Modbus RTU 通訊協定介紹

Modicon

Modicon 是一家做 PLC (可程式邏輯控制器)的廠商, 一般 PLC 控制器內部常用處理資料有位元(Bit, 1bit)及字組(WORD,16bits).

Modicon PLC 針對控制器內部變數 進一步定義

輸入接點	[Input]	(Bit, 1bit)
輸出接點	[Coil]	(Bit, 1bit)
輸入字組	[input registers]	(WORD,16bits)
保持字組	[Holding Register]	(WORD,16bits)

Modicon PLC 變數定義

Modicon PLC 變數名稱, 都是以數字定義的.

Modicon PLC 變數定義(**完整**)

變數	讀/寫	**變數名稱開頭**	變數數量	**變數名稱及範圍**
輸入接點 [Input]	唯讀	**1**	65536(Bits)	**100001 ~ 165536**
輸出接點 [Coil]	讀寫	**0**	65536(Bits)	**000001 ~ 065536**
輸入字組 [input registers]	唯讀	**3**	65536(Word)	**300001 ~ 365536**
保持字組 [Holding Register]	讀寫	**4**	65536(Word)	**400001 ~ 465536**

Modicon PLC 完整變數名稱都是 6 位數, 1 個<資料別>**變數名稱數字**+5 個地址數字.

但有些設備變數地址都小於 10000, 所以有另個簡易的定址

Modicon PLC 變數定義(**簡易**)

變數	讀/寫	**變數名稱開頭**	變數數量	**變數名稱及範圍**
輸入接點 [Input]	唯讀	**1**	10000(Bits)	**10001 ~ 19999**
輸出接點 [Coil]	讀寫	**0**	10000(Bits)	**00001 ~ 09999**
輸入字組 [input registers]	唯讀	**3**	10000(Word)	**30001 ~ 39999**
保持字組 [Holding Register]	讀寫	**4**	10000(Word)	**40001 ~ 49999**

Modicon PLC 簡易變數名稱都是 5 位數, 1 個<資料別>**變數名稱數字**+4 個地址數字.

Protocol(通訊協定)

Modicon 有針對所屬 PLC, 設計的通訊協定 名稱就叫 **Modbus**

Modbus 一般有三種通訊協定

通訊協定	通訊媒介	編碼系統	校驗碼
Modbus ASCII	串列	ASCII(0–9, A–F)	LRC
Modbus RTU	**串列**	**8–bit binary**	**CRC16**
Modbus TCP	網路/TCP	8–bit binary	by TCP checksum

為什麼要用 Modbus RTU????

因為 Modbus RTU 通訊格式(資料編碼),通訊效率是優良的!
因為 Modbus RTU 是一個公開的通訊協定!
因為 Modbus RTU 是一個公開的通訊協定!
因為 Modbus RTU 是一個公開的通訊協定! (因為很重要,要寫三次)
通訊協定資料 https://modbus.org/docs/PI_MBUS_300.pdf

Modbus RTU 通訊架構

Modbus RTU 通訊, 是主從架構, 1 個**主站(Master)**, 多個**從站(Slave, 一個從站也可以)**.以半雙工方式通訊.
一個至多個從站,以站號(Byte, 0~255, 一般 0 跟 255 保留給特定用途)來區分,
一個通訊裝置(從站)分配一個站號.(主站不需要站號!!!)

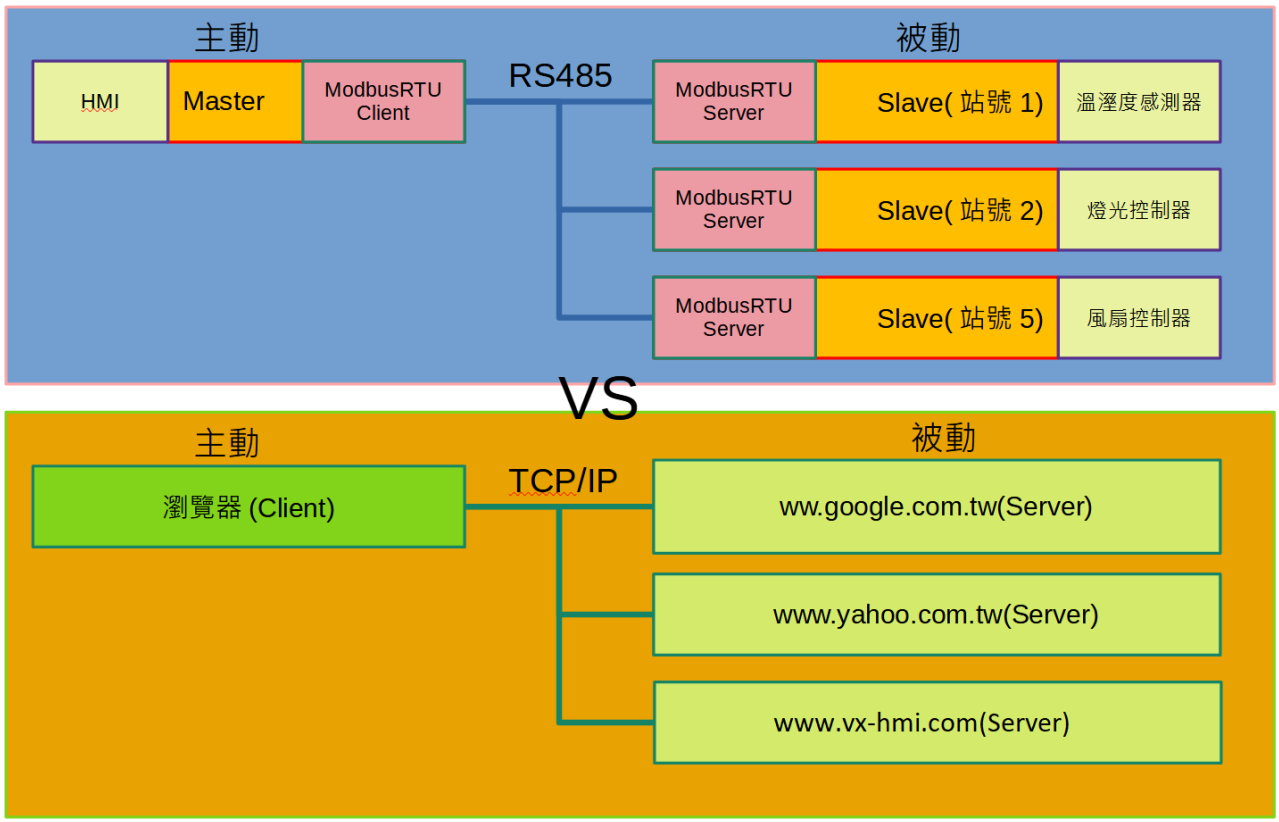
以線路的角度來看

傳輸線路	Voltage System	傳輸特性	組態	ModbusRTU 通訊
TTL	Voltage level-based	全雙工	Point-to-point	一個 Master, 一個 Slave
RS-232	Voltage level-based	全雙工	Point-to-point	一個 Master, 一個 Slave
RS-485	**Differential**	**半雙工**	**Multi-drop**	**一個 Master, 一個至多個 Slave**

透過 RS485 可以實現多台機器通訊, 其他(TTL,RS-232)只能 2 台之間通訊

Modbus RTU 通訊方式

Modbus RTU 通訊中,**Master 主宰的通訊秩序**.
只有 Master 可以發出通訊要求, 對應站號的 Slave 回應通訊要求.



Modbus RTU 通訊順序

以上圖架構為範例

Master:發出通訊站號 1, 讀取 400001~400004(數量 4 個 WORD).
同時接收封包的 Slave(1):回應通訊, 傳回 400001~400004 變數.
同時接收封包的 Slave(2):站號不對,不回應.
同時接收封包的 Slave(5):站號不對,不回應.

Master:發出通訊站號 5, 寫入 400010~400011(數量 2 個 WORD).
同時接收封包的 Slave(1):站號不對,不回應.
同時接收封包的 Slave(2):站號不對,不回應.
同時接收封包的 Slave(5):回應通訊, 將 接收的 400010~400011 變數, 寫入控制器內部對應變數位置.

Master:發出通訊站號 2, 讀取 400020~400021(數量 2 個 WORD).
同時接收封包的 Slave(1):站號不對,不回應.
同時接收封包的 Slave(2):回應通訊, 傳回 400020~400021 變數.
同時接收封包的 Slave(5):站號不對,不回應.
....
上述 站號,讀或寫,變數位址,都可依實際應用修改.

Modbus RTU 通訊封包

https://modbus.org/docs/PI_MBUS_300.pdf Page9

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1–T2–T3–T4	8 BITS	8 BITS	*n* x 8 BITS	16 BITS	T1–T2–T3–T4

Figure 4 RTU Message Frame

PI–MBUS–300 **Modbus Protocol 9**

Modbus RTU 是以時間間隔(START,END) 來區分封包. 時間間格大於 3.5 字元傳送時間.
(以 9600N81 計算,(1/9600)*10)*3.5=3.645ms)

ADDRESS 欄位: 標示 Slave 站號

FUNCTION 欄位: 標示此通訊功能碼(是讀取還是寫入, 變數是 0,1,3,4?)

DATA 欄位:對應每個 <通訊功能碼> 有不同的資料格式, 需參考 通訊功能碼格式.

CRC CHECK 欄位:ModbusRTU 檢查碼(CRC16), CRC16 程式碼可參考
https://modbus.org/docs/PI_MBUS_300.pdf Page114

ModbusRTU 通訊功能碼

變數類別	讀/寫	通訊功能碼	功能碼敘述	功能碼資料格式
0	讀取	01	Read Coil Status	page24
	寫入	05	Force Single Coil	page32
1	讀取	02	Read Input Status	page26
3	讀取	04	Read Input Registers	page30
4	讀取	03	Read Holding Registers	page28
	單一變數寫入	06	Preset Single Register	page34
	多個變數寫入	16(10 Hex)	Preset Multiple Regs	page46

功能碼資料格式文件:https://modbus.org/docs/PI_MBUS_300.pdf

ModbusRTU 通訊封包範例(Master)

Master 讀取站號 33,變數 401000~401003 (https://modbus.org/docs/PI_MBUS_300.pdf page28)

03 Read Holding Registers

Description

Reads the binary contents of holding registers (4X references) in the slave. Broadcast is not supported.

Appendix B lists the maximum parameters supported by various controller models.

Query

The query message specifies the starting register and quantity of registers to be read. Registers are addressed starting at zero: registers 1–16 are addressed as 0–15.

Here is an example of a request to read registers 40108–40110 from slave device 17:

QUERY

Field Name	Example (Hex)
Slave Address	11
Function	03
Starting Address Hi	00
Starting Address Lo	6B
No. of Points Hi	00
No. of Points Lo	03
Error Check (LRC or CRC)	—

Figure 14 Read Holding Registers – Query

Slave Address	21H	站號:33, 等於 16 進位 21H.
Function	03H	功能碼:03, 等於 16 進位 03H.
Starting Address Hi	03H	**變數 401000, 對應地址為 999,(地址為去掉變數類別字 4, 數字減 1) 地址 999 等於 16 進位 03E7H.**
Starting Address Lo	E7H	
No. of Points Hi	00H	401000~401003, 變數總共 4 個, 等於 16 進位 0004H.
No. of Points Lo	04H	
CRC Lo	F3H	CRC16 [210303E70004] = 1AF3H
CRC Hi	1AH	

所以 Master 要 讀取站號 33,變數 401000~401003, 要傳送 8Bytes, [210303E70004F31A].

ModbusRTU 通訊封包範例(Slave)

Slave(33)回應 讀取站號 33,變數 401000~401003
(https://modbus.org/docs/PI_MBUS_300.pdf page29)

Response

The register data in the response message are packed as two bytes per register, with the binary contents right justified within each byte. For each register, the first byte contains the high order bits and the second contains the low order bits.

Data is scanned in the slave at the rate of 125 registers per scan for 984–X8X controllers (984–685, etc), and at the rate of 32 registers per scan for all other controllers. The response is returned when the data is completely assembled.

Here is an example of a response to the query on the opposite page:

RESPONSE

Field Name	Example (Hex)
Slave Address	11
Function	03
Byte Count	06
Data Hi (Register 40108)	02
Data Lo (Register 40108)	2B
Data Hi (Register 40109)	00
Data Lo (Register 40109)	00
Data Hi (Register 40110)	00
Data Lo (Register 40110)	64
Error Check (LRC or CRC)	—

Figure 15 Read Holding Registers – Response

The contents of register 40108 are shown as the two byte values of 02 2B hex, or 555 decimal. The contents of registers 40109–40110 are 00 00 and 00 64 hex, or 0 and 100 decimal.

Slave Address	21H	站號:33, 等於 16 進位 21H.
Function	03H	功能碼:03, 等於 16 進位 03H.
Byte Count	08H	讀取變數 4 個 WORD, 等於 8 個 BYTE, 等於 16 進位 08H.
Data Hi (401000)	30H	預設變數為:12345 等於 16 進位 3039H.
Data Lo (401000)	39H	
Data Hi (401001)	D4H	預設變數為:54321 等於 16 進位 D431H.
Data Lo (401001)	31H	
Data Hi (401002)	1AH	預設變數為:6666 等於 16 進位 1A0AH.
Data Lo (401002)	0AH	
Data Hi (401003)	22H	預設變數為:8888 等於 16 進位 22B8H.
Data Lo (401003)	B8H	
CRC Lo	C4H	CRC16 [2103083039D4311A0A22B8] = 18C4H
CRC Hi	18H	

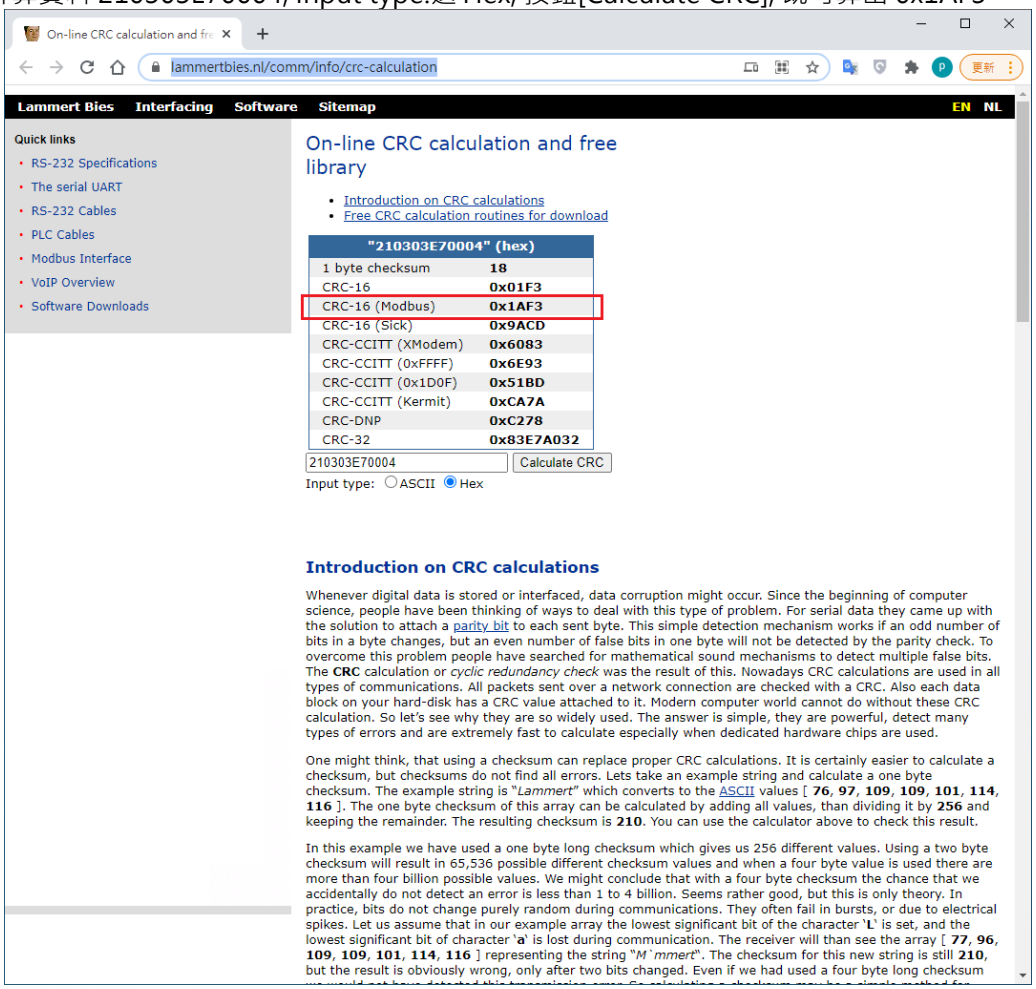
所以 Slave(33)要 回應主站,讀取站號 33,變數 401000~401003,
要傳送 13Bytes, [2103083039D4311A0A22B8C418].

ModbusRTU 通訊封包 CRC 計算檢查

除了原廠文件內所附的程式碼(https://modbus.org/docs/PI_MBUS_300.pdf Page114),另可在網頁另行進行檢查

https://www.lammertbies.nl/comm/info/crc-calculation

填入計算資料 210303E70004, Input type:選 Hex, 按鈕[Calculate CRC], 既可算出 0x1AF3



參考資料:
Modicon: https://www.se.com/tw/zh/work/products/master-ranges/modicon/
Modbus: https://zh.wikipedia.org/wiki/Modbus
CRC Calculation: https://www.lammertbies.nl/comm/info/crc-calculation
Modbus 文件: https://modbus.org/docs/PI_MBUS_300.pdf