

# Redes Industriais e Sistemas Supervisórios

Bacharelado em Engenharia de Controle e Automação

# MODBUS

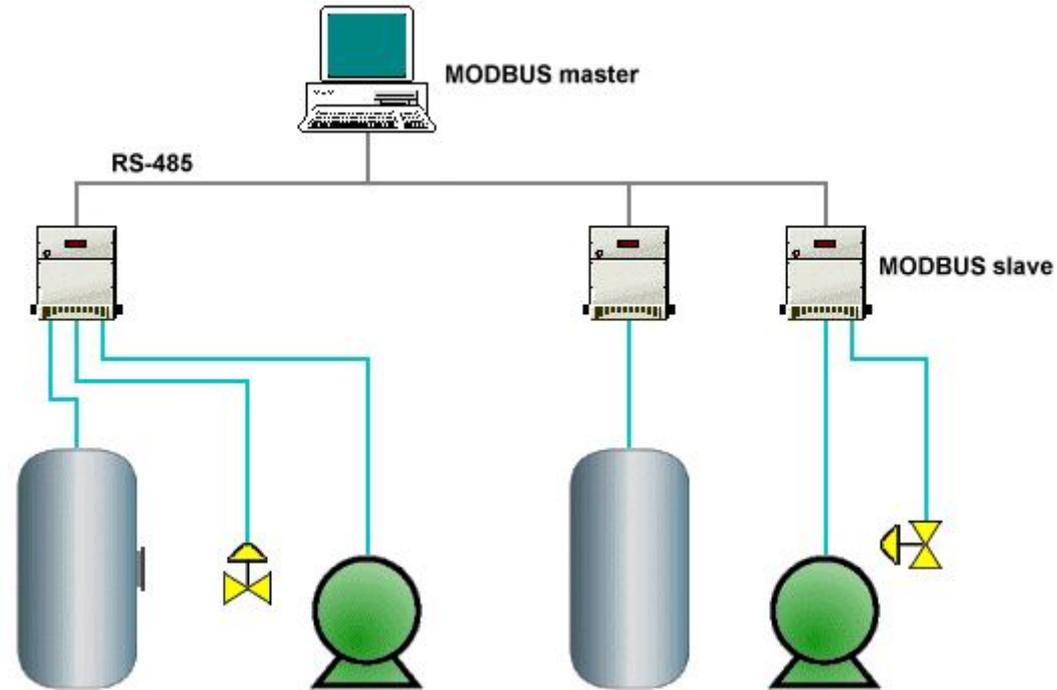
Conexão, Codificação e Funções

# 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.

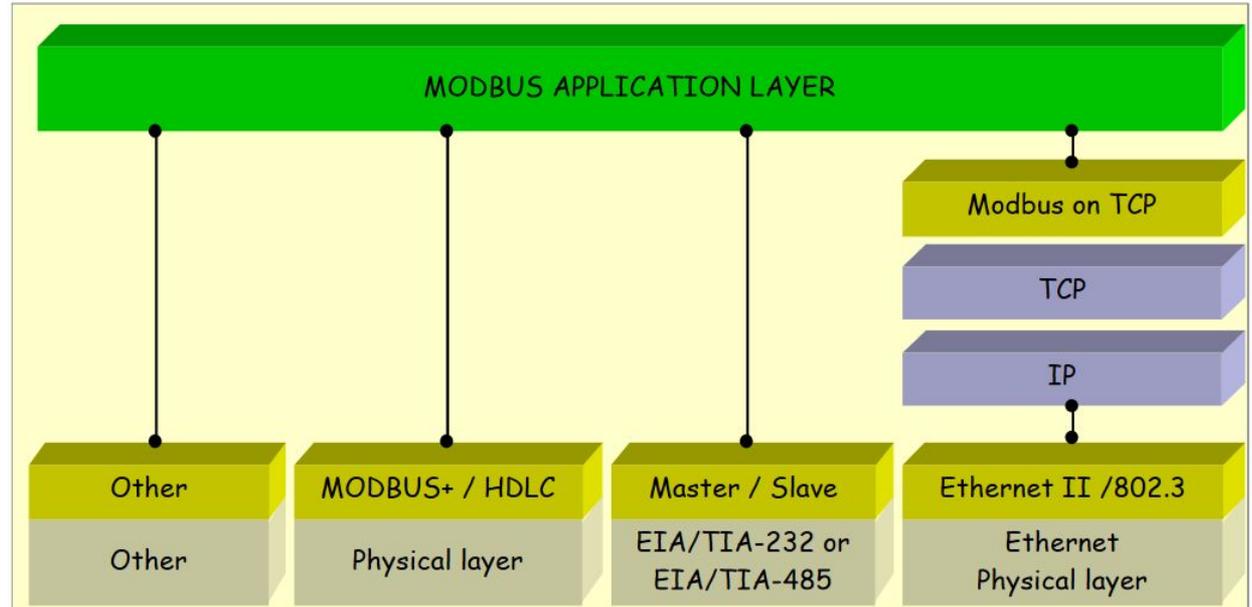
# MODBUS em modo Mestre-Escravo

- 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

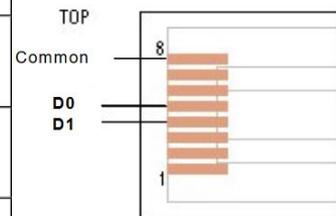
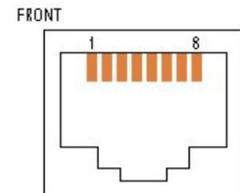
Layer	ISO/OSI Model
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



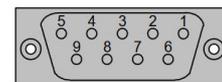
# MODBUS: Conexão recomendada

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	<b>required</b>	D1	D1	B/B'	<b>Transceiver terminal 1, V1 Voltage</b> ( V1 > V0 for binary 1 [OFF] state )
5	9	<b>required</b>	D0	D0	A/A'	<b>Transceiver terminal 0, V0 Voltage</b> ( V0 > V1 for binary 0 [ON] state )
7	2	recommended	VP	--	--	Positive 5...24 V D.C. Power Supply
8	1	<b>required</b>	Common	Common	C/C'	<b>Signal and Power Supply Common</b>

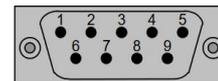
Device side - female



Female (Front view)

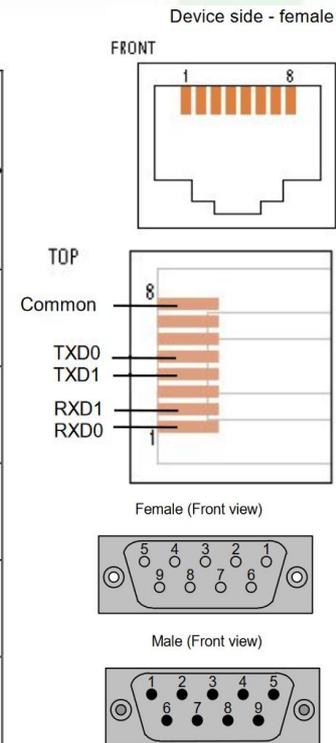


Male (Front view)



# 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'	<b>Receiver terminal 0, Va' Voltage</b> ( Va' > Vb' for binary 0 [ON] state )
2	4	required	RXD1	RXD1	B'	<b>Receiver terminal 1, Vb' Voltage</b> ( Vb' > Va' for binary 1 [OFF] state )
3	3	optional	PMC	--	--	Port Mode Control
4	5	required	TXD1	TXD1	B	<b>Generator terminal 1, Vb Voltage</b> ( Vb > Va for binary 1 [OFF] state )
5	9	required	TXD0	TXD0	A	<b>Generator terminal 0, Va Voltage</b> ( 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'	<b>Signal and Power Supply Common</b>



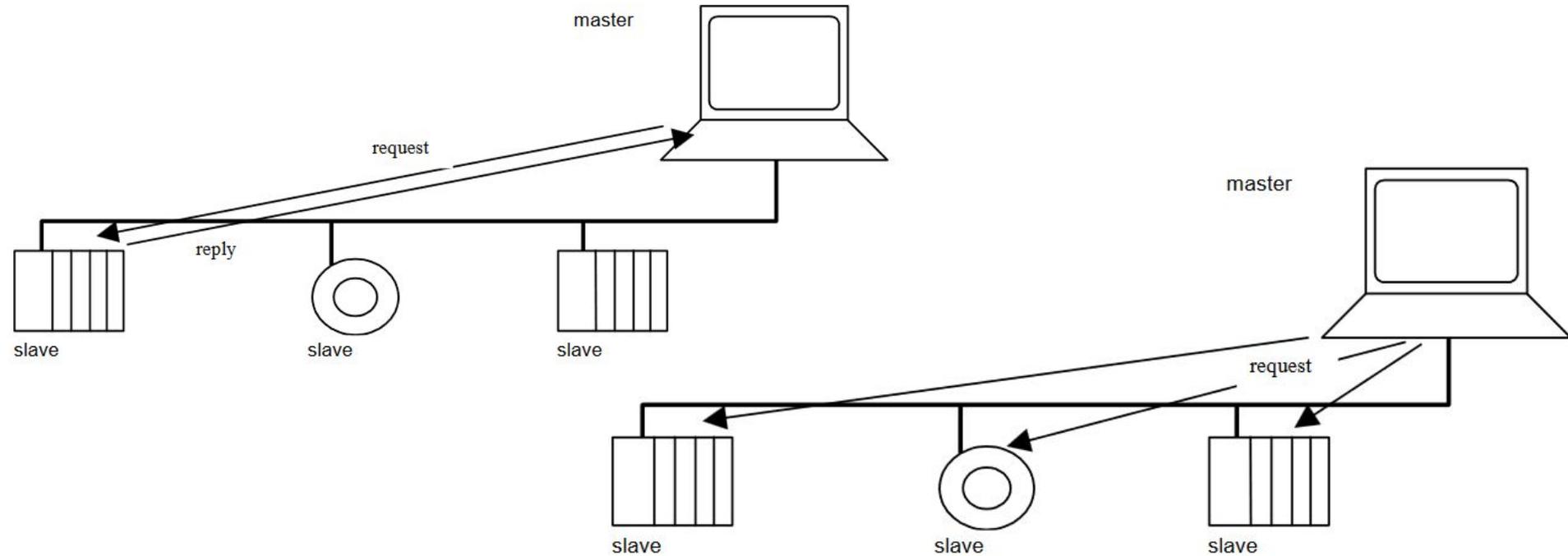
# MODBUS: recomendação de cores para fios

	<b>Signal Names</b>	<b>Recommended Color</b>
	<b>D1-TXD1</b>	<b>yellow</b>
	<b>D0-TXD0</b>	<b>brown</b>
	<b>Common</b>	<b>grey</b>
<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

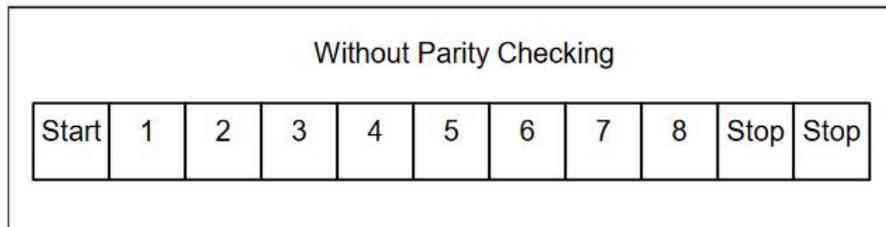
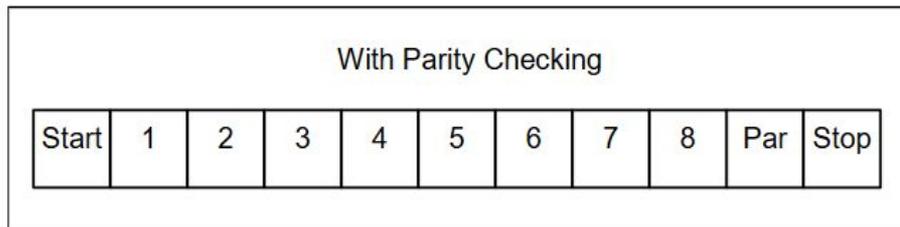
- Uma mensagem em MODBUS pode ser uma sequência que varia desde alguns poucos bytes (menos de 10) até algumas centenas (máximo de 256 bytes).
- Cada um dos serviços possui um formato de mensagem:
  - requisição;
  - resposta.

# Unicast x Broadcast

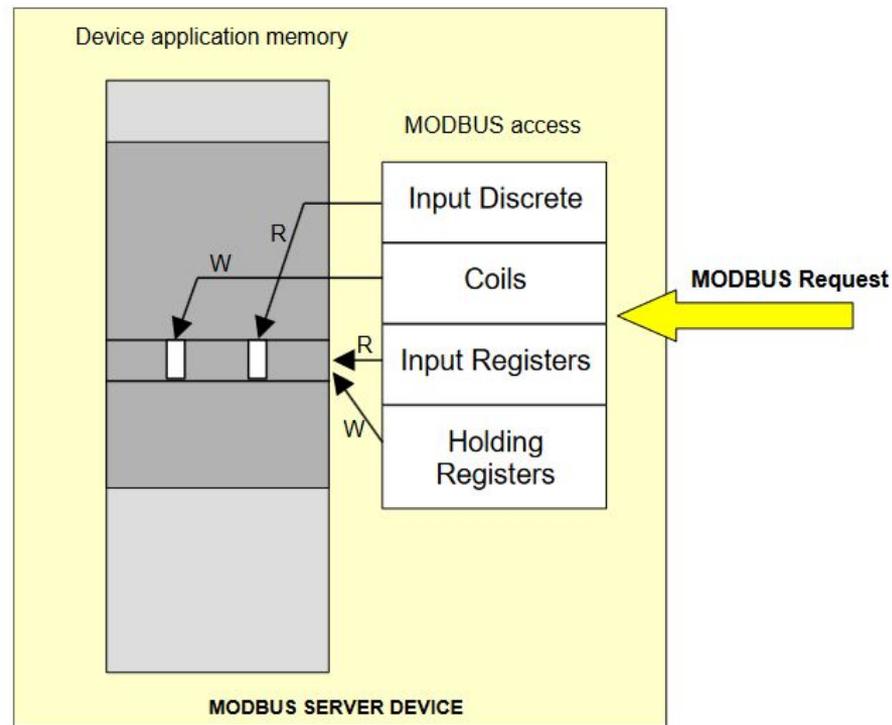
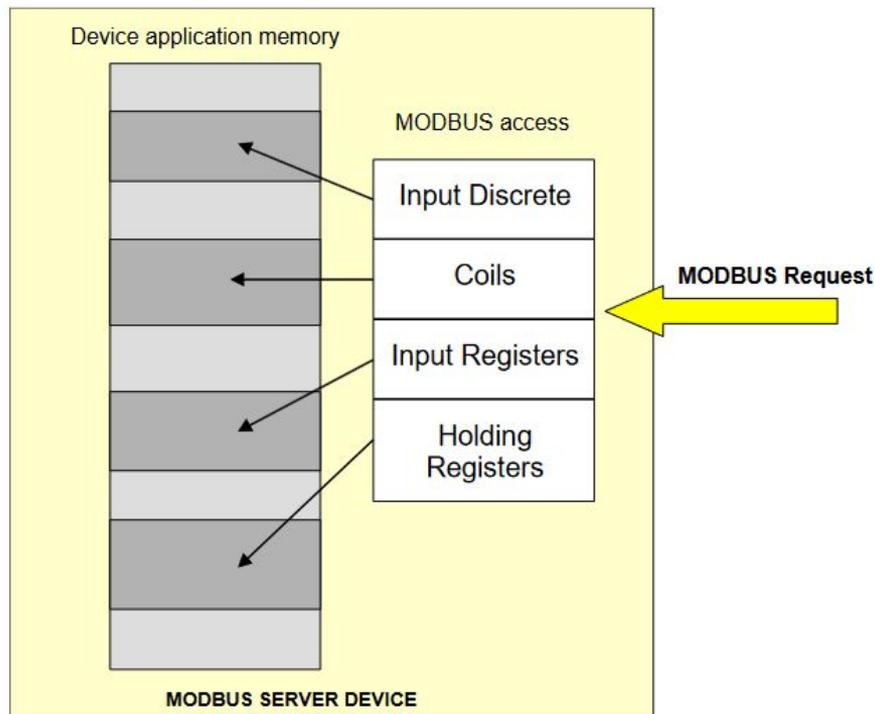


# Codificação de Mensagem em MODBUS

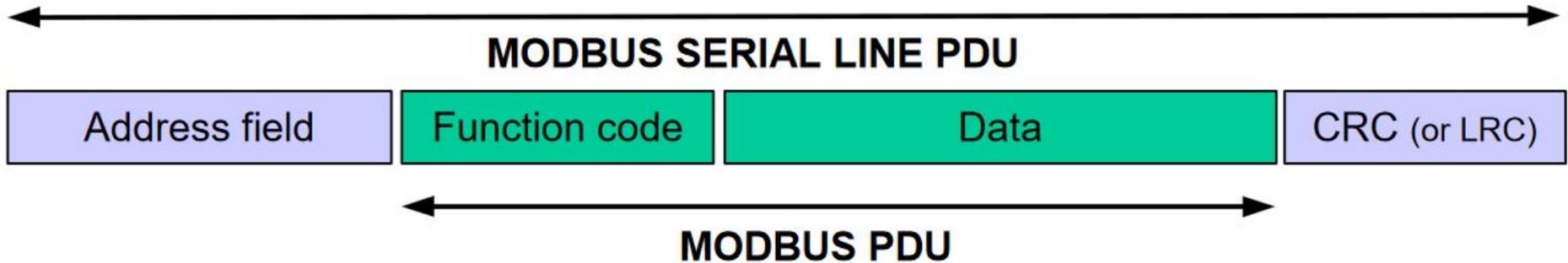
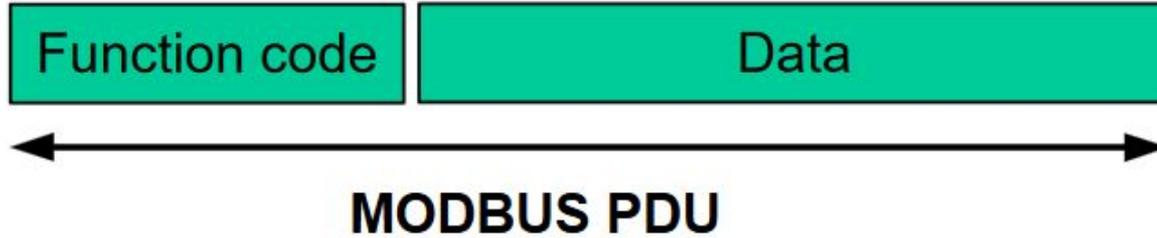
- As trocas de informações entre dispositivos, utiliza um conjunto de caracteres hexadecimais ou ASCII.
  - **MODBUS ASCII:** transmite dados de sete bits.
    - Gera mensagens legíveis, mas consome mais recursos da rede.
  - **MODBUS RTU** (*remote terminal unit*): Binário de oito bits



# Modelos de organização de memória



Unidade de Dados de Protocolo  
*Protocol Data Unit (PDU)*

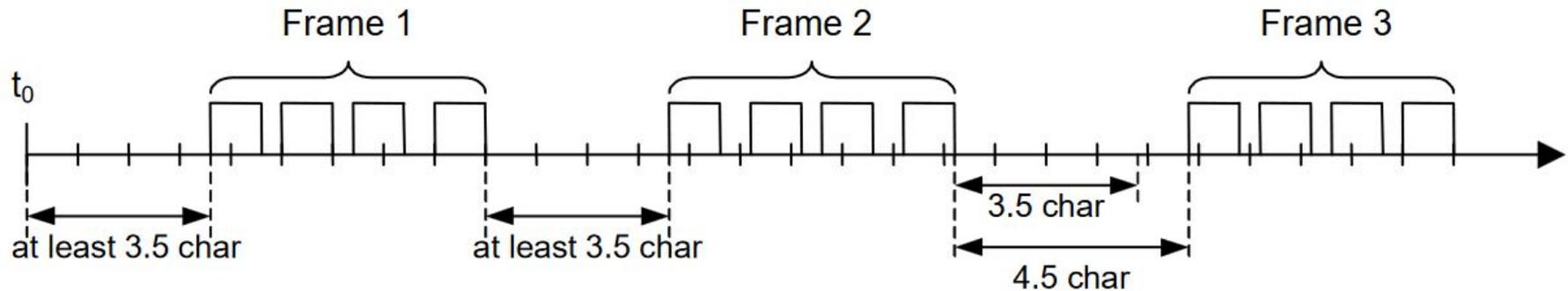
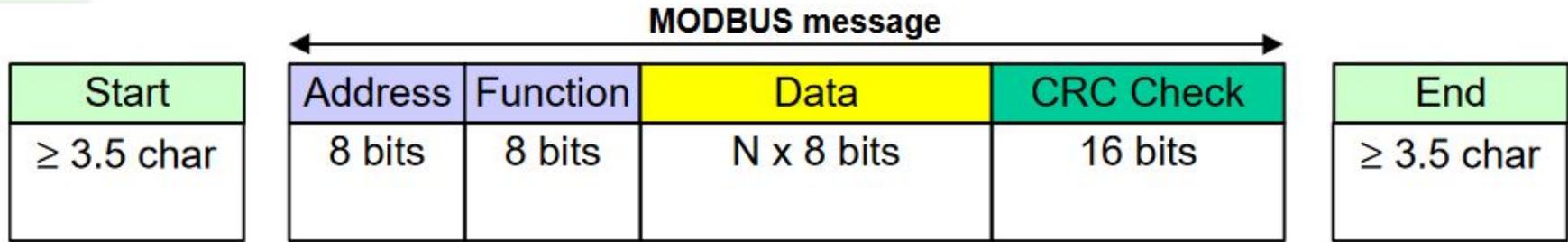


## *FRAME* de mensagem em MODBUS RTU

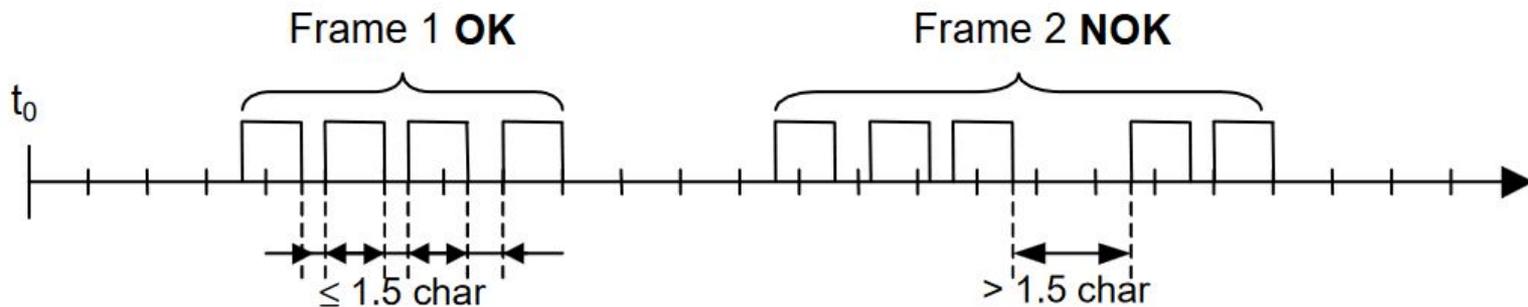
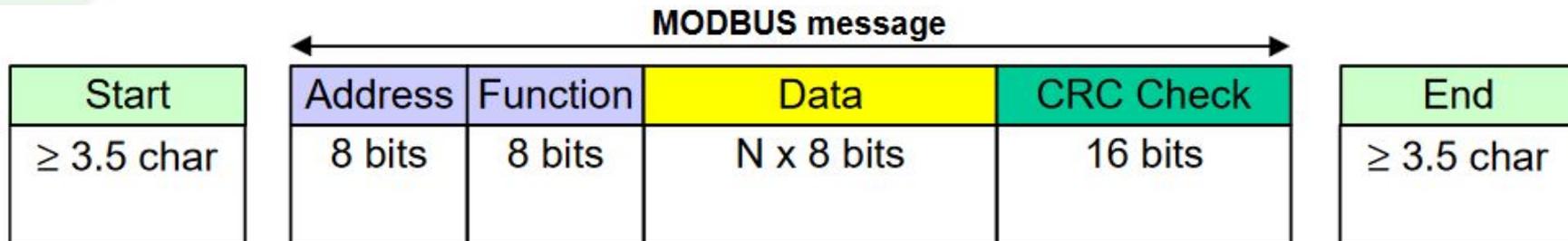
Slave Address	Function Code	Data	CRC
1 byte	1 byte	0 up to 252 byte(s)	2 bytes CRC Low   CRC Hi

Tamanho máximo do frame: 256 bytes

# Temporização de Mensagem em MODBUS



# Codificação de Mensagem em MODBUS



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

# 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	<b>Broadcast address</b>
1 .. 247	<b>Slave individual addresses</b>
248 .. 255	<b>Reserve</b>

# Codificação de Mensagem em MODBUS

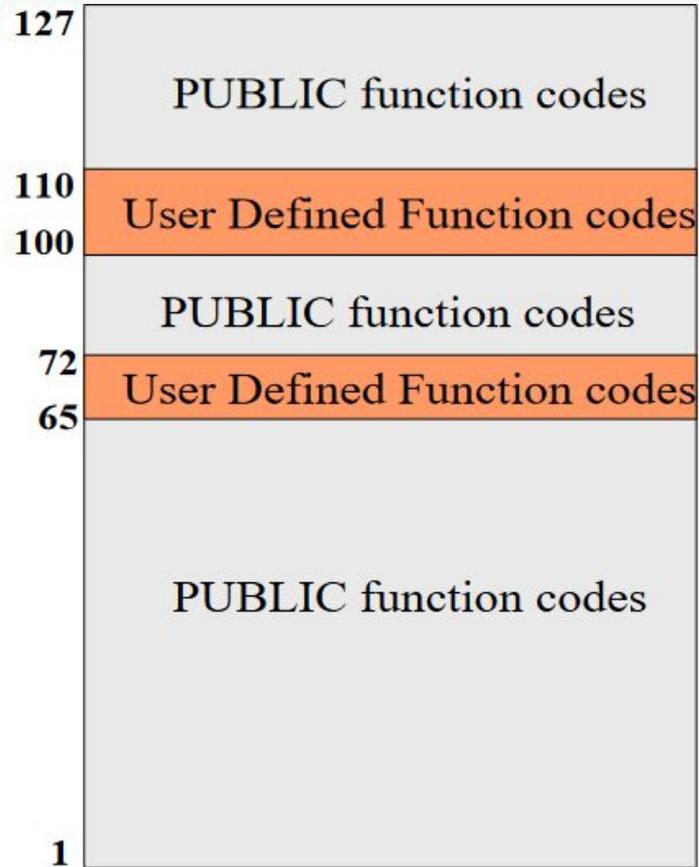
End Disp	Com	Dados				CRC
02	03	00	00	00	0A	2 caracteres

- 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		(hex)	Section
				code	Sub code		
<b>Data Access</b>	<b>Bit access</b>	Physical Discrete Inputs	Read Discrete Inputs	<b>02</b>		<b>02</b>	6.2
		Internal Bits Or Physical coils	Read Coils	<b>01</b>		<b>01</b>	6.1
			Write Single Coil	<b>05</b>		<b>05</b>	6.5
			Write Multiple Coils	<b>15</b>		<b>0F</b>	6.11
	<b>16 bits access</b>	Physical Input Registers	Read Input Register	<b>04</b>		<b>04</b>	6.4
		Internal Registers Or Physical Output Registers	Read Holding Registers	<b>03</b>		<b>03</b>	6.3
			Write Single Register	<b>06</b>		<b>06</b>	6.6
			Write Multiple Registers	<b>16</b>		<b>10</b>	6.12
			Read/Write Multiple Registers	<b>23</b>		<b>17</b>	6.17
			Mask Write Register	<b>22</b>		<b>16</b>	6.16
			Read FIFO queue	<b>24</b>		<b>18</b>	6.18
	<b>File record access</b>	Read File record		<b>20</b>		<b>14</b>	6.14
		Write File record		<b>21</b>		<b>15</b>	6.15
	<b>Diagnostics</b>	Read Exception status		<b>07</b>		<b>07</b>	6.7
		Diagnostic		<b>08</b>	<b>00-18,20</b>	<b>08</b>	6.8
Get Com event counter		<b>11</b>		<b>0B</b>	6.9		
Get Com Event Log		<b>12</b>		<b>0C</b>	6.10		
Report Server ID		<b>17</b>		<b>11</b>	6.13		
Read device Identification		<b>43</b>	<b>14</b>	<b>2B</b>	6.21		
<b>Other</b>	Encapsulated Interface Transport		<b>43</b>	<b>13,14</b>	<b>2B</b>	6.19	
	CANopen General Reference		<b>43</b>	<b>13</b>	<b>2B</b>	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	<b>0x01</b>
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of coils	2 Bytes	1 to 2000 (0x7D0)

## Response

Function code	1 Byte	<b>0x01</b>
Byte count	1 Byte	<b>N*</b>
Coil Status	<b>n</b> Byte	n = N or N+1

## Error

Function code	1 Byte	<b>Function code + 0x80</b>
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:

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

## 03 (0x03) Read Holding Registers

### Request

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

### Response

Function code	1 Byte	<b>0x03</b>
Byte count	1 Byte	2 x <b>N</b> *
Register value	<b>N</b> * x 2 Bytes	

\***N** = Quantity of Registers

### Error

Error code	1 Byte	<b>0x83</b>
Exception code	1 Byte	01 or 02 or 03 or 04

## 03 (0x03) Read Holding Registers

Requisição de leitura dos registradores 108 até 110:

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

# 06 (0x06) Write Single Register

## Request

Function code	1 Byte	<b>0x06</b>
Register Address	2 Bytes	0x0000 to 0xFFFF
Register Value	2 Bytes	0x0000 to 0xFFFF

## Response

Function code	1 Byte	<b>0x06</b>
Register Address	2 Bytes	0x0000 to 0xFFFF
Register Value	2 Bytes	0x0000 to 0xFFFF

## Error

Error code	1 Byte	<b>0x86</b>
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:

<b>Request</b>		<b>Response</b>	
<i>Field Name</i>	<i>(Hex)</i>	<i>Field Name</i>	<i>(Hex)</i>
Function	<b>06</b>	Function	<b>06</b>
Register Address Hi	<b>00</b>	Register Address Hi	<b>00</b>
Register Address Lo	<b>01</b>	Register Address Lo	<b>01</b>
Register Value Hi	<b>00</b>	Register Value Hi	<b>00</b>
Register Value Lo	<b>03</b>	Register Value Lo	<b>03</b>

# 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](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](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](https://www.modbus.org/docs/Modbus_over_serial_line_V1_02.pdf).