於前面的 TCP Byte，ASCII 起始字元及後面的 Error Check、結束字元等都是一樣規定，參考前一節內容即可。

Function Code-1：讀取 DI 資料，於 Modbus 規定 Relay Address 由 00001 開始。但是通信規約內取後面四位數，且由零起算，例如：於文件上 Relay Address 爲 00345，其通信規約內轉換的 Address 爲 344。

由 Device Address 17 讀取 Relay Address 20 – 32 的 DI 資料，通信規約內 Start Address 爲 19，讀取點數 13。

Query Message	通信內容 十六進位
Device Address	11
Function Code	01
Start Address (Hi byte)	00
Start Address (Lo byte)	13
No. of points (Hi byte)	00
No. of points (Lo byte)	0D

回傳資料以一個 Byte 即 8 bits 爲一組，每一個 Bit 表示一點 Relay On/Off 狀態。例如下表
Data(Relay 27 – 20)的狀態爲 ON-ON-OFF-ON-OFF-OFF-ON-ON。
Data(Relay 32 – 28)的狀態爲 OFF-ON-OFF-ON-ON-ON。（前面 3 bit 不算，因爲只到 Relay 32 爲止）
其個別 Relay 狀態，舉例： Relay 27 爲 ON、Relay 31 爲 ON、Relay 23 爲 OFF。

Response Message	通信內容 十六進位
Device Address	11
Function Code	01
Byte count	02
Data (Relay 27 – 20)	D3
Data (Relay 32 – 28)	17

圖(2-8)：Example of Function Code - 1 Message

Function Code-2：讀取 DO 資料，於 Modbus 規定 Relay Address 由 10001 開始。但是通信規約內取後面四位數，且由零起算，例如：於文件上 Relay Address 爲 10678，其通信規約內轉換的 Address 爲 677。

由 Device Address 23 讀取 Relay Address 10102 – 10134 的 D0 資料，通信規約內 Start Address 爲 101，讀取點數 33。

Query Message	通信內容 十六進位
Device Address	17
Function Code	02
Start Address (Hi byte)	00
Start Address (Lo byte)	65
No. of points (Hi byte)	00
No. of points (Lo byte)	21

回傳資料以一個 Byte 即 8 bits 爲一組，每一個 Bit 表示一點 Relay On/Off 狀態。例如下表
Data(Relay 109 – 102)的狀態爲 ON-OFF-ON-OFF-ON-OFF-ON-OFF。
Data(Relay 117 – 110)的狀態爲 OFF-ON-OFF-OFF-OFF-ON-OFF-ON。
Data(Relay 125 – 118)的狀態爲 OFF-OFF-ON-OFF-OFF-ON-ON-ON。
Data(Relay 133 – 126)的狀態爲 ON-OFF-OFF-OFF-OFF-OFF-ON-ON。
Data(Relay 134 – 134)的狀態爲 ON。（前面 7 bit 不算，因爲只到 Relay 134 爲止）

Response Message	通信內容 十六進位
Device Address	17
Function Code	02
Byte count	05
Data (Relay 109 – 102)	AA
Data (Relay 117 – 110)	45
Data (Relay 125 – 118)	27
Data (Relay 133 – 126)	83
Data (Relay 134 – 134)	01

圖(2-9)：Example of Function Code - 2 Message

Function Code-3：讀取 AO 資料，於 Modbus 規定 Register Address 由 40001 開始。但是通信規約內取後面四位數，且由零起算，例如：於文件上 Register Address 爲 44321，其通信規約內轉換的 Address 爲 4320。

由 Device Address 41 讀取 Register Address 40765 – 40770 的 A0 資料，通信規約內 Start Address 爲 764，讀取點數 6。

Query Message	通信內容 十六進位
Device Address	29
Function Code	03
Start Address (Hi byte)	02
Start Address (Lo byte)	FC
No. of registers (Hi byte)	00
No. of registers (Lo byte)	06

回傳資料以兩個 Bytes 表示 16 bits 整數值。例如下表

Register 40765 整數值：99
Register 40766 整數值：12336
Register 40767 整數值：－1417
Register 40768 整數值：789
Register 40769 整數值：767
Register 40770 整數值：1

Response Message	通信內容 十六進位
Device Address	29
Function Code	03
Byte count	0C
Data-1 (Hi byte)	00
Data-1 (Lo byte)	63
Data-2 (Hi byte)	30
Data-2 (Lo byte)	30
Data-3 (Hi byte)	FA
Data-3 (Lo byte)	77
Data-4 (Hi byte)	03
Data-4 (Lo byte)	15
Data-5 (Hi byte)	02
Data-5 (Lo byte)	FF
Data-6 (Hi byte)	00
Data-6 (Lo byte)	01

圖(2-10)：Example of Function Code - 3 Message

Function Code-4：讀取 AI 資料，於 Modbus 規定 Register Address 由 30001 開始。但是通信規約內取後面四位數，且由零起算，例如：於文件上 Relay Address 爲 30988，其通信規約內轉換的 Address 爲 987。

由 Device Address 30 讀取 Register Address 30123 – 30127 的 AI 資料，通信規約內 Start Address 爲 122，讀取點數 5。

Query Message	通信內容 十六進位
Device Address	1E
Function Code	04
Start Address (Hi byte)	00
Start Address (Lo byte)	7A
No. of registers (Hi byte)	00
No. of registers (Lo byte)	05

回傳資料以兩個 Bytes 表示 16 bits 整數值。例如下表
Register 30123 整數值：2581
Register 30124 整數值：57
Register 30125 整數值：969
Register 30126 整數值：－24544
Register 30127 整數值：170

Response Message	通信內容 十六進位
Device Address	1E
Function Code	04
Byte count	0A
Data-1 (Hi byte)	0A
Data-1 (Lo byte)	15
Data-2 (Hi byte)	00
Data-2 (Lo byte)	39
Data-3 (Hi byte)	03
Data-3 (Lo byte)	C9
Data-4 (Hi byte)	A0
Data-4 (Lo byte)	20
Data-5 (Hi byte)	00
Data-5 (Lo byte)	AA

圖(2-11)：Example of Function Code - 4 Message

Function Code-5：寫入 DO 一點資料，Address 規定與 Function Code-2 一樣。

由 Device Address 10 寫入 Relay Address 10012 的 D0 資料，通信規約內 Start Address 爲 11。如果設定爲 ON 於 Force Data 設定十六進位 0xFF00，如果設定爲 OFF 於 Force Data 設定十六進位 0x0000。

Query Message	通信內容 十六進位
Device Address	0A
Function Code	05
Start Address (Hi byte)	00
Start Address (Lo byte)	0B
Force Data (Hi byte)	FF
Force Data (Lo byte)	00

以 Query Message 作爲 Response Message 傳回。

Response Message	通信內容 十六進位
Device Address	0A
Function Code	05
Start Address (Hi byte)	00
Start Address (Lo byte)	0B
Force Data (Hi byte)	FF
Force Data (Lo byte)	00

圖(2-12)：Example of Function Code - 5 Message

Function Code-6：寫入 AO 一點資料，Address 規定與 Function Code-3 一樣。

由 Device Address 13 寫入 Register Address 40112 的 A0 資料，通信規約內 Start Address 爲 111。設定 16 bits 整數值爲 999 即是十六進位 0x03E7。

Query Message	通信內容 十六進位
Device Address	0D
Function Code	06
Start Address (Hi byte)	00
Start Address (Lo byte)	6F
Preset Data (Hi byte)	03
Preset Data (Lo byte)	E7

以 Query Message 作爲 Response Message 傳回。

Response Message	通信內容 十六進位
Device Address	0D
Function Code	06
Start Address (Hi byte)	00
Start Address (Lo byte)	6F
Preset Data (Hi byte)	03
Preset Data (Lo byte)	E7

圖(2-13)：Example of Function Code - 6 Message

Function Code-15：寫入 DO 多點資料，Address 規定與 Function Code-2 一樣。

由 Device Address 17 寫入 Relay Address 10011 – 10022 的 D0 資料，通信規約內 Start Address 爲 10，寫入點數 12。所設定狀態如下：

第一個 Force Data byte

Bit	0	1	0	1	0	1	0	1
Relay	18	17	16	15	14	13	12	11

第二個 Force Data byte

Bit	0	0	0	0	0	0	1	1
Relay	-	-	-	-	22	21	20	19

Query Message	通信內容 十六進位
Device Address	11
Function Code	0F
Start Address (Hi byte)	00
Start Address (Lo byte)	0A
No. of relay (Hi byte)	00
No. of relay (Lo byte)	0C
Byte Count	02
Force Data (Relay 18 – 11)	55
Force Data (Relay 22 – 19)	03

以 Query Message 前面 6 bytes 作爲 Response Message 回傳。

Response Message	通信內容 十六進位
Device Address	11
Function Code	0F
Start Address (Hi byte)	00
Start Address (Lo byte)	12
No. of relay (Hi byte)	00
No. of relay (Lo byte)	03

圖(2-14)：Example of Function Code - 15 Message

Function Code-16：寫入 AO 多點資料，Address 規定與 Function Code-3 一樣。

由 Device Address 39 寫入 Register Address 40310 – 40312 的 A0 資料，通信規約內 Start Address 爲 309，寫入點數 3。寫入數值如下所示：每個 register 數值爲 16 bits 整數值。
Register 40310 設定值：784
Register 40311 設定值：12706
Register 40312 設定值：－16183

Query Message	通信內容 十六進位
Device Address	27
Function Code	10
Start Address (Hi byte)	01
Start Address (Lo byte)	35
No. of registers (Hi byte)	00
No. of register (Lo byte)	03
Byte count	06
Data-1 (Hi byte)	03
Data-1 (Lo byte)	10
Data-2 (Hi byte)	31
Data-2 (Lo byte)	A2
Data-3 (Hi byte)	C0
Data-3 (Lo byte)	C9

以 Query Message 前面 6 bytes 作爲 Response Message 回傳。

Response Message	通信內容 十六進位
Device Address	27
Function Code	10
Start Address (Hi byte)	01
Start Address (Lo byte)	35
No. of registers (Hi byte)	00
No. of register (Lo byte)	03

圖(2-15)：Example of Function Code - 16 Message

2 TCP/IP 的通信規約

Modbus/TCP 主要格式已於「1.2.資料基本格式」說明清楚。此處再提醒讀者的是 IP Address 與 Modbus Address 的區分，Slave 設備必須具有給外部多個 Master 連線的能力。

2.1 IP Address 與 Modbus Address 的區分

於同一 Ethernet 網路系統上 IP Address 必須是唯一的，可以說如同 Modbus Address 的唯一編號來區分串列式連線上的各別設備。其主要差別在於 IP Address 是由作業系統面所管理，Modbus Address 則是由通信規約內所制定的。於 Modbus/TCP 通信規約的定義，其 Modbus Address 欄位還是被保留，但是可以不用。因此市面上 Modbus/TCP 的設備，此欄位值有些永遠設定爲零，有些還是沿用，需要特別注意，否則可能無法連線。

2.2 Modbus Slave 設備需具備被多個 Master 連線架構

於串列式通信上只有一個Modbus Master設備，然後下面連上多台Modbus Slave設備。也就是說，每次通信一定由Modbus Master主動送出Query Message，然後某一台Slave回應Response Message，一次只有一個通信再進行。但是於Ethernet網路上，則可能有多個Modbus Master同時會連線至同一台Modbus Slave上，此時Slave系統就要有接受多個連線架構的功能。所以一般具備Modbus/TCP Slave設備，都會列出最多允許幾個Master連線的規格。