Modbus: ¿registro 40001 o dirección 0? 6 comprobaciones

El manual dice 40001, el master lee 40001 y recibes el valor del registro siguiente o la excepción 02. Números como 40001 son una convención: en la trama, las direcciones empiezan en 0, así que el holding register 40001 viaja como dirección 0. Comprueba qué convención usan tu manual y tu software antes de leer. Válido para Modbus RTU y Modbus TCP.

Número de registro y dirección en la trama



Número, no dirección: la primera cifra indica la tabla y nunca se envía. El código de función elige la tabla.



Desfase de uno: una resta equivocada lleva la lectura al registro siguiente. La respuesta puede parecer válida.

No está en la especificación

La especificación de modbus.org solo dice que los datos se direccionan desde cero. 40001 y 4xxxx vienen de la convención Modicon que usan muchos manuales.

Lee antes de escribir

Prueba solo con lecturas hasta conocer la convención: escribir en el registro siguiente puede cambiar una consigna real.

Seis comprobaciones, en este orden

Comprobación	Qué hacer	Resultado correcto
1. Tabla	Primera cifra: 0 coils, 1 discrete inputs, 3 input registers, 4 holding registers. No se envía: el código de función elige la tabla.	4xxxx se lee con FC 03.
2. Trama	En la trama, las direcciones empiezan en 0. El registro 40001 viaja como dirección 0 (0x0000).	Primer holding register = 0x0000.
3. Cálculo	Dirección = registro - 40001, no 40000. El registro 40010 es la dirección 9.	40010 da 9.
4. Seis cifras	400001 es el mismo primer registro, en una notación con sitio para las 65536 direcciones. Resta 400001.	400001 da 0.
5. Convención	Hay manuales con direcciones desde 0, otros desde 1 y otros en hexadecimal. Hay software que acepta 40001 y lo convierte; una librería puede esperar la dirección tal cual.	Manual y software usan la misma convención.
6. Prueba	Lee N y N-1 en un registro con un valor conocido (número de serie, versión, un valor de la pantalla). La excepción 02 también es una pista.	Uno de los dos coincide.

Qué indica el síntoma

Síntoma	Causas posibles	Siguiente paso
Recibes el valor del registro siguiente	Desfase de uno: has restado 40000, o el software ya convierte.	Comprobaciones 3 y 5; prueba N-1.
Excepción 02 en el último registro del mapa	Desfase de uno, o una cantidad que pasa del final del mapa.	Comprobación 6; reduce la cantidad.
Funciona desde el SCADA y no desde el PLC (o al revés)	Uno convierte 40001 y el otro espera la dirección.	Comprobación 5: ¿el campo pide registro o dirección?
El manual da 0x0000 o "dirección 0"	Ya es la dirección del protocolo.	No restes nada.
El manual da 400001	Notación de seis cifras.	Comprobación 4.
3xxxx leído con FC 03: excepción 02 o valor erróneo	Input register leído como holding register.	Comprobación 1: los input registers usan FC 04.

Según la especificación

- "In the PDU Registers are addressed starting at zero": los registros numerados del 1 al 16 se direccionan del 0 al 15.
- Cada dato se direcciona del 0 al 65535.
- Excepción 02, Illegal Data Address: la dirección, o la dirección más la cantidad, no está permitida en el servidor.

Tabla de conversión

0xxxx	coils	FC 01	- 1
1xxxx	discrete inputs	FC 02	- 10001
3xxxx	input registers	FC 04	- 30001
4xxxx	holding registers	FC 03	- 40001

Librería Modbus de Industrial Shields

- La versión 1.1.0 (Arduino PLC, ESP32 PLC) usa la dirección del protocolo, en base 0: el valor que le pasas va a la trama tal cual.
- `readHoldingRegisters(31, 9, 1)` lee el registro 40010 del esclavo 31, si su manual cuenta los 4xxxx desde 1.

Una prueba rápida

Lee dos registros desde N-1: una sola petición devuelve N-1 y N. Si N es 0, lee 0 y 1.

Compara con un valor que puedas ver en el equipo. Después, anota la convención en tu proyecto.

Referencias: MODBUS Application Protocol Specification V1.1b3 (modbus.org), apartados 4.3, 4.4, 6.3 y 7; Schneider Electric, FAQ FA168406 sobre números de registro y direcciones Modbus; Kepware (PTC), Modbus Address Descriptions; Industrial Shields: Modbus RTU con Arduino y ESP32 PLC, librería arduino-Modbus 1.1.0. La especificación y los manuales de los equipos prevalecen sobre esta guía general.