

COMUNICACIONES

MODBUS: BUS INDUSTRIAL DE REFERENCIA

presentado por:

Francisco Javier Ferrández Pastor

BUS DE CAMPO

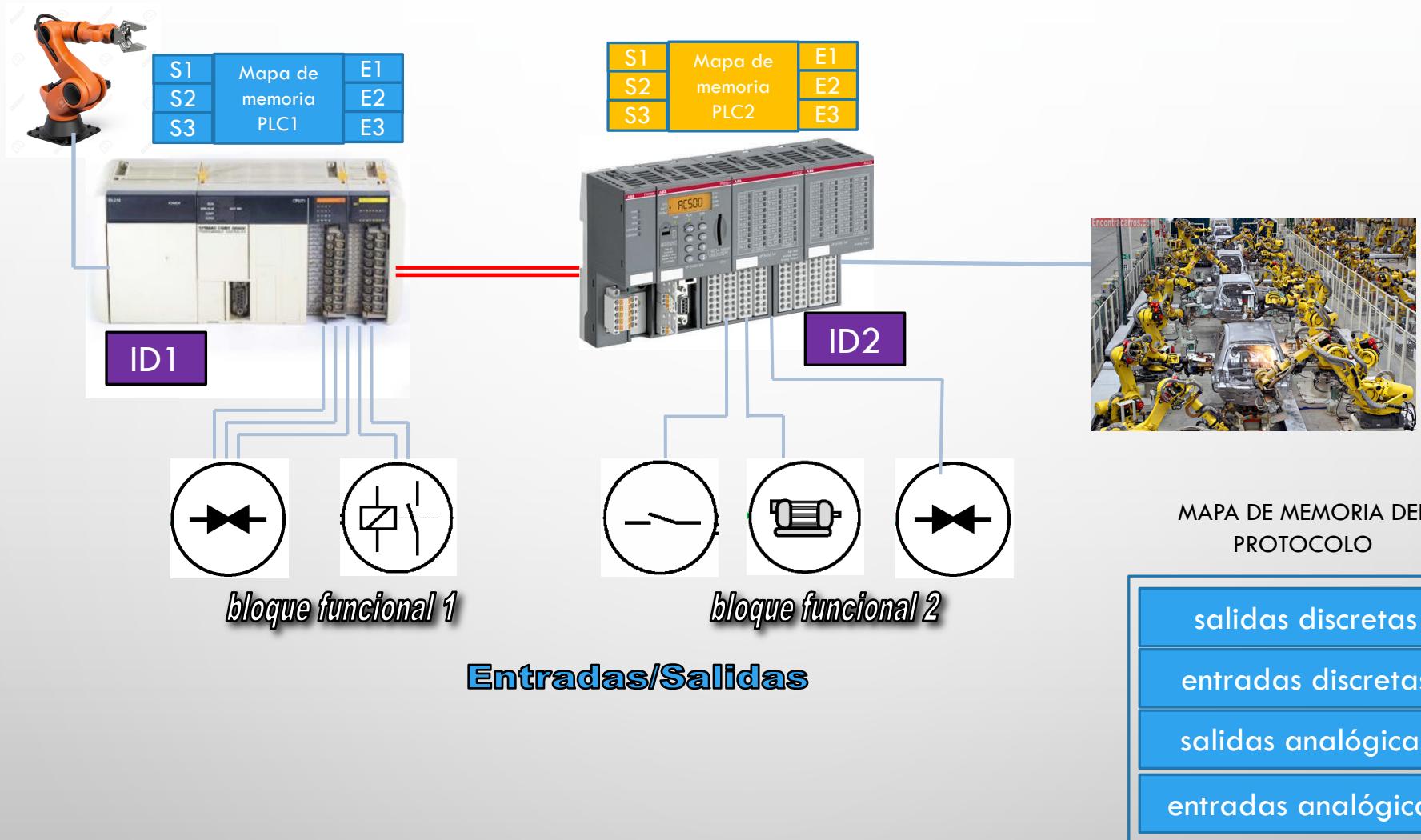
MODBUS

Modbus es un protocolo de comunicación serie desarrollado y publicado por Modicon en 1979. En su origen el uso de **Modbus** estaba orientado exclusivamente al mundo de los controladores lógicos programables o PLCs de Modicon. Sin embargo, a día de hoy, el protocolo **Modbus** es el protocolo de comunicaciones más común utilizado en entornos industriales, sistemas de telecontrol y monitorización.

Lo que implica de forma implícita que: tanto a nivel local como a nivel de red, en su versión TCP/IP, seguirá siendo uno de los protocolos de referencia en las llamadas Smart Grids, redes de sensores, telecontrol y un largo etc de sistemas de información que ya empiezan a asomar la cabeza en nuestro día a día.

BUS DE CAMPO

MODBUS: ANTECEDENTES

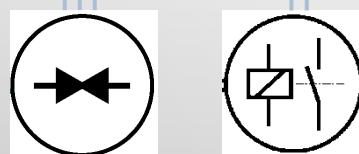
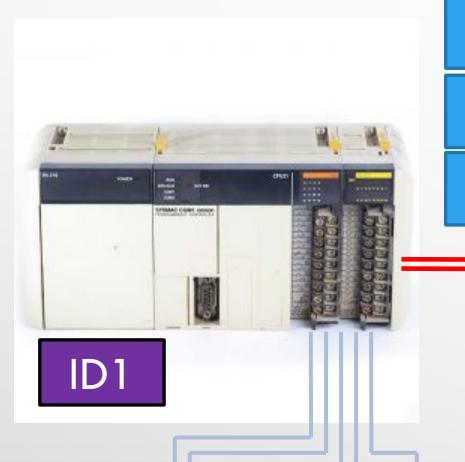


BUS DE CAMPO

MODBUS: ANTECEDENTES

MAPA DE MEMORIA DEL PROTOCOLO

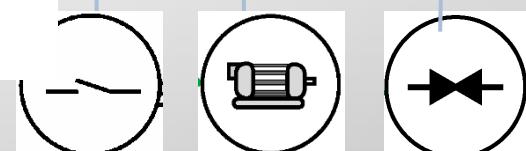
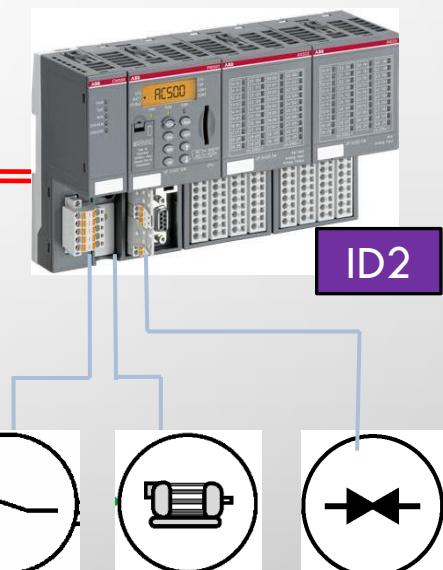
COILS	@0 - @9999
INPUTS	@10001 - @19999
INPUT REGISTERS	@30001- @40000
HOLDING REGISTERS	@40001- @50000



bloque funcional 1

¿Qué funciones puedo realizar?

Tabla 3. Funciones MODBUS	
Código	Función
01 o 02	Leer N bits (máximo 255)
03 o 04	Leer N registros (máx 52)
05	Escribir 1 bit
06	Escribir 1 registro



bloque funcional 2

Entradas/Salidas

BUS DE CAMPO

MODBUS: ANTECEDENTES

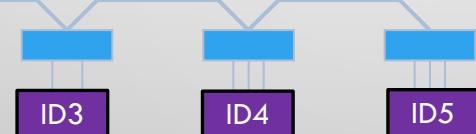
MAPA DE MEMORIA DEL PROTOCOLO

COILS	@1 - @9999
INPUTS	@10001 - @19999
INPUT REGISTERS	@30001- @40000
HOLDING REGISTERS	@40001- @50000

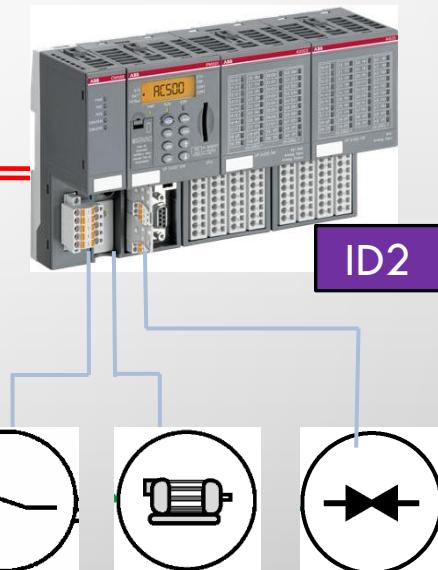


¿Qué funciones puedo realizar?

Código	Función
01 o 02	Leer N bits (máximo 255)
03 o 04	Leer N registros (máx 52)
05	Escribir 1 bit
06	Escribir 1 registro



Entradas/Salidas



bloque funcional 2

BUS DE CAMPO

MODBUS

El objeto del protocolo **Modbus** es bien sencillo:

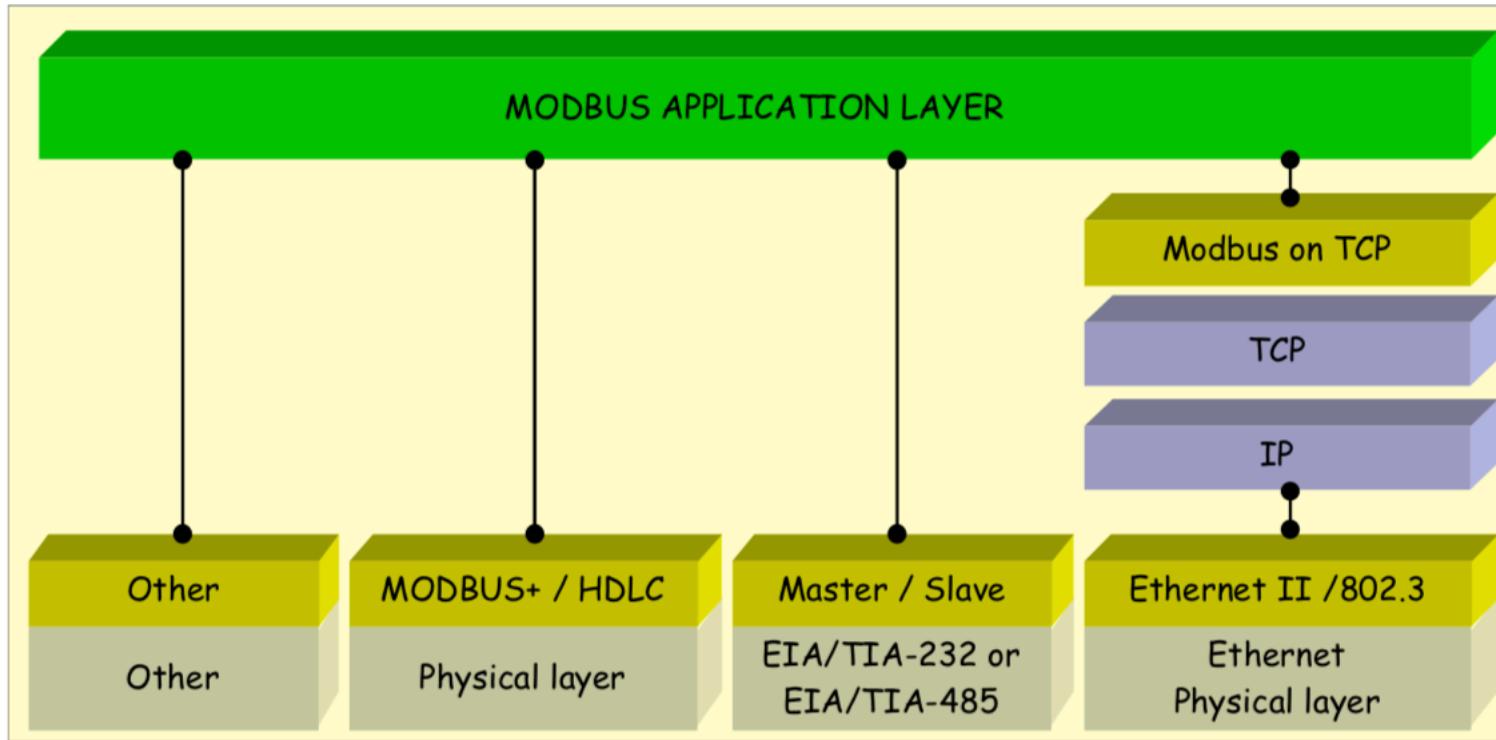
La transmisión de información entre distintos equipos electrónicos conectados a un mismo bus. Existiendo en dicho bus un solo dispositivo maestro (**Master**) y varios equipos esclavos (**Slaves**) conectados.

En su origen estaba orientado a una conectividad a través de líneas serie como pueden ser RS-232 o RS-485, pero con el paso del tiempo han aparecido variantes como la **Modbus TCP**, que permite el encapsulamiento del **Modbus** serie en tramas Ethernet TCP/IP de forma sencilla.

El protocolo **Modbus** se ubica en la capa de aplicación.

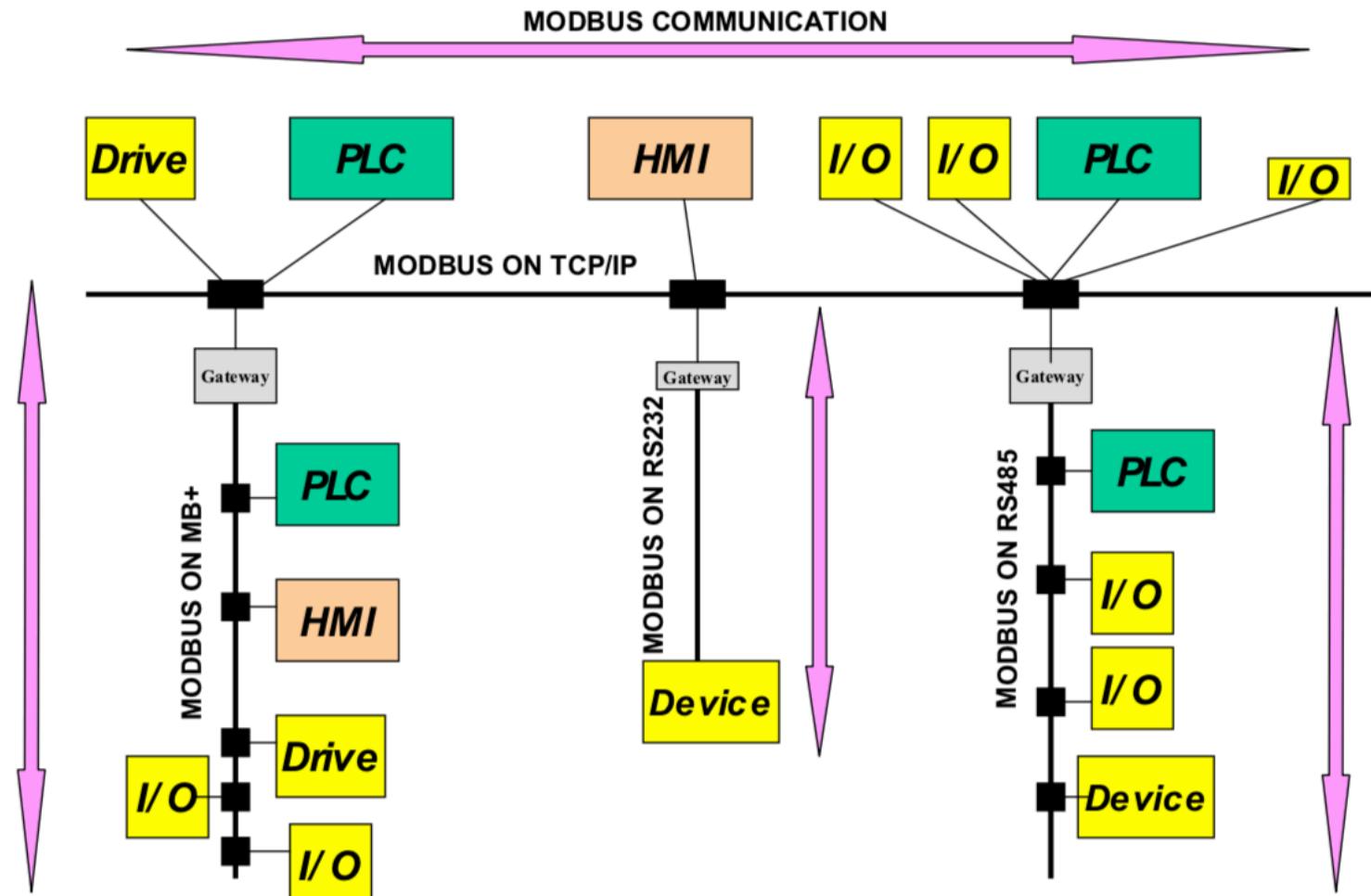
BUS DE CAMPO

MODBUS



BUS DE CAMPO

MODBUS: ARQUITECTURA



BUS DE CAMPO

MODBUS

El protocolo define una unidad de datos independiente de las capas de comunicación. Se trata de la PDU (Protocol Data Unit).

El mapeado en buses específicos o redes puede introducir campos de información Adicionales, es la ADU (Application Data Unit)

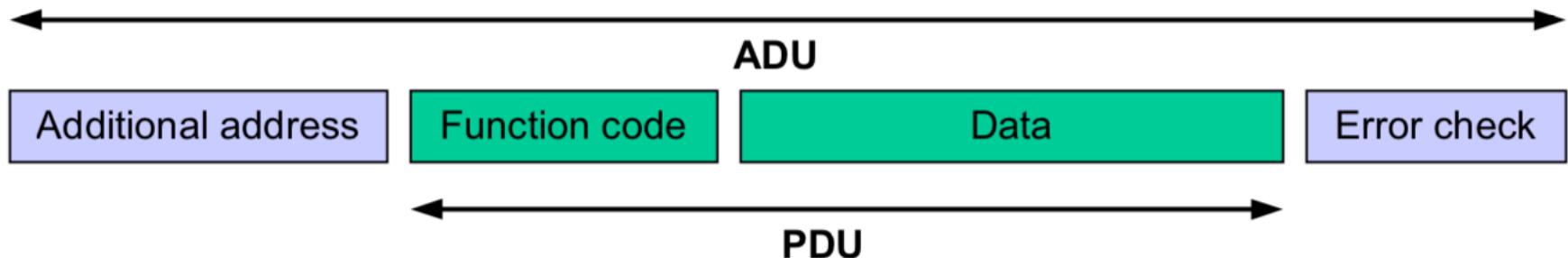


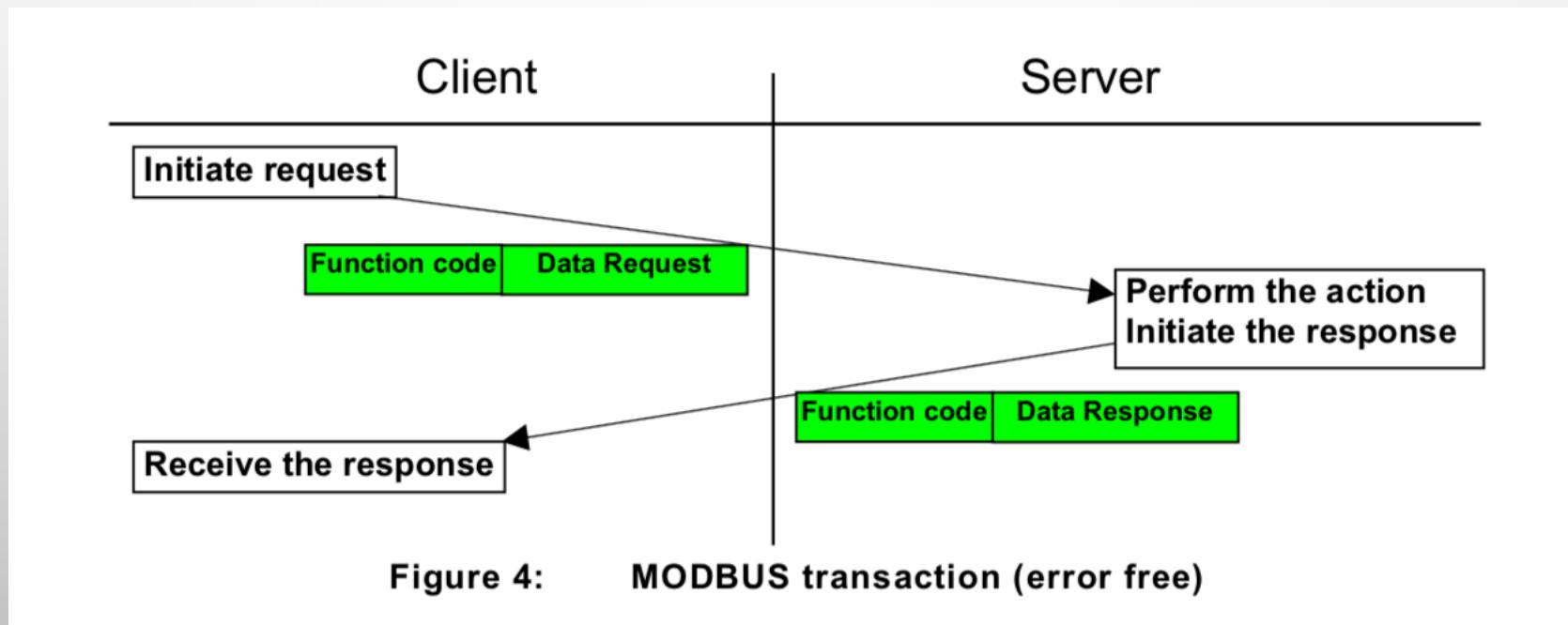
Figure 3: General MODBUS frame

BUS DE CAMPO

MODBUS

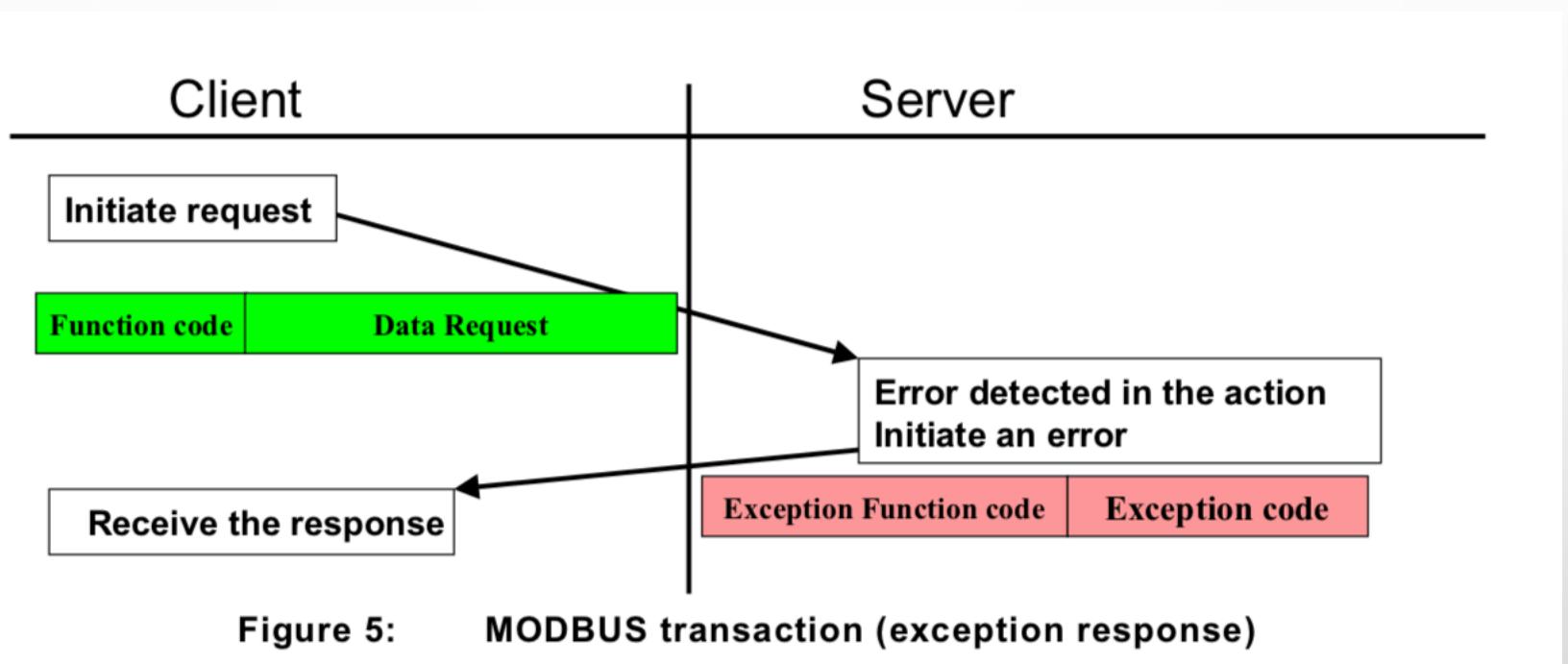
El protocolo define una unidad de datos independiente de las capas de comunicación. Se trata de la PDU (Protocol Data Unit).

El mapeado en buses específicos o redes puede introducir campos de información Adicionales, es la ADU (Application Data Unit)



BUS DE CAMPO

MODBUS



BUS DE CAMPO

MODBUS

4.3 MODBUS Data model

MODBUS bases its data model on a series of tables that have distinguishing characteristics. The four primary tables are:

Primary tables	Object type	Type of	Comments
Discretes Input	Single bit	Read-Only	This type of data can be provided by an I/O system.
Coils	Single bit	Read-Write	This type of data can be alterable by an application program.
Input Registers	16-bit word	Read-Only	This type of data can be provided by an I/O system
Holding Registers	16-bit word	Read-Write	This type of data can be alterable by an application program.

BUS DE CAMPO

MODBUS

		Function Codes				
		code	Sub code	(hex)	Section	
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs	02	6.2	
		Internal Bits Or Physical coils	Read Coils	01	6.1	
			Write Single Coil	05	6.5	
			Write Multiple Coils	15	6.11	
	16 bits access	Physical Input Registers	Read Input Register	04	6.4	
		Internal Registers Or Physical Output Registers	Read Holding Registers	03	6.3	
			Write Single Register	06	6.6	
			Write Multiple Registers	16	6.12	
			Read/Write Multiple Registers	23	6.17	
			Mask Write Register	22	6.16	
			Read FIFO queue	24	6.18	
		File record access	Read File record	20	6.14	
			Write File record	21	6.15	
Diagnostics			Read Exception status	07	6.7	
			Diagnostic	08	00-18,20	
			Get Com event counter	11	OB	
			Get Com Event Log	12	0C	
			Report Slave ID	17	11	
			Read device Identification	43	14	
Other		Encapsulated Interface Transport		2B	6.21	
				13,14	6.19	

BUS DE CAMPO

MODBUS

4.3 MODBUS Data model

MODBUS bases its data model on a series of tables that have distinguishing characteristics. The four primary tables are:

Primary tables	Object type	Type of	Comments
Discretes Input	Single bit	Read-Only	This type of data can be provided by an I/O system.
Coils	Single bit	Read-Write	This type of data can be alterable by an application program.
Input Registers	16-bit word	Read-Only	This type of data can be provided by an I/O system
Holding Registers	16-bit word	Read-Write	This type of data can be alterable by an application program.

BUS DE CAMPO

MODBUS

El hecho que se haya extendido su uso hasta convertirse en uno de los protocolos más usados en el sector industrial se debe a varias razones diferenciales respecto a otros protocolos:

- El estándar **Modbus** es público, lo que permite a los fabricantes desarrollar dispositivos tanto **Master** como **Slave** sin royalties aplicados al protocolo. Este hecho facilita el acceso a la información y estructura del protocolo que, además, es muy básica pero funcional para su objetivo.
- Desde un punto de vista técnico, su implementación es muy sencilla y en consecuencia el tiempo de desarrollo se acorta considerablemente respecto a otros protocolos en los que se complica la estructura de las tramas y en consecuencia el acceso a los datos que no están almacenados en estructuras complejas.
- La transmisión de información no está comprometida a ningún tipo de datos. Lo que implica cierta flexibilidad a la hora del intercambio de información. Que quiere decir esto? Para expresarlo de forma más clara, si se transmite un dato de 16bits de información su representación no está sujeta a ninguna restricción, por lo que puede tratarse de un dato tipo Word con signo, un entero sin signo de 16bits o la parte alta de una representación tipo Float de 32bits, etc. La representación del valor vendrá definida por la especificación que el fabricante dé del dispositivo, lo que permite la representación de un amplio rango de valores.

BUS DE CAMPO

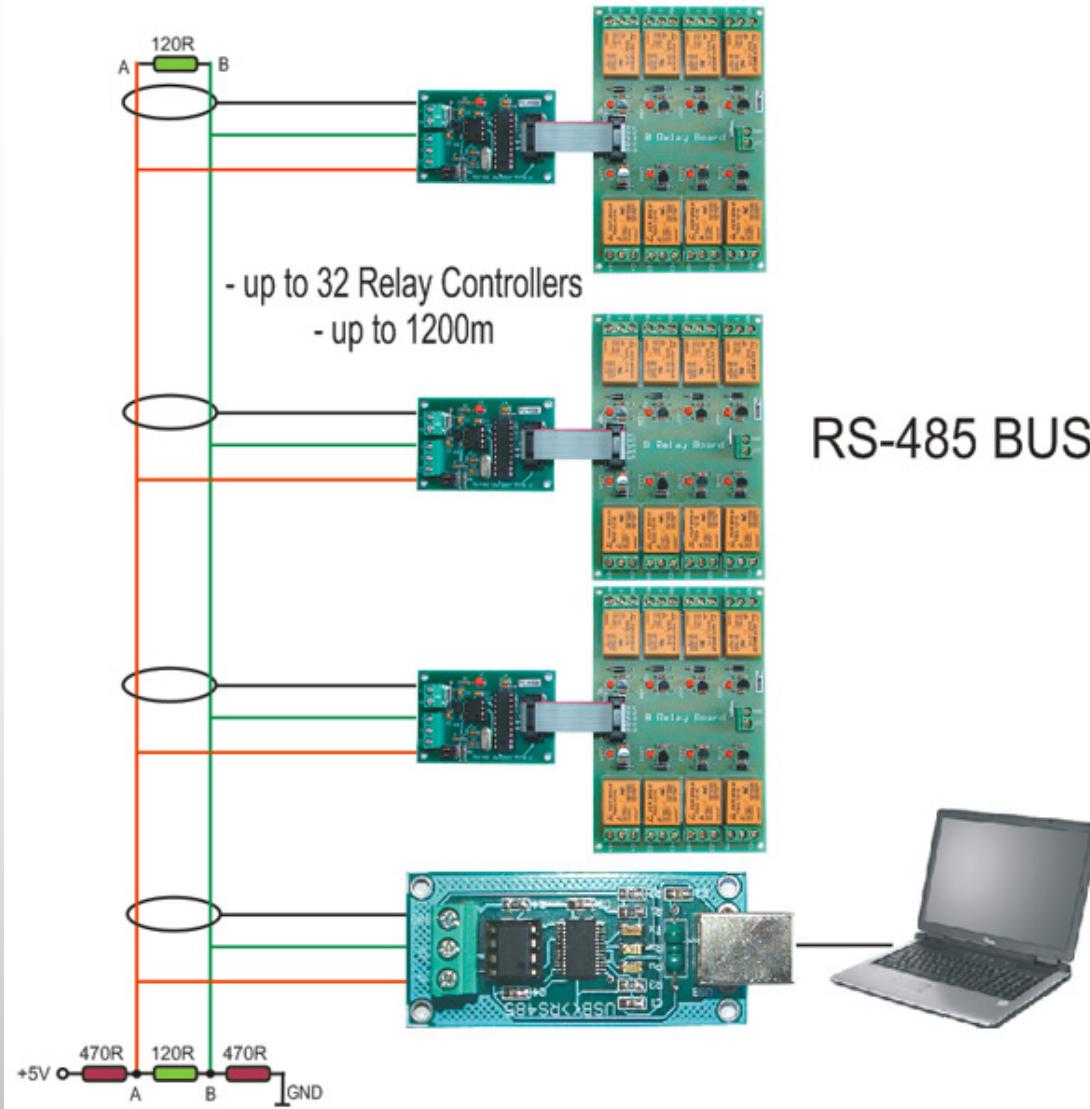
MODBUS

Características del bus:

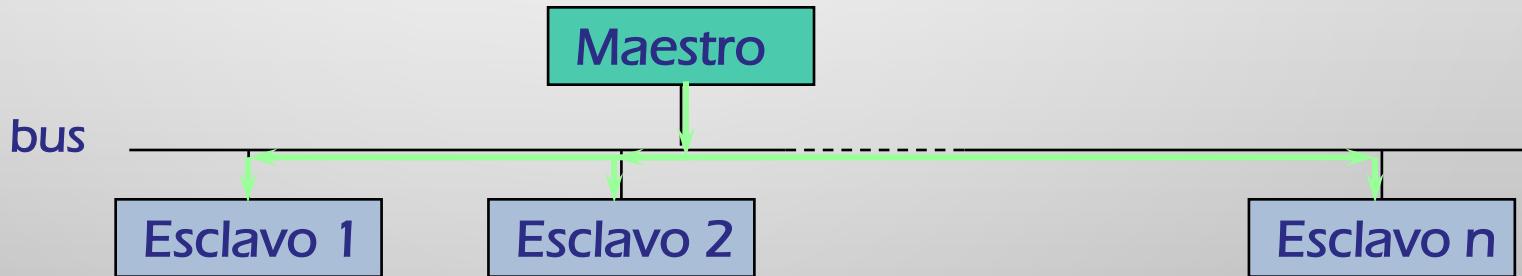
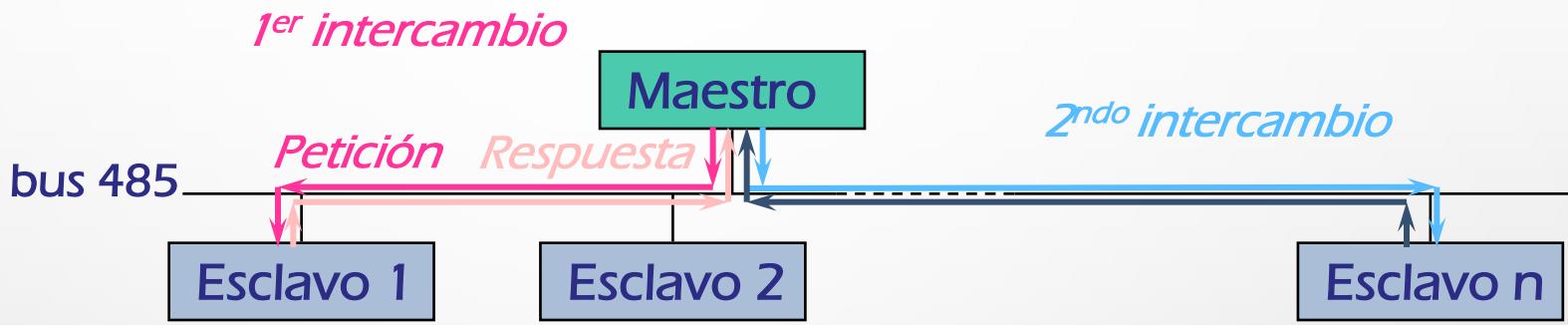
- Está definido como un sistema en bus de transmisión multipunto diferencial, es ideal para transmitir a altas velocidades sobre largas distancias (35 Mbps hasta 10 metros y 100 Kbps en 1.200 metros) y a través de canales ruidosos, ya que reduce los ruidos que aparecen en los voltajes producidos en la línea de transmisión.
- El medio físico de transmisión es un par entrelazado que admite hasta 32 estaciones en 1 solo hilo, con una longitud máxima de 1.200 metros operando entre 300 y 19200 bps y la comunicación half-duplex (semiduplex).
- Desde 2003 está siendo administrado por la Telecommunications Industry Association (TIA) y titulado como TIA-485-A.222.

BUS DE CAMPO

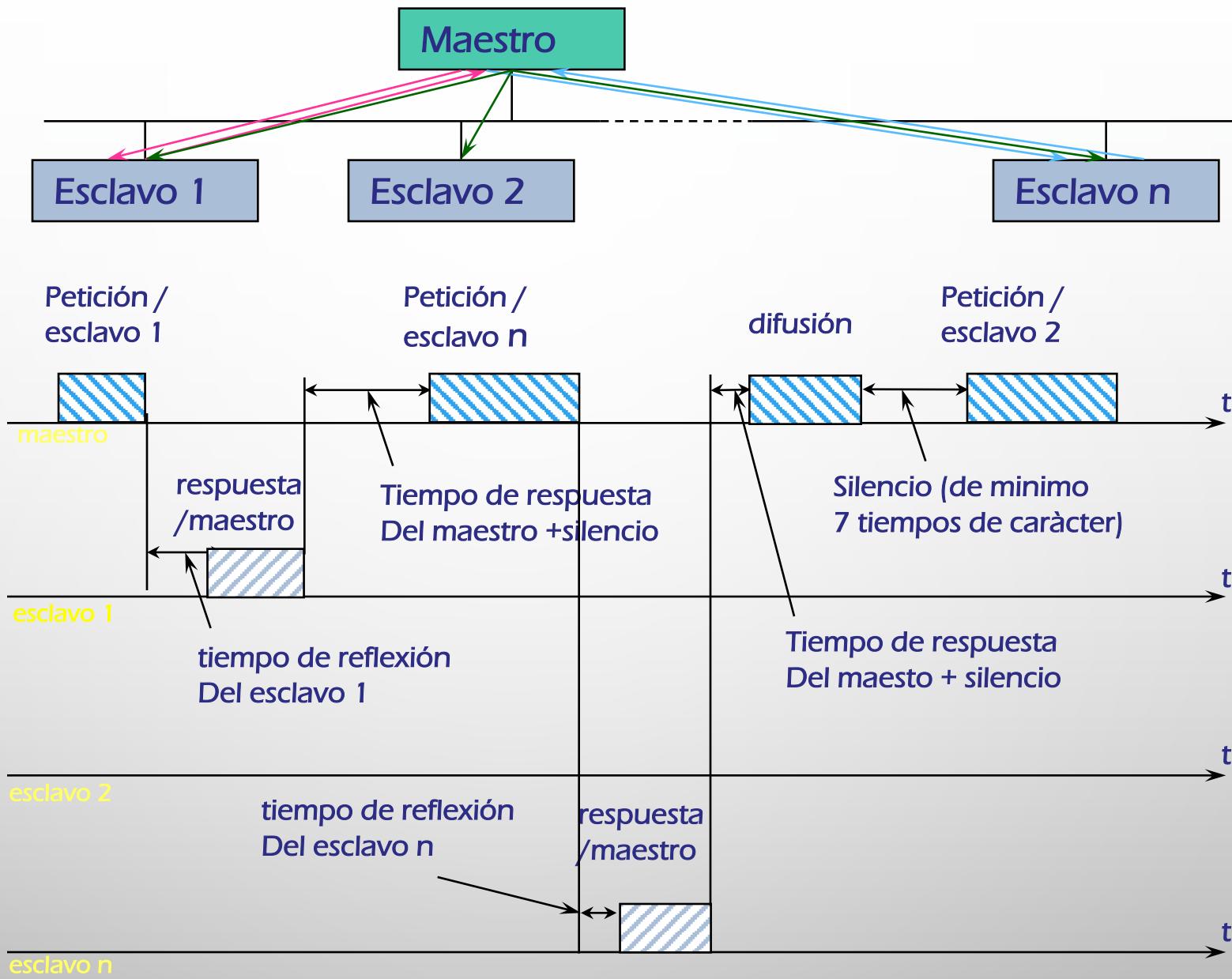
MODBUS



Proceso de Petición / respuesta (Query / response)



Proceso de Petición / respuesta (Query / response)

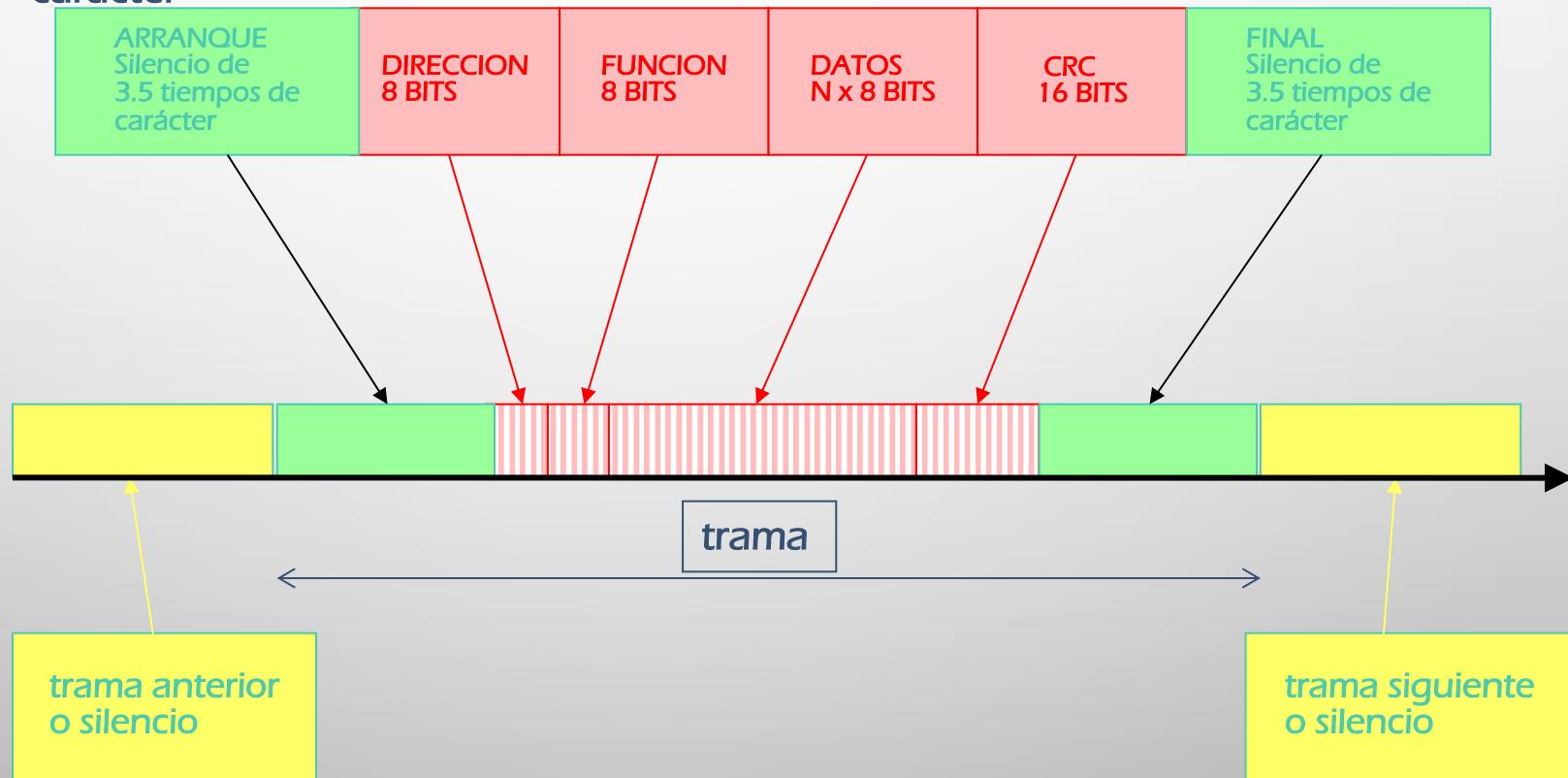


Mensaje Modbus : Trama RTU

El protocolo Modbus establece el formato para la petición del maestro, colocando en ella :

- ✓ la dirección del dispositivo esclavo (0 en caso de 'difusión' hacia todos los esclavos),
- ✓ un código de función que define la acción solicitada,
- ✓ cualquier dato que haya de enviarse
- ✓ un campo de comprobación de error.

Se colocan al arranque y al final un silencio de por lo menos 3.5 tiempos de carácter



FUNCIONES MODBUS

✓ FUNCIONES DE LECTURA / ESCRITURA

- CÓDIGO 01 / 02 : LEER ESTADOS DE BOBINAS / ENTRADAS
- CÓDIGO 03 / 04 : LEER REGISTROS MANTENIDOS / ENTRADAS
- CÓDIGO 05 : FORZAR UNA ÚNICA BOBINA
- CÓDIGO 06 : PREESTABLECER UN ÚNICO REGISTRO
- CÓDIGO 15 : FORZAR MÚLTIPLES BOBINAS

✓ FUNCIONES DE MANTENIMIENTO

POR EJEMPLO : BUSCAR CONTADOR DE EVENTOS DE COMUNICACIÓN

✓ FUNCIONES DE CONTROL

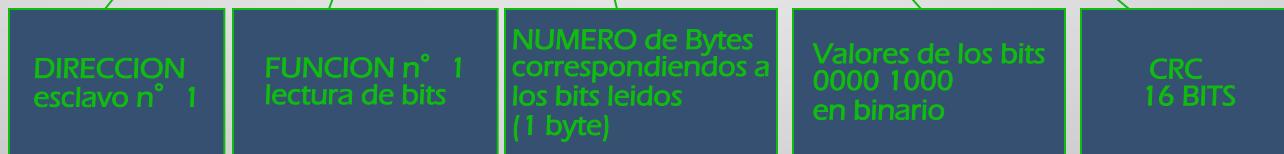
POR EJEMPLO : PASAR EN RUN / STOP UN PLC ESCLAVO

UTILIZACIÓN DE UN ANALIZADOR DE PROTOCOLO

Petición al esclavo 1



VISUALISATION BUFFER D'ECHANGE NON DECODES																			
Nom associé aux données : NORMAL SUR 8 BITS																			
No	COM	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Départ	Durée
1	2	01	01	00	08	00	08	BC	0E									0.00	4.56
2	1	01	01	01	08	50	4E											18.02	3.39
3	2	01	03	00	00	00	01	84	0A									610.08	4.58
4	1	01	03	02	00	0A	38	43										631.46	3.93
5	2	01	01	00	08	00	08	BC	0E									1020.15	4.58
6	1	01	01	01	01	90	48											1037.98	3.39
7	2	01	03	00	00	00	01	84	0A									1636.65	4.58
8	1	01	03	02	00	0A	38	43										1653.83	3.93
9	2	01	01	00	08	00	08	BC	0E									2040.46	4.58
10	1	01	01	01	02	D0	49											2062.10	3.40
11	2	01	03	00	00	00	01	84	0A									2657.22	4.55
12	1	01	03	02	00	0A	38	43										2675.15	3.97
13	2	01	01	00	08	00	08	BC	0E									3065.82	4.56
14	1	01	01	01	04	50	4B											3082.72	3.40



Respuesta del esclavo 1