Panasonic Electric Works España, S.A.
San Severo, 20, Barajas Park, 28042 Madrid, España
Tel.:+34 902 414 140 • Fax: +34 913 292 976

Número	**ITExxxxxx1**
Título	**MODBUS RTU. Conceptos Básicos**
Versión	**1.0**

Sobre Este Documento

Este documento tiene como único objetivo el facilitar la ejecución de las funciones más comunes. En ningún caso, este documento tiene carácter oficial ni se podrá responsabilizar a Panasonic por las erratas o información errónea contenida en el mismo.
Panasonic declina toda responsabilidad por el uso de este documento.

Descripción

Modbus un protocolo de comunicaciones, basado en la arquitectura maestro/esclavo o cliente/servidor, diseñado en 1979 por **Modicon** para su gama de controladores lógicos programables (PLCs). Es un protocolo de comunicaciones estándar en la industria dado que es el más común entre los dispositivos electrónicos industriales. Las razones por las cuales el uso de Modbus es superior a otros protocolos de comunicaciones son:

1.- Es público
2.- Su implementación es fácil y requiere poco desarrollo
3.- Maneja bloques de datos sin suponer restricciones

Modbus permite que los PLCs puedan realizar el control de diferentes dispositivos tales como temperaturas, humedades, consumos energéticos, variadores de frecuencia, …. Existen versiones del protocolo Modbus para puerto serie y Ethernet (Modbus/TCP).

En el caso de Modbus para puerto serie, existen dos variantes. **Modbus RTU** que es una representación binaria compacta de los datos. **Modbus ASCII** es una representación legible del protocolo pero menos eficiente. La versión **Modbus TCP** es muy semejante al formato RTU, pero estableciendo la transmisión mediante paquetes TCP/IP (generalmente a través del puerto 502).

Información adaptada de la Wikipedia

Este informe intenta explicar de forma lo más reducida posible el funcionamiento del protocolo **MODUS RTU.**

Dado que el protocolo Modbus RTU es en hexadecimal, en adelante colocaremos la "**h**" detrás de cada byte (8 bits) para indicar que el valor es hexadecimal. Ejemplo trama hexadecimal Modbus RTU

0Ah 03h 00h 00h 00h 03h 04h 0Bh

Si desea ampliar esta información puede visitar la página web: www.modbus.org

Panasonic

Direcciones Modbus RTU

Modbus establece los siguientes tipos de direcciones

Contacto: Variables booleanas de lectura y escritura
Entradas: Variables booleanas de solo lectura
Registros de Retención: Variables de 16 bits de lectura y escritura
Registros de Entrada: Variables de 16 bits de solo lectura

Esas direcciones quedan definidas por lo que llamaremos página o lo que es lo mismo valor del primer dígito

Dato Modbus	Direcciones Modbus	Dígito inicial	Rango
Contacto	Página 0	0x	000000-099999
Entrada	Página 1	1x	100000-199999
Registros de Entrada	Página 3	3x	300000-399999
Registros de Retención	Página 4	4x	400000-499999

Funciones Modbus RTU

Modbus RTU trabaja con una serie de funciones codificadas mediante un byte hexadecimalmente (ej. **03h** leer registros de retención). Las funciones MODBUS RTU más comunes son:

Función Modbus Decimal	Código de la Función Hexadecimal	Significado	Descripción
1	01h	Lectura de contactos	Obtener el estado ON/OFF de un contacto
2	02h	Lectura de entradas	Obtener el valor ON/OFF de un contacto de entrada
3	03h	Lectura de registros de retención	Obtener el valor de un registros de retención
4	04h	Lectura de registros de entrada	Obtener el valor de un registro de entradas
5	05h	Forzar un simple contacto	Forzar a ON o a OFF un contacto
6	06h	Escribir en un registro de retención	Escribir un valor en un registros de retención
15	0Fh	Forzar múltiples contactos	Forzar a ON o a OFF varios contactos seguidos
16	10h	Escribir en múltiples registros de retención	Escribir valores en varios registros de retención

Existen otras funciones Modbus pero no son objeto de estudio de este informe

Panasonic

Tramas Modbus RTU

Como se observa en las tablas anteriores, la función a utilizar ya especifica directamente sobre que direcciones de memoria se va a actuar por lo que podríamos organizar las dos tablas en una de la siguiente manera.

Función	Significado	Rango de Direcciones Modbus
01h	Lectura de contactos	000000-099999
02h	Lectura de entradas	100000-199999
03h	Lectura de registros de retención	400000-499999
04h	Lectura de registros de entrada	300000-399999
05h	Forzar un simple contacto	000000-099999
06h	Escribir en un registro de retención	400000-499999
0Fh	Forzar múltiples contactos	000000-099999
10h	Escribir en múltiples registros de retención	400000-499999

Dado que la función a utilizar ya establece el área de memoria sobre la que va a actuar, al indicar el área de memoria se omite su página. Es decir, si queremos leer el registro de retención Modbus RTU **400100**, utilizaremos la función **03h** y la dirección **00h 64h** (**100** en decimal)

La trama que un maestro ha de enviar a una estación Modbus RTU consta de los siguientes campos:

1 Byte: Dirección del esclavo
1 Byte: Código de la función
2 Bytes: Dirección Modbus de inicio (sin incluir la página)
2 Bytes: Cantidad de direcciones Modbus sobre los que actuar
1 Byte: Número de bytes de los datos a enviar. Solo en funciones de escritura.
X Bytes: Datos. Solo en funciones de escritura. Longitud variable
2 Bytes: CRC16 (Cyclic Redundancy Check de 16 bits)

La trama de respuesta del esclavo consta de los siguientes campos

1 Byte: Dirección del esclavo
1 Byte: Código de la función a la que responde
2 Bytes: Dirección Modbus de inicio (sin incluir la página)
1 Byte: Cantidad de bytes de los datos respuesta. Solo si es respuesta a una lectura
X Bytes: Datos. Sólo para responder a peticiones de lectura de datos. Longitud variable
2 Bytes: CRC16 (Cyclic Redundancy Check de 16 bits)

Nota: El CRC16 se utiliza por el esclavo para asegurarse que la trama recibida es correcta y que no se ha modificado algún byte por ruido eléctrico u otro motivo.
El maestro realiza un cálculo de todos los bytes que va a enviar. Ese cálculo es el llamado CRC16 que incorpora a la trama de envío. Al recibir el esclavo ese comando realiza el mismo cálculo y lo compara con el valor recibido. Si es igual, acepta la orden y en caso contrario la desecha e informa al maestro de que lo ha desechado.

Ejemplo de trama Modbus RTU del maestro al esclavo y su respuesta

Maestro:

0Ah	**03h**	**00h 00h**	**00h03h**	**04h B0h**

Esclavo número 10.
Leer registros de datos de retención.
Dirección Modbus inicial de retención 400000
Total 3 registros de retención (400000-400002)
CRC16 (**04h B0h**)

Esclavo:

0Ah	**03h**	**06h**	**1Dh 71h**	**00h E6h**	**00h 32h**	**4Dh E1h**

Esclavo número 10.
Respuesta a la solicitud **03h**
Los datos vienen repartidos en 6 bytes
Contenido del primer dato (**1Dh 71h** = 7537)
Contenido del segundo dato (**00h E6h** = 230)
Contenido del tercer dato (**00h 32h** = 50)
CRC16 (**4Dh E1h**)

Códigos de Error

Como en todo protocolo se establecen unos códigos de error para que el maestro y el esclavo pueden informarse de diferentes eventos y actuar en consecuencia.

Pueden ocurrir dos tipos de error en las comunicaciones Modbus RTU

Error de Time-Out

El maestro lanza un comando que no es respondido por el esclavo.
Este es el caso típico que se produce ante rotura de cableado, diferencia de configuración de puertos de comunicaciones (baudios, paridad, …) e incluso de ausencia de ese número de esclavo en la red.

Este error de Time-Out ha de ser detectado automáticamente por el maestro, normalmente mediante un tiempo de espera configurable llamado Time-Out.

El Time-Out suele ser un valor configurable por el usuario y será el tiempo de espera máximo que esperará el maestro a recibir una respuesta ante un comando. Si transcurrido este tiempo no se ha recibido una respuesta, el maestro dará error y podrá actuar en consecuencia, por ejemplo realizando reintentos o saltándose a ese esclavo

Para solucionar este tipo de error se ha de revisar el hardware y configuraciones del hardware

Error de Tratamiento de Datos

El esclavo recibe una trama del maestro pero, por la información que contiene no puede ser tratada.

En este caso, la respuesta del esclavo tiene el siguiente formato

XXh	YYh+80h	ZZh	CRC16

Dónde:

XXh = Número de esclavo
YYh + **80h**= Número de la función + **80h**. Ej. Si la función es **03h** devuelva **83h**
ZZh = Código de error

Los códigos de error más comunes son:

Códigos de Error

Código	Tipo de Error	Significado
01	Función ilegal	La función recibida no esta permitida en el esclavo.
02	Dirección ilegal	La dirección esta fuera del rango permitido.
03	Dato ilegal	El dato contiene un valor no válido.
04	Falla en el dispositivo	El controlador no responde o ha ocurrido un error.
05	Reconocimiento (ACK)	Se ha aceptado la función y se esta procesando.
06	Ocupado	El mensaje ha sido recibido sin error, pero el dispositivo no puede procesarlo en este momento.
07	Reconocimiento Negativo (NAK)	La función solicitada no puede realizarse en este momento.

Ayúdenos a Mejorar

Si lo desea puede ponerse en contacto con nosotros en la siguiente dirección de correo:

soporte.tecnico@eu.panasonic.com

Si desea realizar cualquier consulta sobre este informe que no le haya quedado claro, indicar una errata, corregir la información o simplemente evaluar la utilidad de este informe, le rogamos que incluya en el asunto del mail el número del mismo.

Así mismo, estaremos encantados de atender sus solicitudes sobre futuros informes o acciones que considere que Panasonic debería realizar por lo que le ruego utilice este mail como buzón de sugerencias.