

Modbus TCP 對應表

17

最後更新:2026-05-11 |  負責人:KC

此文件描述 MES I/O Gateway 的 **Modbus TCP** 雙向通訊規格：

- **Server (Slave)** 側:Gateway 開 listen socket,外部 HMI/SCADA 連進來讀寫內部 IO (§ 2- § 4)
- **Client (Master)** 側:Gateway 主動連外部 Modbus TCP slave,把 register 值橋接到內部變數池 (§ 7,2026-05-11 補上)

項目	值	備註
Server listen port	502 (韌體預設)	PRD-Factory-Test v1.2 一度誤標 5000,以韌體 Modbus TCP Server 實作為準
Address scheme	Zero-based	詳見 § 2
認證 / TLS	無	部署時靠網段隔離;未來看需求補

01

1. 架構特色 (v5.9)

為兼顧系統輕量性與最大擴充彈性,本專案採用 **0-based 固定位址對映 (Fixed Address Map)** 與 **Base-16 偏移法**,確保主機與未來擴充模組之位址空間絕不衝突。HMI 或 SCADA 得以直接對指定位址讀寫以完成控制與狀態蒐集。

2. 暫存器映射全域總覽 (Register Map)

類型代碼	通用名稱 (HMI 型號)	實際實體與對應位址	權限
0x	Coils	控制繼電器與 DO 輸出 (0-255)	R/W
1x	Discrete Inputs	讀取實體開關 DI 狀態 (0-255)	Read Only
3x	Input Registers	讀取類比訊號 AI 原始值 (0-255)	Read Only
4x	Holding Registers	系統內部變數池/快取區 (0-1023)	R/W

3. 實體 I/O 詳細位址分佈 (0x, 1x, 3x)

Gateway 主機與 5 組擴展模組的實體 I/O 透過「每模組 16-bit 為一個區間」進行無縫排列。若 HMI 需操作「Expansion 0」的第 1 個 DO，請寫入位址 $16 + 0 = 16$ 。

設備來源	Coils (0x) 位址 (寫/讀)	DIs (1x) 位址 (唯讀)	Input Regs (3x) 位址 (唯讀)
Host 主機	0 ~ 3 (DO1-DO4)	0 ~ 7 (DI0-DI7)	0 ~ 7 (AI0-AI7, 乘16倍)
(保留)	4 ~ 15	8 ~ 15	8 ~ 15
擴充模組 0	16 ~ 23	16 ~ 31	16 ~ 23
擴充模組 1	32 ~ 39	32 ~ 47	32 ~ 39
擴充模組 2	48 ~ 55	48 ~ 63	48 ~ 55
擴充模組 3	64 ~ 71	64 ~ 79	64 ~ 71
擴充模組 4	80 ~ 87	80 ~ 95	80 ~ 87

[AI (Input Register) 補充說明]: 內部 ADC 精度為 12-bit (0-4095) 轉換為 0-10V。為了與 16-bit 暫存器系統接軌，主機的 3x AI 數值已經乘以 16 倍，輸出範圍為 **0 ~ 65520** (等比例對應 0~10V)。

04

4. 虛擬數據位址分佈 (4x Holding Registers)

系統提供大量 (1024 槽位) 高速陣列 SRAM 空間供 Modbus TCP 存取，適合用作 **Rule Engine** 聯動目標或 **TCP Parser** 資料傾印。建議的規劃區段如下：

Holding Regs (4x)	推薦用途	實作現況 (v5.9)
0 ~ 99	內部系統控制變數池 (VAR0-VAR15)	支援以 Rule Engine 直接存取與覆寫。
100 ~ 199	TCP 通道數據區段 (信號輸入)	[系統自動分配預設位址] 給予那些在 TCP IO 被設定為「  輸入」的通道供外部 SCADA 寫入。
200 ~ 499	TCP 通道數據區段 (狀態輸出)	[系統自動分配預設位址] 給予那些在 TCP IO 被設定為「  輸出」的通道供外部 SCADA 讀取。
500 ~ 1011	(保留供 Modbus RTU 或進階應用)	目前作為暫存緩衝保留。
1012 ~ 1023	系統擴充保留區	保留供未來特定系統狀態使用。

4.1. TCP 通道 (TCP I/O) 暫存器配置原則

當通道選擇協議為 **Modbus TCP** 時，代表該通道會在 MES I/O Gateway 本機的 **4x Holding Registers** 空間中配置一塊區域，這使 Gateway 本身做為一個 **Modbus Server (Slave)** 供外部設備 (HMI / SCADA) 連線訪問。

配置規則 (自動指派機制)：

- **方向為「 輸入」**:如果您將 Holding Register 設為 **0** (自動分配),韌體會從 **100** 開始尋找空位配發。外部圖控即可透過存取這段位址,將最新的狀態資訊寫入給 Gateway 以觸發內部規則(被動抓取信號)。
- **方向為「 輸出」**:如果您將 Holding Register 設為 **0** (自動分配),韌體會從 **200** 開始尋找空位配發。外部圖控即可透過存取這段位址,讀取出本通道最新的產出資料或是經過 Converter 轉換完成的緩衝數據。

(註:若您有多字組長度需求,例如連續 8 個 Words,SCADA 直接對該起始分配位址進行連續區塊存取即可。)

05

5. 常見問答 (FAQ)

- **Q: HMI 面板要求打「偏移量」,我需要加 1,還是加 40001? A:** MES I/O Gateway 遵從工業標準的 **Zero-based Addressing**。請直接在「位址 (Address)」欄位填入本表列出的數字 (**0、16、32...**)。若您的軟體要求格式如 **40001**、**10017**,請注意那些通常是 **1-based** (加一偏移),本系統一律以最純粹的 **Base-Address 0** 為設計核心。

06

6. 測試與驗證 (2026-05-11 補)

由於缺乏實機 Modbus TCP 治具,採用 **pymodbus 模擬器** 跑端到端:

工具	用途
<code>scripts/modbus-sim/master_client.py</code>	模擬外部 SCADA / HMI,連到 Gateway :502 讀寫
<code>scripts/modbus-sim/slave_server.py</code>	模擬外部 Modbus TCP slave,給 Gateway 當 client 連
<code>scripts/modbus-sim/smoke_test.sh</code>	端到端 smoke test 腳本,產出缺口報告

可用上述腳本對 Gateway :502 做端到端讀寫驗證, `smoke_test.sh` 會產出涵蓋與缺口報告。

07

7. Client 側 (Gateway 當 Master 連外部 Slave)

對應 firmware `modbusTcpTargets[]`、設定頁「Modbus TCP Targets」區塊 (WI-043 / WI-051)。

Gateway 可同時對多個外部 Modbus TCP slave 設備發起連線並輪詢。每個 target 在配置中包含：

欄位	說明
<code>host</code>	slave 的 IP 或 hostname
<code>port</code>	通常 <code>502</code>
<code>slaveId</code>	Modbus unit ID (多數設備用 1)
<code>pollIntervalMs</code>	輪詢間隔 (建議 ≥ 1000)
<code>registers[]</code>	要讀取的 holding/input register 清單

讀進來的值會橋接到內部變數池 (VAR0~VAR15)，可被 RuleEngine 當 signal source 使用。

7.1 限制與設計原則

- **單向讀取為主**：目前 Client 側只支援讀 (FC03/FC04)，寫入請走 RS485 路徑 (透過 Converter 回寫 RS485 暫存器, 32 位元值跨兩暫存器並需注意 Endianness)。Modbus TCP 寫入是後續延伸 (暫無需求)
- **連線失敗 retry**：失敗會自動退避重試，連續 N 次失敗會在 UI 顯示告警
- **target 數量上限**：目前韌體預留 4 個 slot

7.2 Client telemetry (WI-117 Gap 5, v5.9.97+)

`GET /api/modbus-tcp/targets` 回傳的每個 target object 額外帶下列欄位 (皆為 runtime, 不存檔)：

欄位	型別	說明
<code>lastSuccessMs</code>	<code>uint32</code>	最近一次成功 poll 的 <code>millis()</code> 時間戳 (0 = 從未成功)
<code>lastErrorMs</code>	<code>uint32</code>	最近一次失敗 poll 的 <code>millis()</code> 時間戳 (0 = 從未失敗)
<code>successCount</code>	<code>uint32</code>	開機後成功 poll 累計數
<code>errorCount</code>	<code>uint32</code>	開機後失敗 poll 累計數
<code>nowMs</code>	<code>uint32</code>	韌體目前的 <code>millis()</code> , 前端可用 <code>(nowMs - lastSuccessMs)</code> 算出「上次成功幾秒前」

`POST /api/modbus-tcp/targets` 改動目標設定時, 所有上述計數會被歸零。

詳細 UI 操作流程見操作手冊 Modbus TCP 章節。

08

8. Server 側即時連線指標 (WI-117 Gap 1, v5.9.97+)

`GET /api/system` 回傳新增 `modbusTcp` 物件：

```
{
  "modbusTcp": {
    "port": 502,
    "running": true,
    "connections": 1,
    "requestCount": 1234,
    "errorCount": 2,
    "acceptedCount": 7,
    "rejectedUnitCount": 0,
    "lastRequestMs": 12345678,
    "lastClient": "192.168.51.10"
  }
}
```

欄位

說明

`connections`

目前活躍 socket 數 (韌體單實例最多 1)

`requestCount` /`errorCount`

累計處理／錯誤請求數 (含通訊錯誤與 exception 回應)

`acceptedCount`

累計接受連線次數 (重連會 +1)

`rejectedUnitCount`

因 § 9 unit-id 政策被拒絕的請求數

`lastRequestMs`最近一次成功處理的 `millis()` (前端可換算「N 秒前」)`lastClient`最近一次接受的對端 IP, UI 顯示在 dashboard  Modbus TCP 卡片

9. Unit ID 政策（WI-117 Gap 3，v5.9.97+）

Modbus TCP 慣例：

Unit ID	政策	韌體行為
0	broadcast	靜默丟棄，不回應
1	primary slave	接受並處理
2 ~ `254`	對應其他下游 slave	回 exception code 0x0B (Gateway Target Device Failed to Respond)
255	TCP-only sentinel / "any"	接受並處理

被拒絕的請求會累加到 `/api/system → modbusTcp.rejectedUnitCount`，方便 SCADA 整合排錯。