

Redes Industriais e Sistemas Supervisórios

Bacharelado em Engenharia de Controle e Automação

MODBUS

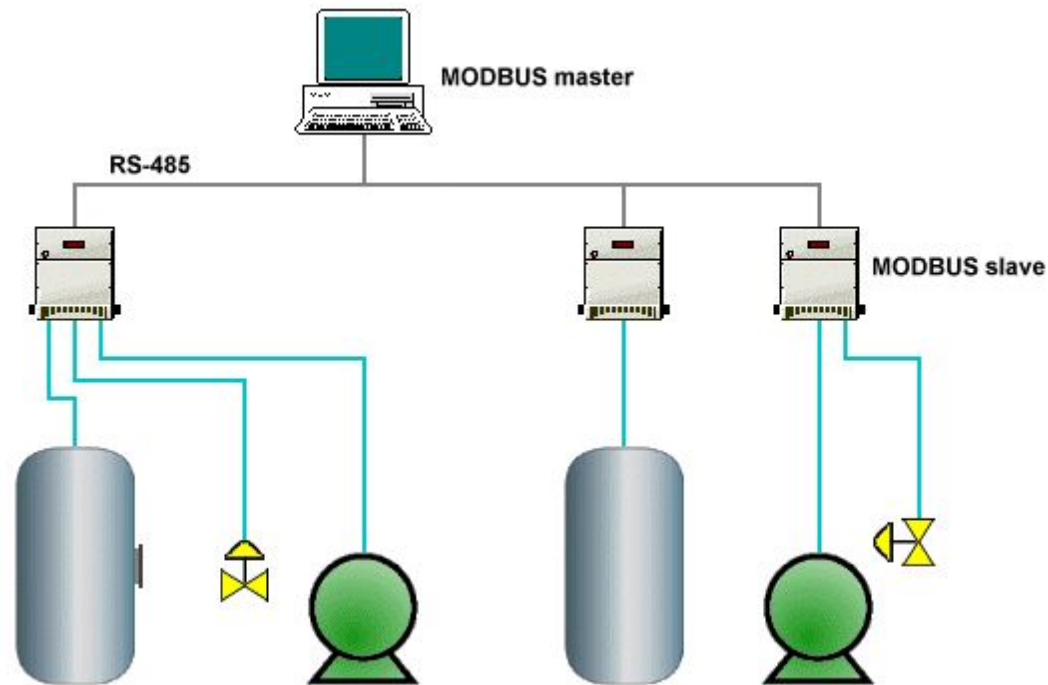
Conexão, Codificação e Funções

MODBUS

- O MODBUS é um **protocolo para barramentos de campo** criado pela **Modicon**, empresa fabricante de produtos para automação, visando inicialmente uso em seus próprios produtos.
- Porém, com o tempo, o MODBUS foi sendo adotado por um grande número de fabricantes, passando de um protocolo proprietário para um **protocolo aberto**.
- Atualmente é utilizado por milhares de fabricantes, sendo **o mais popular** entre os protocolos de barramento de campo utilizados atualmente.

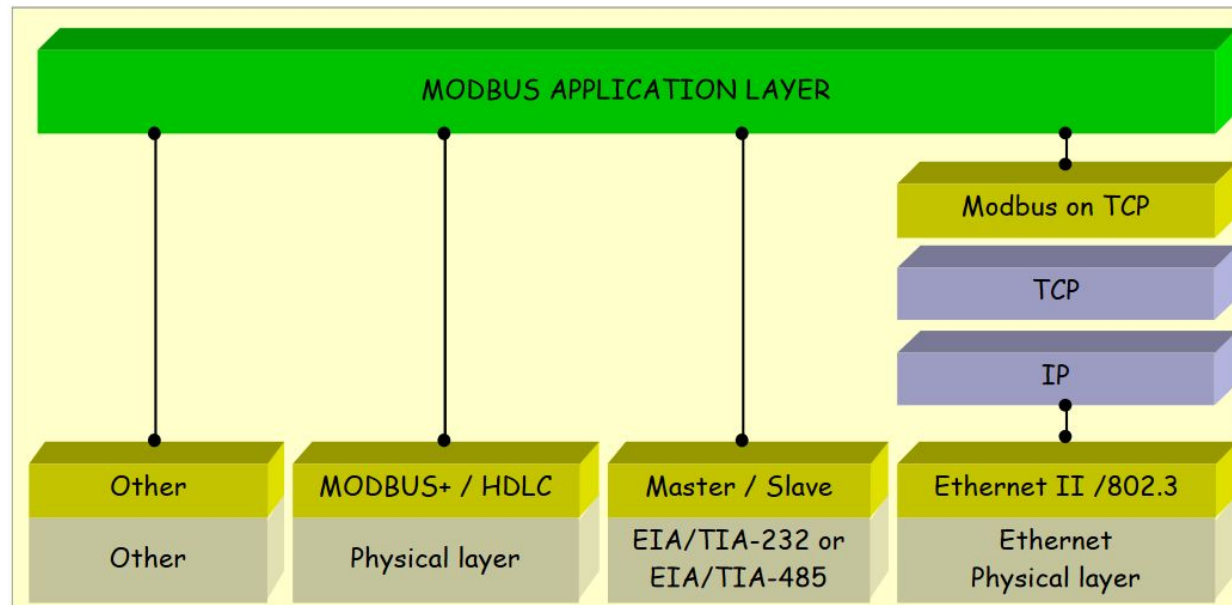
MODBUS em modo Mestre-Escravo

- O MODBUS é baseado no modelo mestre-escravo ou **cliente-servidor**;
- **Toda comunicação** deve **passar** necessariamente por um dispositivo **mestre**.
- Cada rede MODBUS pode possuir um mestre e até 247 escravos.



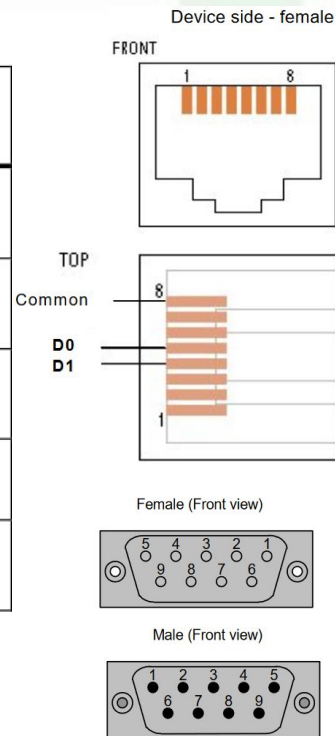
MODBUS e o modelo ISO/OSI

Layer	ISO/OSI Model
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



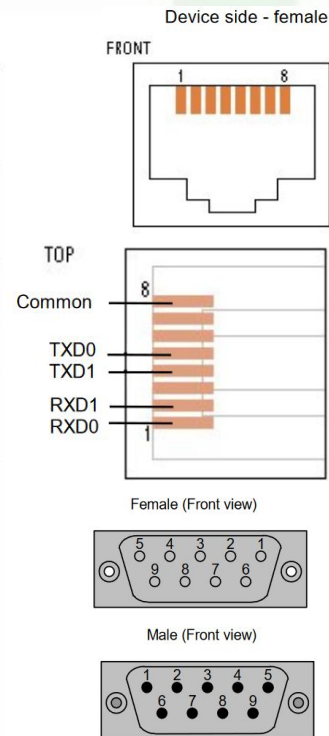
MODBUS: Conexão recomendada

Pin on RJ45	Pin on D9-shell	Level of requirement	IDv Circuit	ITr Circuit	EIA/TIA-485 name	Description for IDv
3	3	optional	PMC	--	--	Port Mode Control
4	5	required	D1	D1	B/B'	Transceiver terminal 1, V1 Voltage (V1 > V0 for binary 1 [OFF] state)
5	9	required	D0	D0	A/A'	Transceiver terminal 0, V0 Voltage (V0 > V1 for binary 0 [ON] state)
7	2	recommended	VP	--	--	Positive 5...24 V D.C. Power Supply
8	1	required	Common	Common	C/C'	Signal and Power Supply Common



MODBUS: Conexão recomendada

Pin on RJ45	Pin on D9-shell	Level of requirement	IDv Signal	ITr Signal	EIA/TIA-485 name	Description for IDv
1	8	required	RXD0	RXD0	A'	Receiver terminal 0, Va' Voltage (Va' > Vb' for binary 0 [ON] state)
2	4	required	RXD1	RXD1	B'	Receiver terminal 1, Vb' Voltage (Vb' > Va' for binary 1 [OFF] state)
3	3	optional	PMC	--	--	Port Mode Control
4	5	required	TXD1	TXD1	B	Generator terminal 1, Vb Voltage (Vb > Va for binary 1 [OFF] state)
5	9	required	TXD0	TXD0	A	Generator terminal 0, Va Voltage (Va > Vb for binary 0 [ON] state)
7	2	recommended	VP	--	--	Positive 5...24 V DC Power Supply
8	1	required	Common	Common	C/C'	Signal and Power Supply Common



MODBUS: recomendação de cores para fios

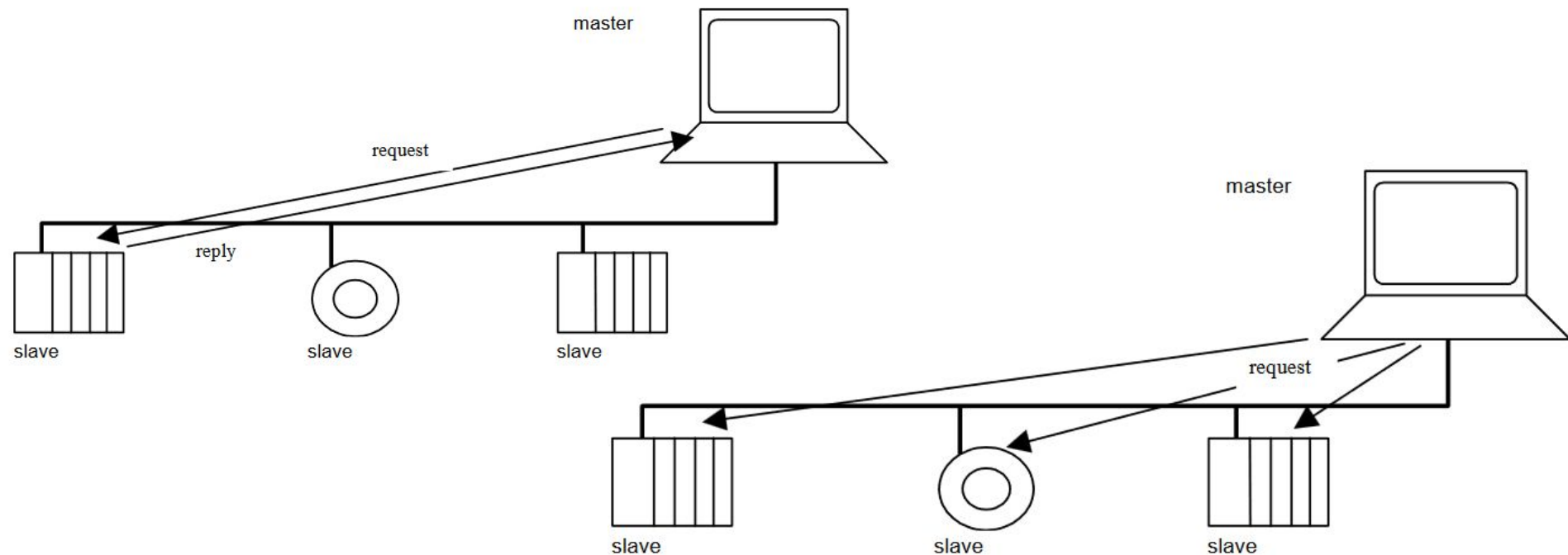
	Signal Names	Recommended Color
	D1-TXD1	yellow
	D0-TXD0	brown
	Common	grey
<i>4W (Optional)</i>	<i>RXD0</i>	<i>white</i>
<i>4W (Optional)</i>	<i>RXD1</i>	<i>blue</i>

Codificação de Mensagem em MODBUS

- Uma mensagem em MODBUS pode ser uma sequência que varia desde alguns poucos bytes (menos de 10) até algumas centenas (máximo de 256 bytes).
- Cada um dos serviços possui um formato de mensagem:
 - requisição;
 - resposta.



Unicast x Broadcast



Codificação de Mensagem em MODBUS

- As trocas de informações entre dispositivos, utiliza um conjunto de caracteres hexadecimais ou ASCII.
- **MODBUS ASCII:** transmite dados de sete bits.
 - Gera mensagens legíveis, mas consome mais recursos da rede.
- **MODBUS RTU** (*remote terminal unit*): Binário de oito bits

With Parity Checking

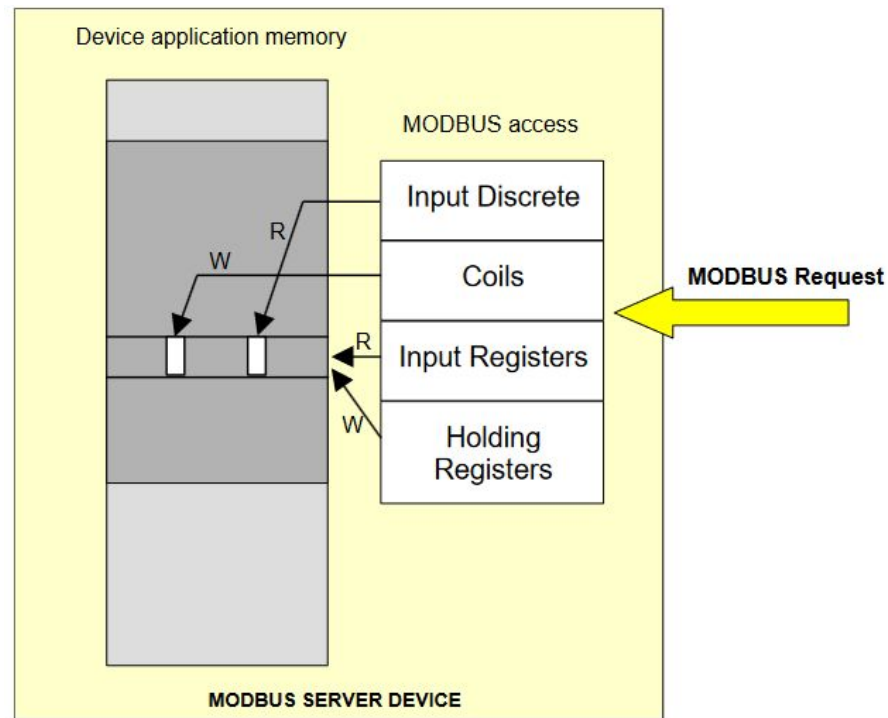
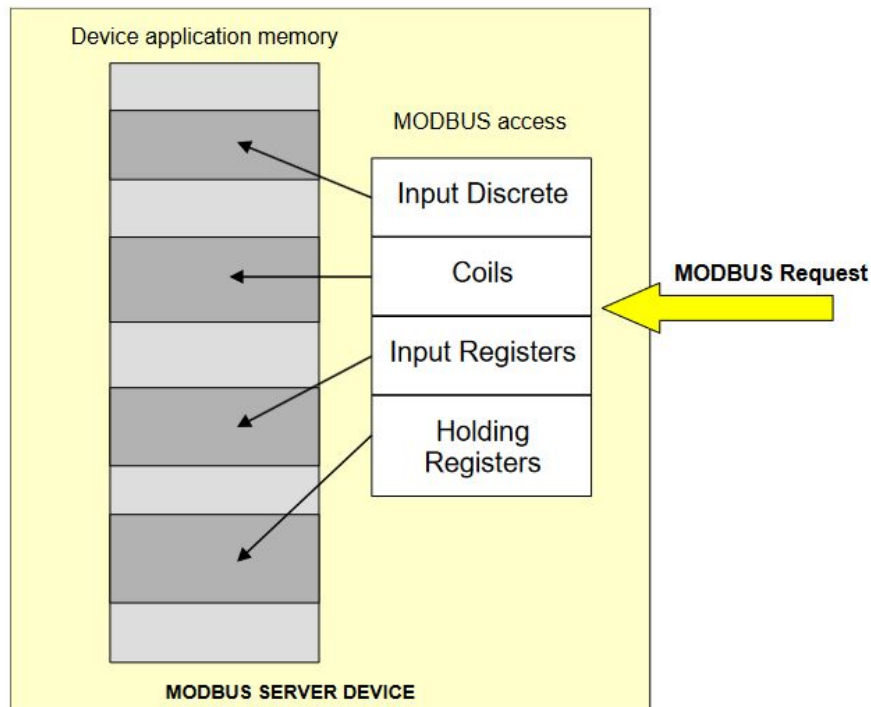
Start	1	2	3	4	5	6	7	8	Par	Stop
-------	---	---	---	---	---	---	---	---	-----	------

Without Parity Checking

Start	1	2	3	4	5	6	7	8	Stop	Stop
-------	---	---	---	---	---	---	---	---	------	------

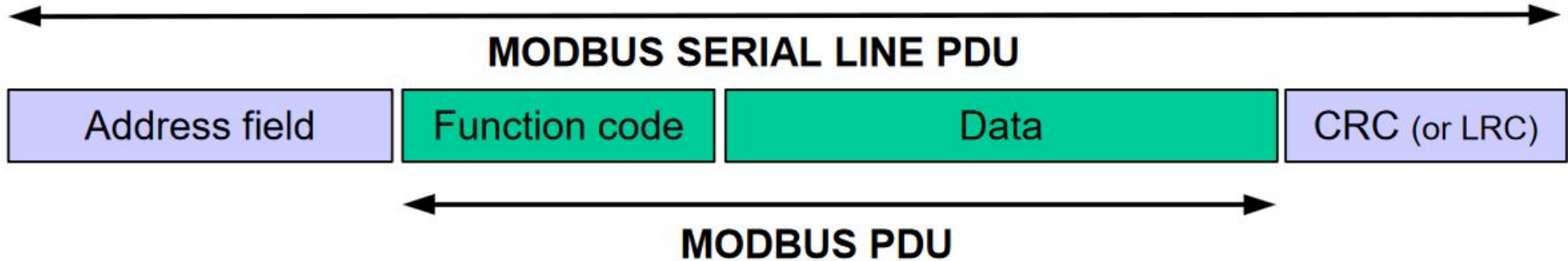
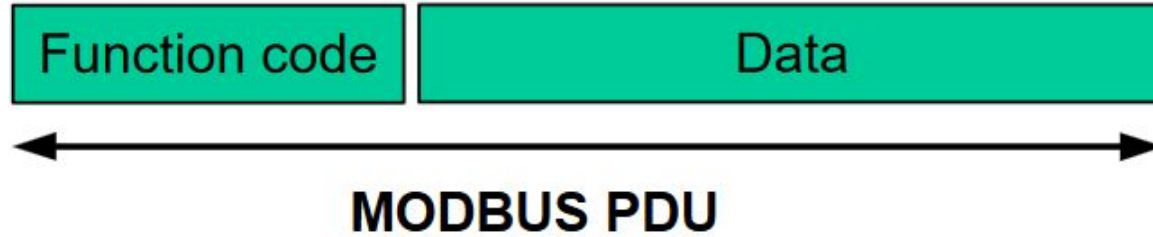


Modelos de organização de memória



Unidade de Dados de Protocolo

Protocol Data Unit (PDU)

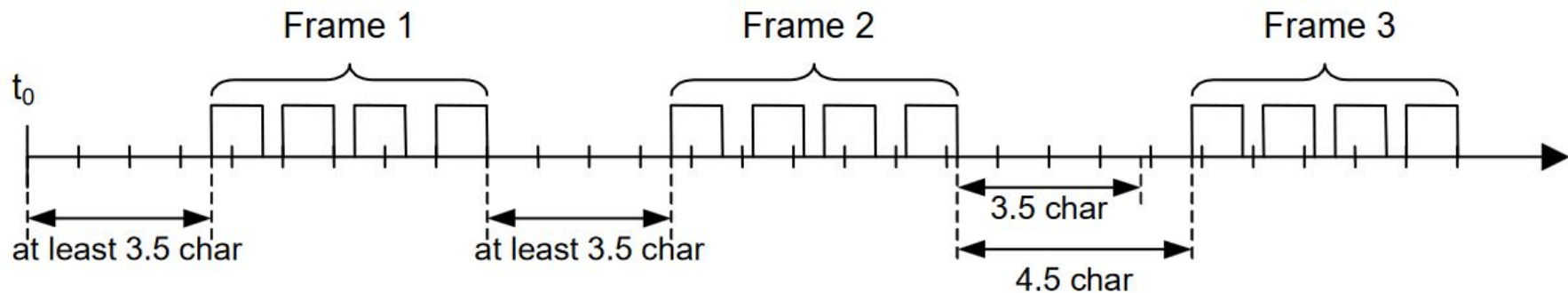
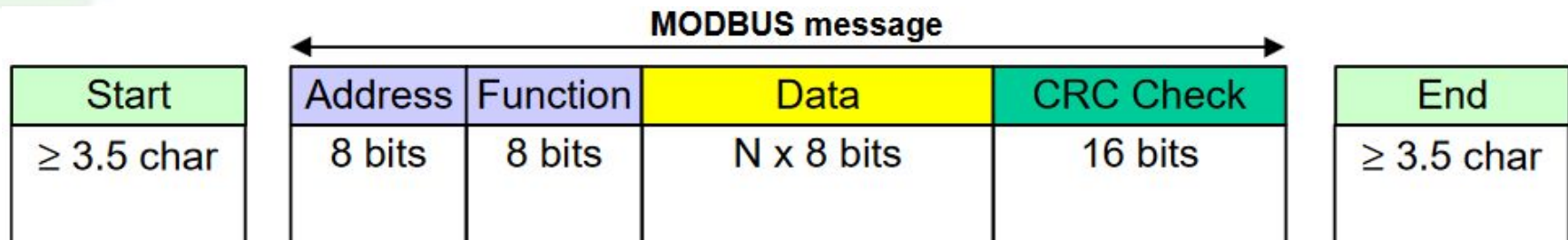


FRAME de mensagem em MODBUS RTU

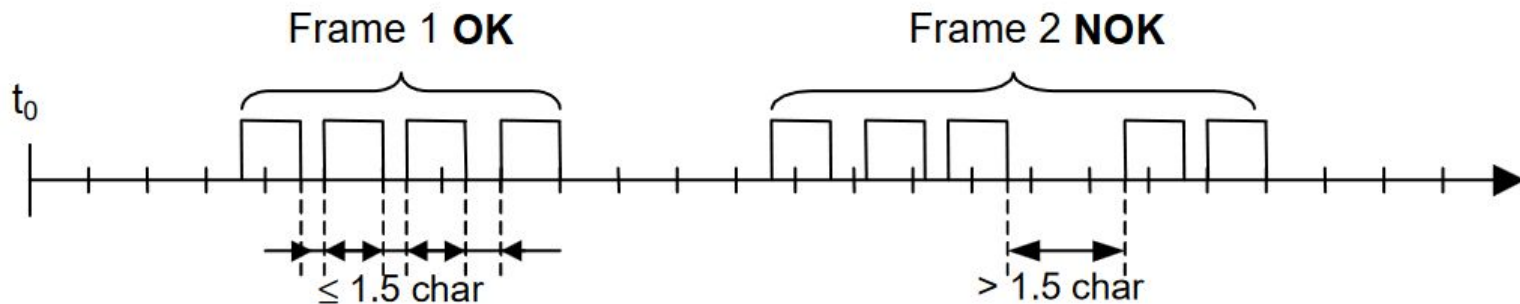
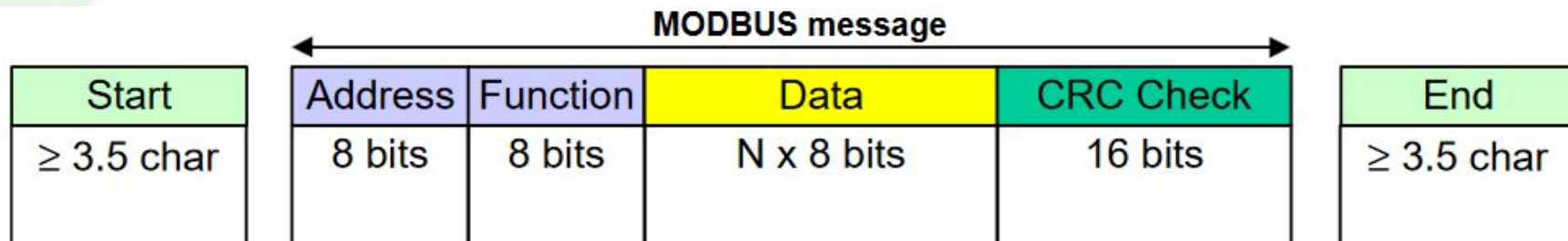
Slave Address	Function Code	Data	CRC
1 byte	1 byte	0 up to 252 byte(s)	2 bytes CRC Low ₁ CRC Hi

Tamanho máximo do frame: 256 bytes

Temporização de Mensagem em MODBUS



Codificação de Mensagem em MODBUS



Baudrate > 19200 bps $t_{1.5} = 750\mu s$
 $t_{3.5} = 1750\mu s$

Codificação de Mensagem em MODBUS

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

Codificação de Mensagem em MODBUS

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- Número de endereço do escravo (1 byte)
- Designa o **destinatário** da mensagem

0	Broadcast address
1 .. 247	Slave individual addresses
248 .. 255	Reserve

Codificação de Mensagem em MODBUS

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

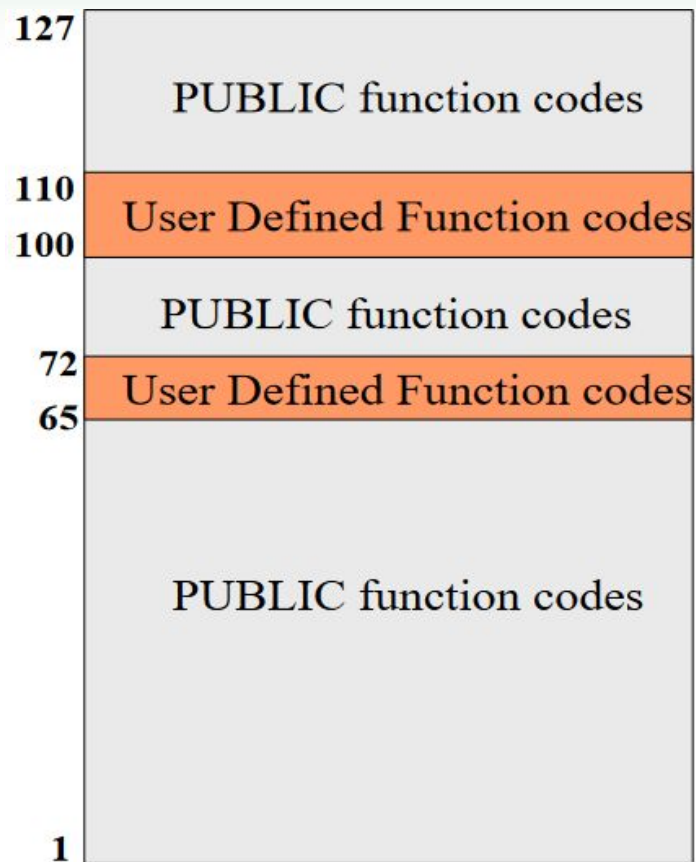
- Código da **função (ou comando)** a realizar (1 byte)
- Designa um comando de escrita ou leitura sobre os escravos
- Isso automaticamente informa o tipo de operando associado
 - Leitura de dados;
 - Escrita de dados;
 - Difusão de dados (Broadcast) .

Código de Funções Públicas MODBUS

				Function Codes			
				code	Sub code	(hex)	Section
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs	02		02	6.2
		Internal Bits Or Physical coils	Read Coils	01		01	6.1
			Write Single Coil	05		05	6.5
			Write Multiple Coils	15		0F	6.11
	16 bits access	Physical Input Registers	Read Input Register	04		04	6.4
		Internal Registers Or Physical Output Registers	Read Holding Registers	03		03	6.3
			Write Single Register	06		06	6.6
			Write Multiple Registers	16		10	6.12
			Read/Write Multiple Registers	23		17	6.17
			Mask Write Register	22		16	6.16
			Read FIFO queue	24		18	6.18
			File record access	Read File record	20		14
	Write File record	21			15	6.15	
Diagnostics			Read Exception status	07		07	6.7
			Diagnostic	08	00-18,20	08	6.8
			Get Com event counter	11		0B	6.9
			Get Com Event Log	12		0C	6.10
			Report Server ID	17		11	6.13
			Read device Identification	43	14	2B	6.21
			Other			Encapsulated Interface Transport	43
			CANopen General Reference	43	13	2B	6.20



Intervalo de Funções Definidas pelo Usuário



Codificação de Mensagem em MODBUS

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- 1 - 01h - Read coil status
- 2 - 02h - Read input status
- 3 - 03h - Read holding registers
- 4 - 04h - Read input registers
- 5 - 05h - Write single-coil status
- 6 - 06h - Write single register
- 15 - 0Fh - Write multiple-coil status
- 16 - 10h - Write multiple registers

Coils

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- 1 - 01h - Read coil status**
- 2 - 02h - Read input status
- 3 - 03h - Read holding registers
- 4 - 04h - Read input registers
- 5 - 05h - Write single-coil status**
- 6 - 06h - Write single register
- 15 - 0Fh - Write multiple-coil status**
- 16 - 10h - Write multiple registers

Tamanho

1-bit

Endereçamento

00001 - 09999

0000h - 270Eh

Discrete Input

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- 1 - 01h - Read coil status
- 2 - 02h - Read input status**
- 3 - 03h - Read holding registers
- 4 - 04h - Read input registers
- 5 - 05h - Write single-coil status
- 6 - 06h - Write single register
- 15 - 0Fh - Write multiple-coil status
- 16 - 10h - Write multiple registers

Tamanho

1-bit

Endereçamento

10001 - 19999

0000h - 270Eh

Input Register

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- 1 - 01h - Read coil status
- 2 - 02h - Read input status
- 3 - 03h - Read holding registers
- 4 - 04h - Read input registers**
- 5 - 05h - Write single-coil status
- 6 - 06h - Write single register
- 15 - 0Fh - Write multiple-coil status
- 16 - 10h - Write multiple registers

Tamanho

16-bits

Endereçamento

30001 - 39999

0000h - 270Eh

Holding Register

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- 1 - 01h - Read coil status
- 2 - 02h - Read input status
- 3 - 03h - Read holding registers**
- 4 - 04h - Read input registers
- 5 - 05h - Write single-coil status
- 6 - 06h - Write single register**
- 15 - 0Fh - Write multiple-coil status
- 16 - 10h - Write multiple registers**

Tamanho

16-bits

Endereçamento

40001 - 49999

0000h - 270Eh

Codificação de Mensagem em MODBUS

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- Dados da Requisição.
 - Pode conter o **endereço respectivo** (2 bytes)
 - designa a **posição de memória inicial** dos dados do escravo;
 - Pode conter ainda bytes que designam o **número de operandos**, dados a transmitir ou a serem lidos do escravo.

Codificação de Mensagem em MODBUS

End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- CRC uma palavra de **controle** (2 bytes)
- Serve para detectar os erros de transmissão
- Tipo [CRC-16](#).

01 (0x01) Read Coils

Request

Function code	1 Byte	0x01
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of coils	2 Bytes	1 to 2000 (0x7D0)

Response

Function code	1 Byte	0x01
Byte count	1 Byte	N*
Coil Status	n Byte	n = N or N+1

Error

Function code	1 Byte	Function code + 0x80
Exception code	1 Byte	01 or 02 or 03 or 04

01 (0x01) Read Coils

Requisição de leitura das saídas discretas de 20 até 38:

Request		Response	
<i>Field Name</i>	<i>(Hex)</i>	<i>Field Name</i>	<i>(Hex)</i>
Function	01	Function	01
Starting Address Hi	00	Byte Count	03
Starting Address Lo	13	Outputs status 27-20	CD
Quantity of Outputs Hi	00	Outputs status 35-28	6B
Quantity of Outputs Lo	13	Outputs status 38-36	05

03 (0x03) Read Holding Registers

Request

Function code	1 Byte	0x03
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of Registers	2 Bytes	1 to 125 (0x7D)

Response

Function code	1 Byte	0x03
Byte count	1 Byte	2 x N *
Register value	N * x 2 Bytes	

***N** = Quantity of Registers

Error

Error code	1 Byte	0x83
Exception code	1 Byte	01 or 02 or 03 or 04

03 (0x03) Read Holding Registers

Requisição de leitura dos registradores 108 até 110:

Request		Response	
Field Name	(Hex)	Field Name	(Hex)
Function	03	Function	03
Starting Address Hi	00	Byte Count	06
Starting Address Lo	6B	Register value Hi (108)	02
No. of Registers Hi	00	Register value Lo (108)	2B
No. of Registers Lo	03	Register value Hi (109)	00
		Register value Lo (109)	00
		Register value Hi (110)	00
		Register value Lo (110)	64

06 (0x06) Write Single Register

Request

Function code	1 Byte	0x06
Register Address	2 Bytes	0x0000 to 0xFFFF
Register Value	2 Bytes	0x0000 to 0xFFFF

Response

Function code	1 Byte	0x06
Register Address	2 Bytes	0x0000 to 0xFFFF
Register Value	2 Bytes	0x0000 to 0xFFFF

Error

Error code	1 Byte	0x86
Exception code	1 Byte	01 or 02 or 03 or 04

06 (0x06) Write Single Register

Requisição para escrever no registrador 2 o valor 0003h:

Request		Response	
Field Name	(Hex)	Field Name	(Hex)
Function	06	Function	06
Register Address Hi	00	Register Address Hi	00
Register Address Lo	01	Register Address Lo	01
Register Value Hi	00	Register Value Hi	00
Register Value Lo	03	Register Value Lo	03

App de teste de comunicação MODBUS



Referências

ANDRADE, F. **Tudo sobre o protocolo MODBUS**. [S. l.: s. n.], 2018. Disponível em: <https://automacaoecartoons.com/2018/11/23/protocolo-modbus/>. Acesso em: 9 out. 2024.

CONTROL SOLUTION MINNESOTA. **Modbus Tutorial from Control Solutions**. [S. l.: s. n.], 2020. Disponível em: https://www.csimn.com/CSI_pages/Modbus101.html.

MODBUS.ORG. **MODBUS APPLICATION PROTOCOL SPECIFICATION V1.1b3**. [S. l.: s. n.], 2012. Disponível em: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf. Acesso em: 9 out. 2024.

MODBUS.ORG. **MODBUS over serial line specification and implementation guide V1.02**. [S. l.: s. n.], 2006. Disponível em: https://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf.