تهیه کننده:

امین موحدی

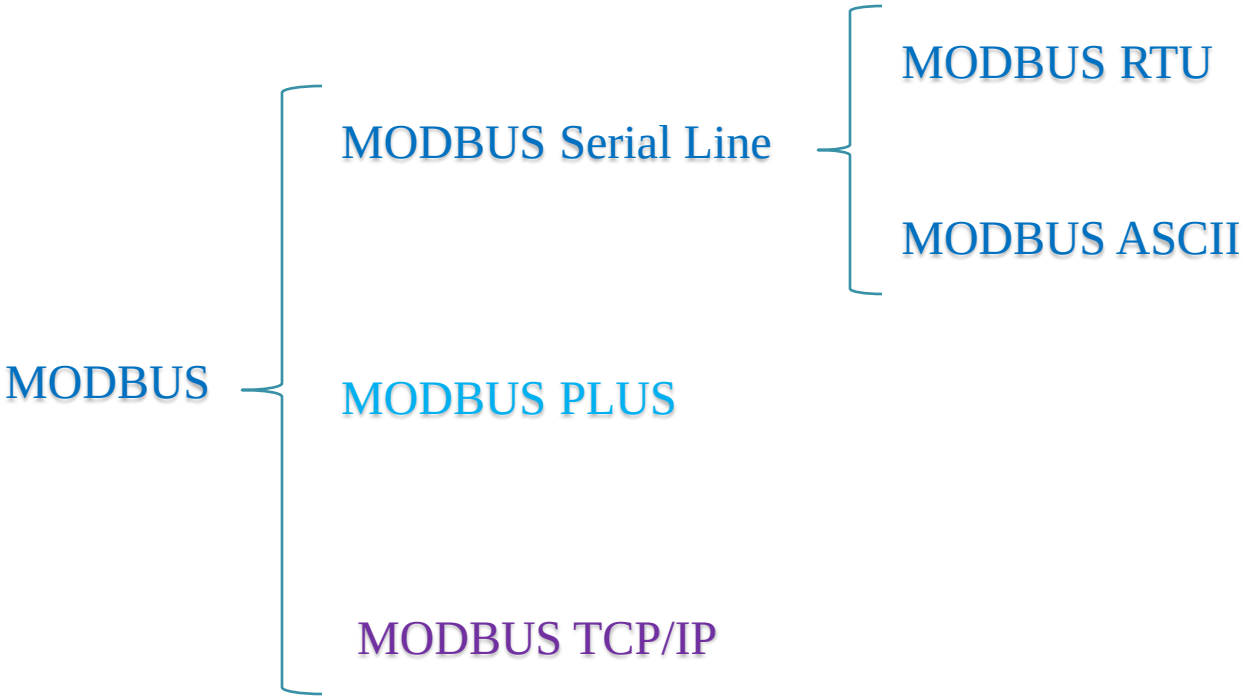
فهرست

- تاریخچه پروتکل MODBUS
- انواع MODBUS
- جایگاه MODBUS در هرم اتوماسیون صنعتی
- بررسی انواع MODBUS
- بررسی پیکربندی شبکه MODBUS

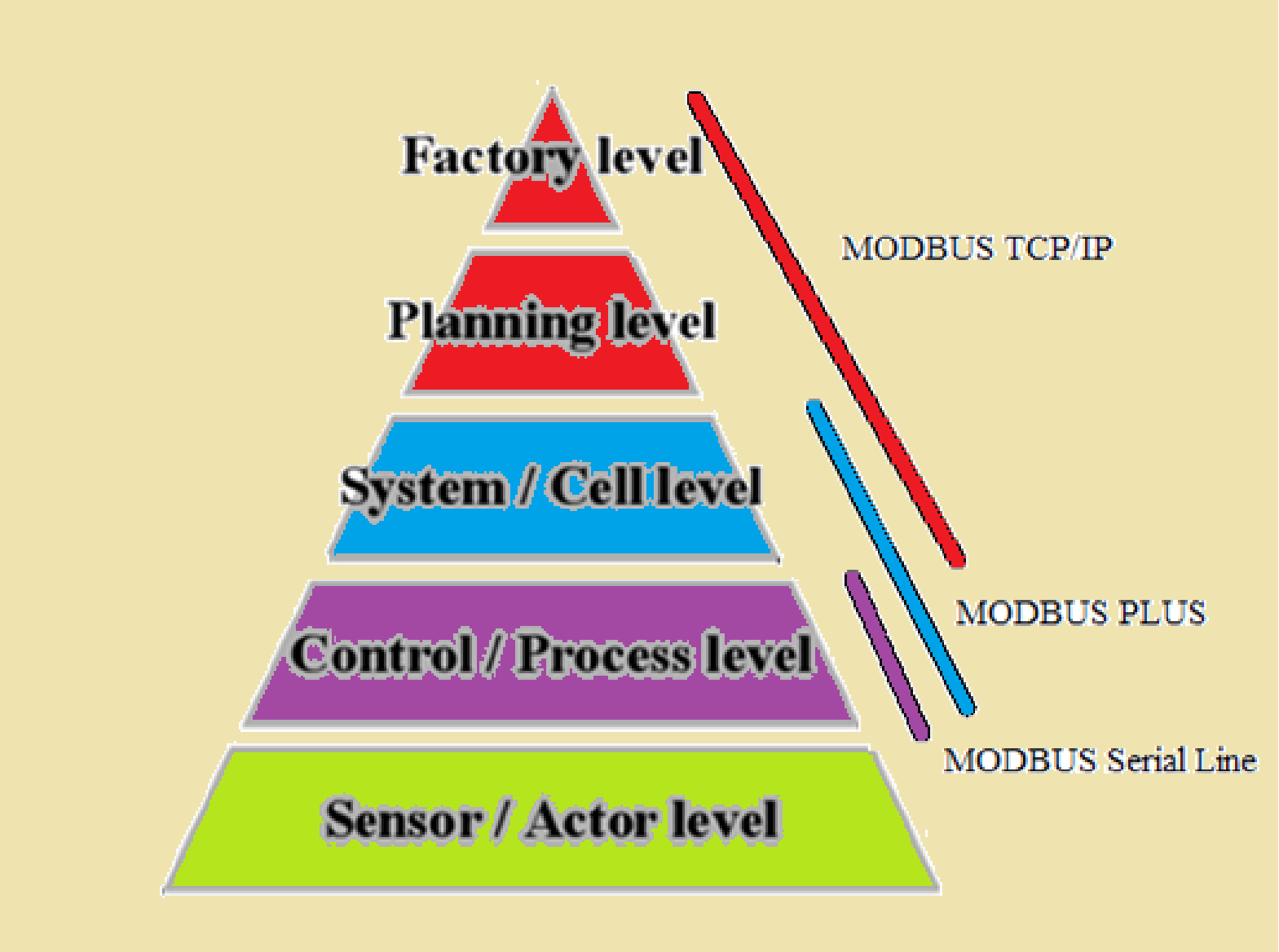
تاریخچه MODBUS

- پروتکل MODBUS توسط شرکت آمریکایی MODICON که یکی از زیر مجموعه های شرکت فرانسوی اشنایدر الکتریک است در سال 1979 بنیان گذاری شد.
- MODBUS دارای بیشترین محبوبیت را در بین پروتکل های صنعتی که امروزه استفاده می شوند را دارد به این دلایل که یادگیری آن ساده ،ارزان وعمومیت دارد.
- MODBUS قریب به 30 سال توانست این محبوبیت را در صنعت پیدا کند و سازندگان هر چه بیشتر برای محصولاتشان از آن استفاده کرده و آن را پشتیبانی کنند.
- MODBUS به سادگي امكان ارتباط بين بسياري از تجهيزات فيلد را با كامپوتر و همچنين سيستمهاي اسكادا را فراهم مي كند.
- MODBUS یک پروتکل برنامه کاربردی است که دارای سه نسخه مختلف برای شبکه بندی است. این سه نسخه به ترتیب MODBUS Serial Line، MODBUS PLUS و MODBUS TCP/IP نام دارد که از این سه نوع MODBUS Serial Line و MODBUS TCP/IPبیشترین کاربرد را دارند.

انواع MODBUS

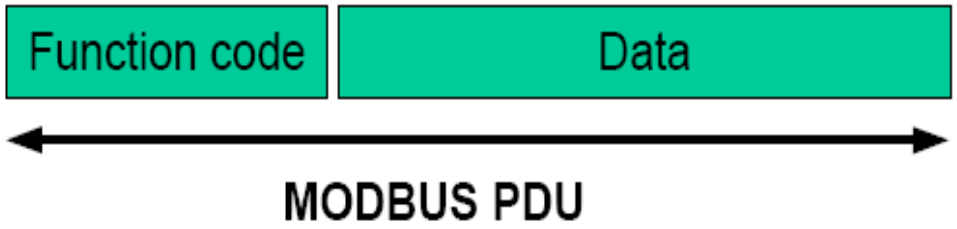


جایگاه MODBUS در هرم اتوماسیون



پروتکل MODBUS

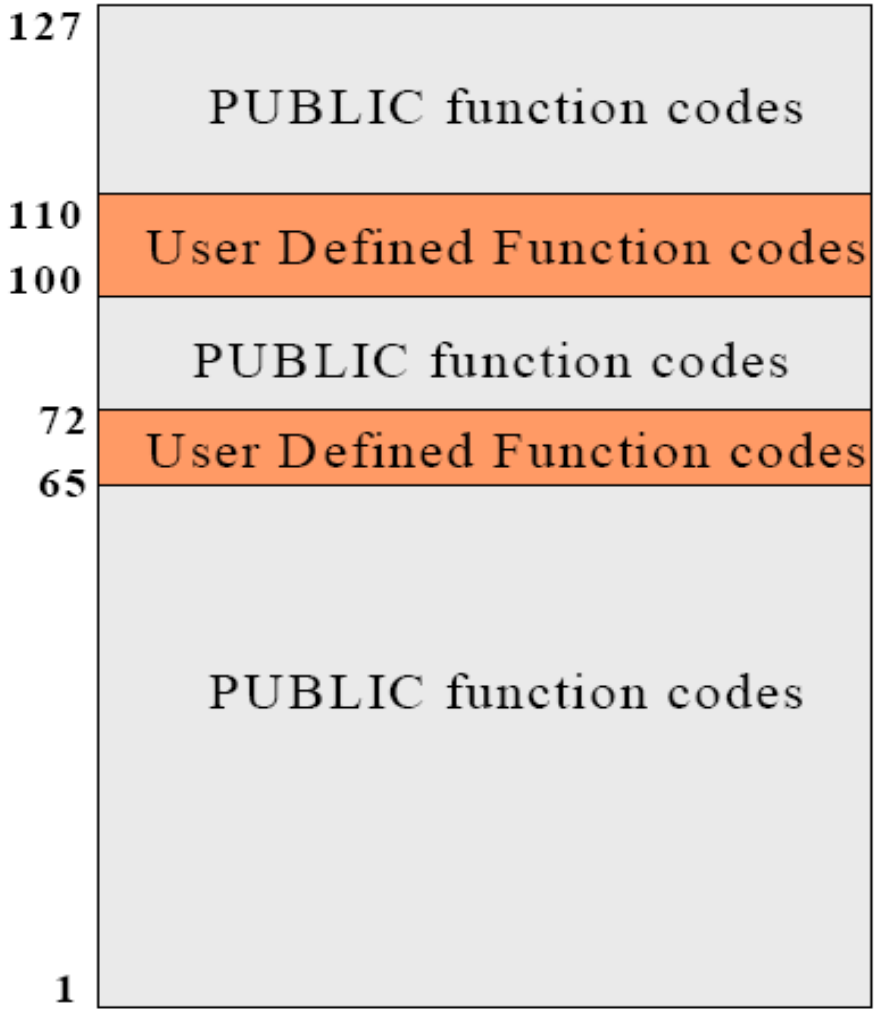
- پروتکل MODBUS از PUD (Protocol Data Unit) های ساده ای تشکیل شده است.



- توابع کد در MODBUS
  - فیلد Function Code یک بایت است که می تواند بین ۱ تا ۲۵۵ دسیمال باشد.
  - Function Code به دو دسته تقسیم می شود.

1. توابع عمومي
2. توابع خاص

انواع توابع کد

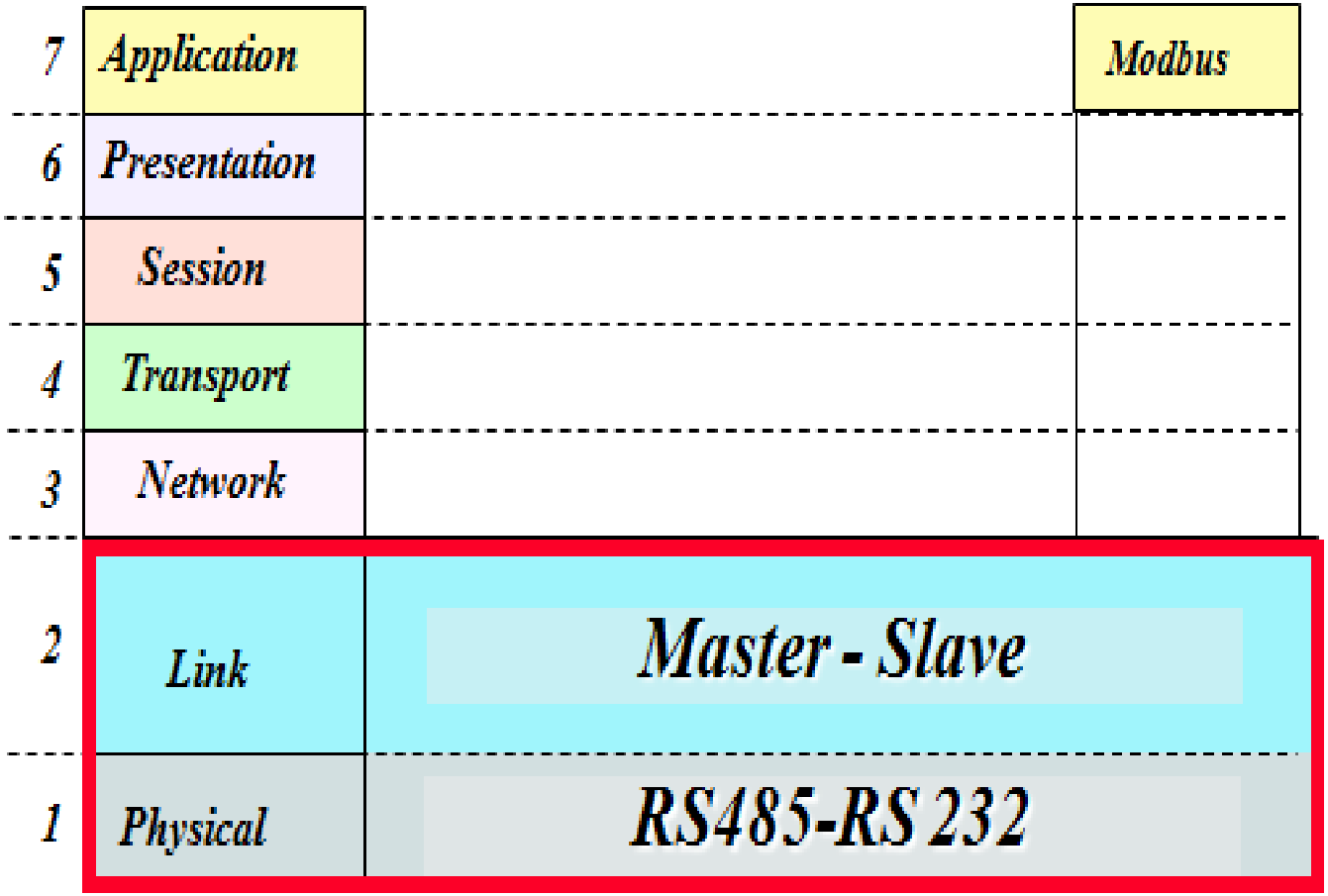


توابع عمومی

				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**	6.14
			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**		**OB**	6.9
			Get Com Event Log	**12**		**0C**	6.10
			Report Slave ID	**17**		**11**	6.13
			Read device Identification	**43**	**14**	**2B**	6.21
	Other		Encapsulated Interface Transport	**43**	**13,14**	**2B**	6.19

Network MODBUS RTU/ASCII

MODBUS از هفت لایه مدل OSI از سه لایه آن استفاده می کند.



لایه پیوند داده در MODBUS

۱. پروتکل Master/Slave

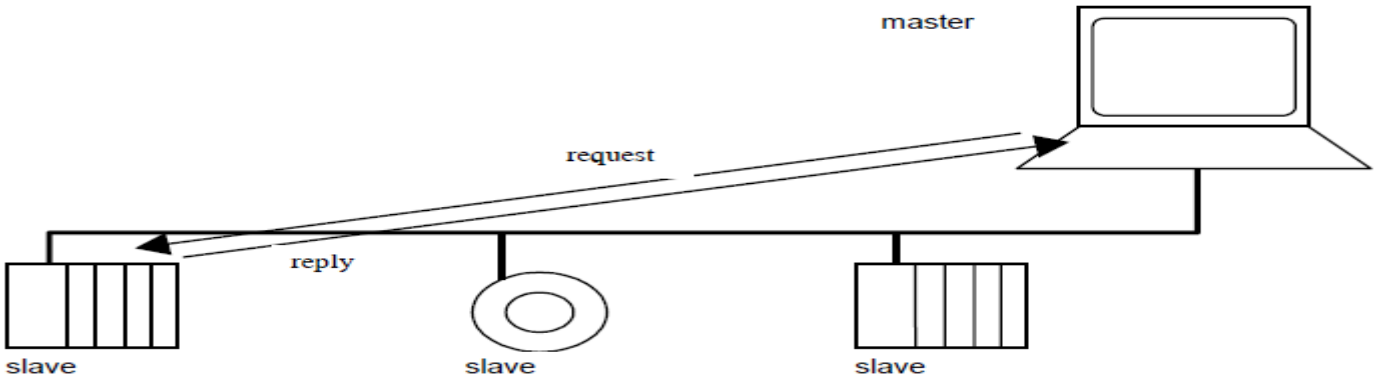
۲. مدهای انتقال RTU/ASCII

✓پروتکل Master/Slave

- این لایه از تکنیک دسترسی Master/Slave استفاده می کند. بنابراین فقط یک Master می تواند باس را دراختیار داشته و با ماکزیمم ۲۴۷ Slaveکه به همان باس متصل هستند ارتباط برقرارکند.
- دراین تکنیک دسترسی Slave ها به باس هیچگاه بودن درخواست Master امکان پذیر نخواهد بود.
- بعد از درخواست فقط Slave ها می توانند با Master ارتباط برقرار کنند و نمی توانند با دیگر Slave ها ارتباط برقرار کنند.

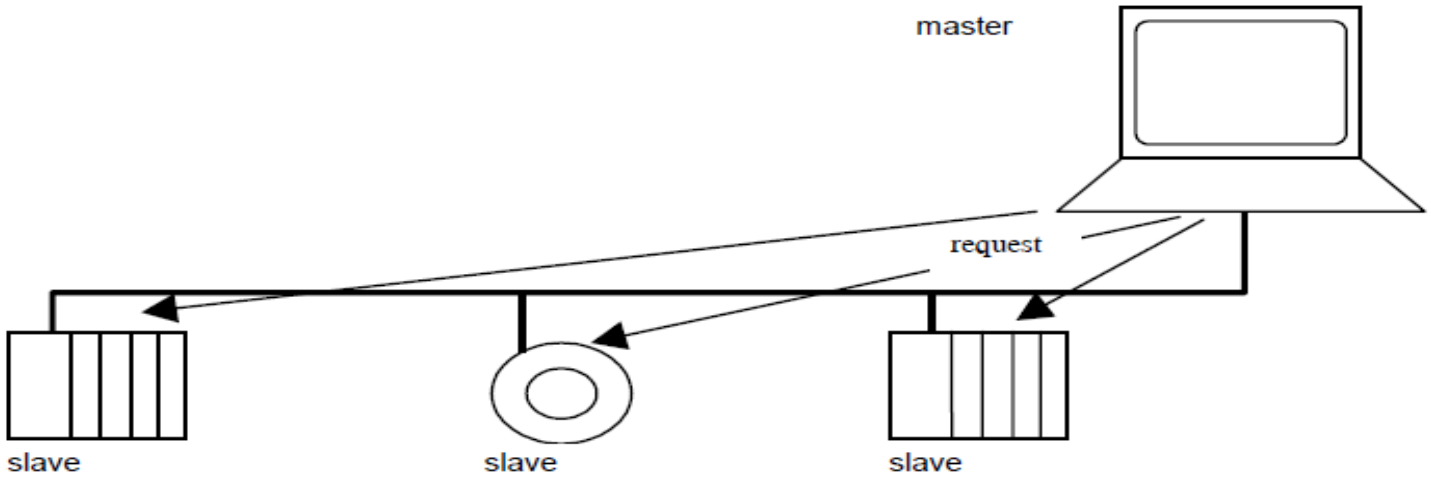
Master به یکی از دو روش زیر درخواست خود را ارسال می کند.

1. مد Unicast: دراین حالت Master از Slave خاصی درخواست دیتا می نماید.
2. مد Broadcast :دراین حالت Master پیام خود را به تمامی Slave ها می فرستد ولی هیچ پاسخی به Master برنمی گردد. برای مد Broadcast آدرس صفر رزور شده است.



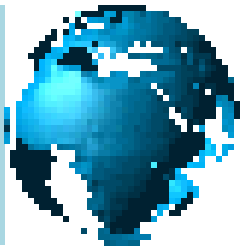
مد Unicast

- مد Broadcast



MODBUS

Modbus RTU/ASCII



کانکتورهای فیزیکی

Point to Point
RS-232
Multi drop
RS-422 and RS-485

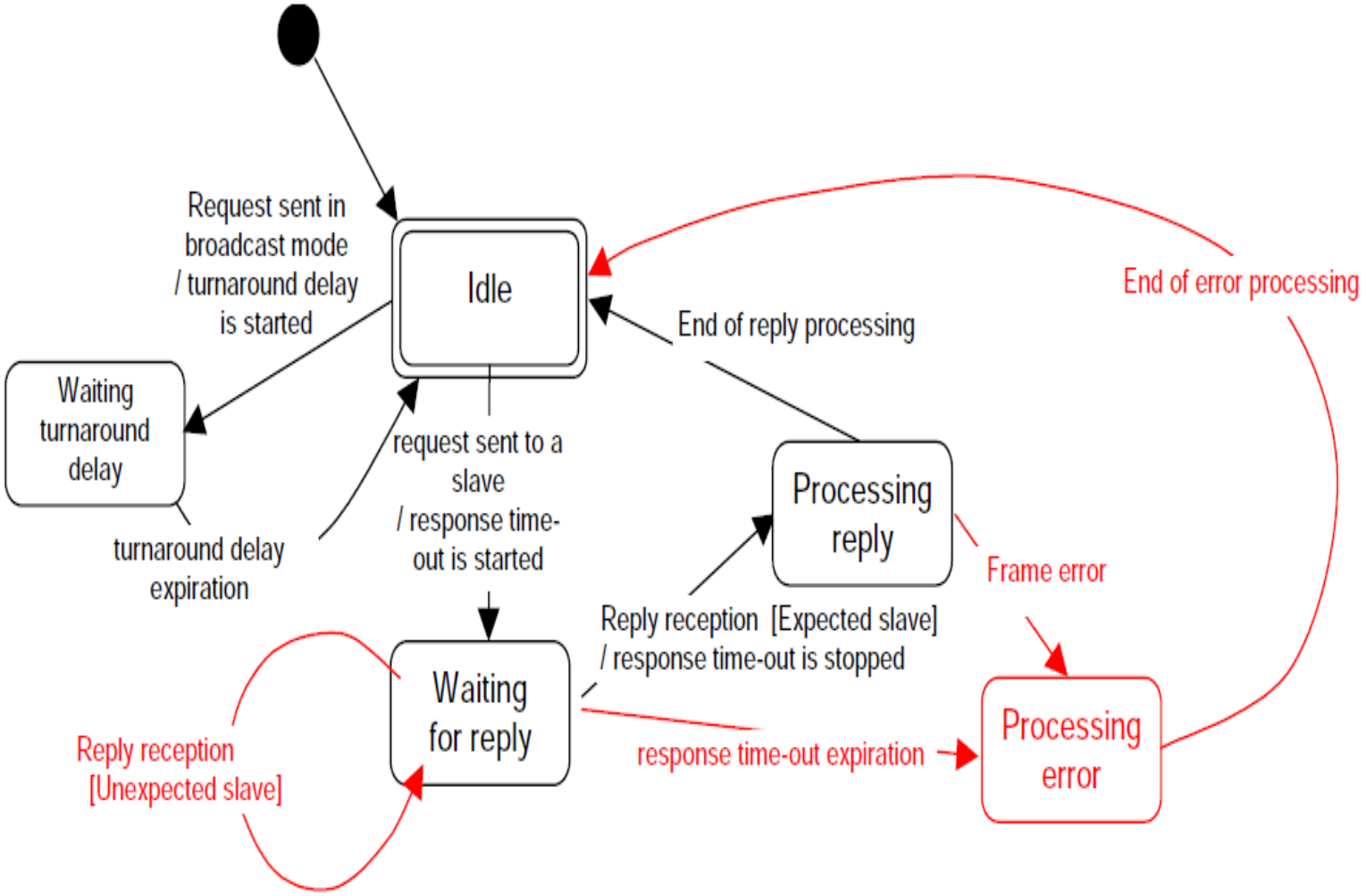
پیاده سازی سخت افزاری

Standard UART technology

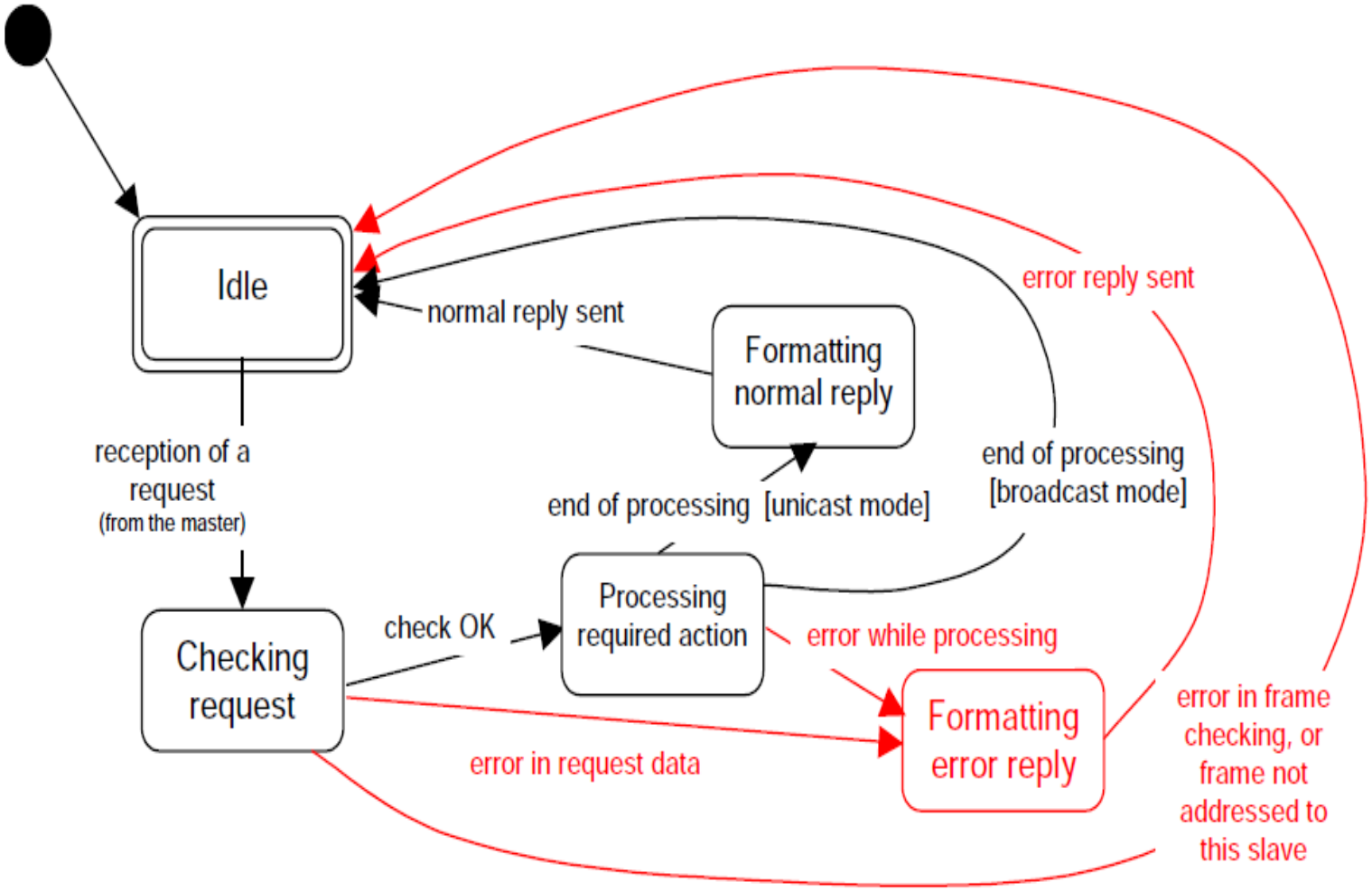
سرعت ارتباط

Baud rates : 1200 to 38400

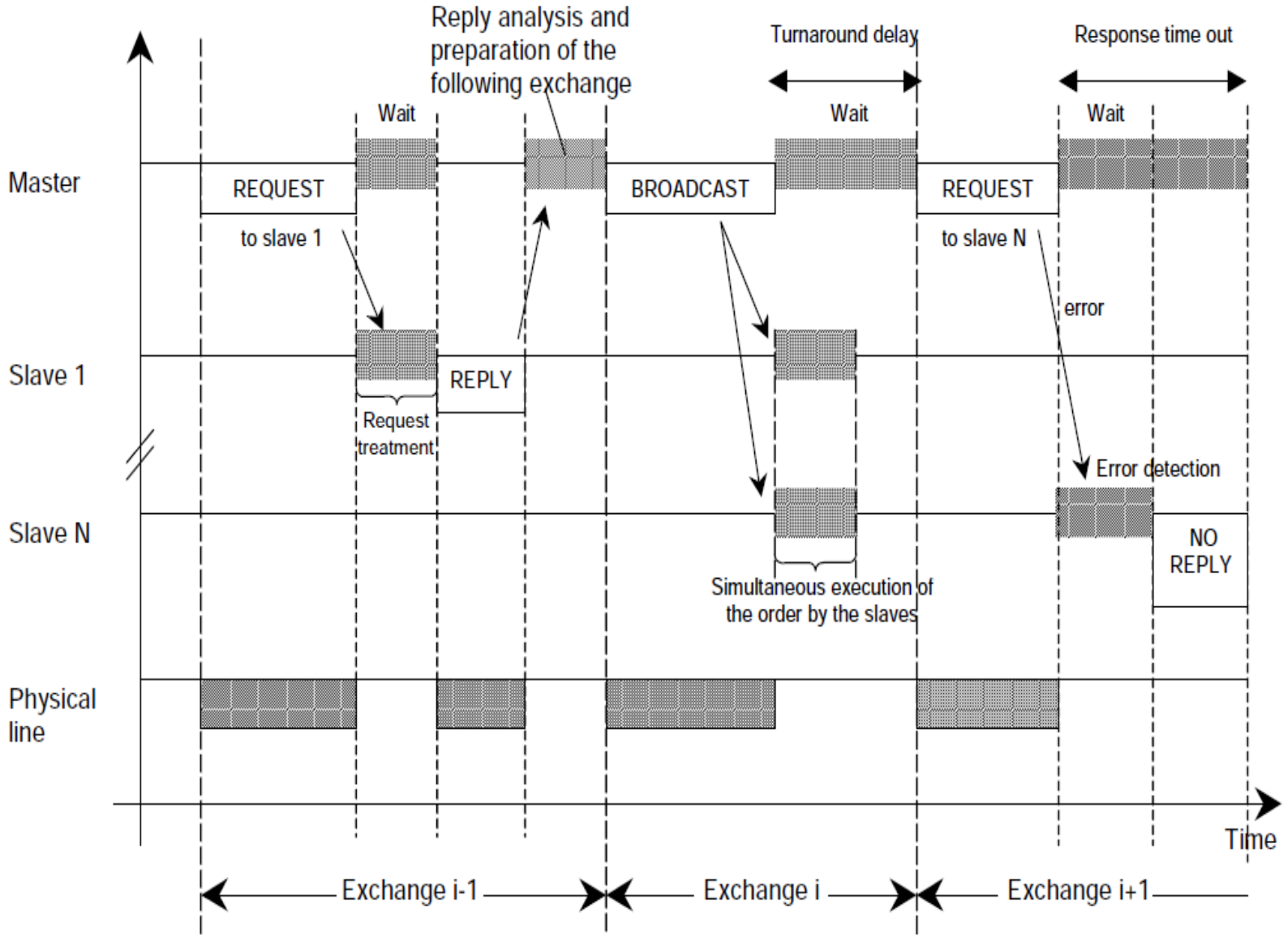
دیاگرام حالت Master



دیاگرام حالت Slave



دیاگرام زمانی بین Master/Slave



✓ساختار فریم بندی درمدل RTU

Start	address	Function Code	Data	Error Check	End
3.5 Char	1 Char	1 Char	n Chars	2 Chars	3.5 Chars
Silence				CRC	Silence

Start =3.5 کاراکتر فاصله زمانی

Address=0 ~ 247

Function code =0~256

Data= برای هر کاراکتر۱۱ بیت و حداکثر252 کاراکتر

➢*در مدل* RTU *هر بایت از داده به صورت زیر دسته بندی می شود.*

1 Start Bit	8 Data Bits	1 Parity Bit (Even/Odd)	1 Stop Bit
1 Start Bit	8 Data Bits	2 Stop Bit	

✓ساختار فریم بندی درمدل ASCII

Start	address	Function Code	Data	Error Check	End
1 Char	2 Chars	2 Chars	n Chars	2 Chars	2 Chars
:				LRC	CR,LF

Start=3A hex

Address=0 ~ 247

Function code =0~256

Data= برای هر کاراکتر ۱۰ بیت و حداکثر ۵۰۴ کاراکتر

➢***در مدل*** ASCII ***هر بایت از داده به صورت زیر دسته بندی می شود.***

1 Start Bit	7 Data Bits	1 Parity Bit (Even/Odd)	1 Stop Bit
1 Start Bit	7 Data Bits	2 Stop Bit	

مرجع آدرس دهی دیوایس ها

- ✓ دیوایس های MODBUS معمولا دارای یک نقشه رجیستر ها هستند که شما باید به نقشه رجیسترهای دیوایس، برای درک عملکرد آنها مراجعه کنید.
- ✓ مدل داده MODBUS ساختار ساده ای دارد که بین چهار نوع داده پایه تقسیم بندی می شود که به ترتیب زیر است.

Table Addresses	Type	Table Name
1-9999	Read or Write	Coils
10001-19999	Read Only	Discrete Inputs
30001-39999	Read Only	Input Registers
40001-49999	Read or Write	Holding Registers

مثال: آدرس های حافظه کنترل دما

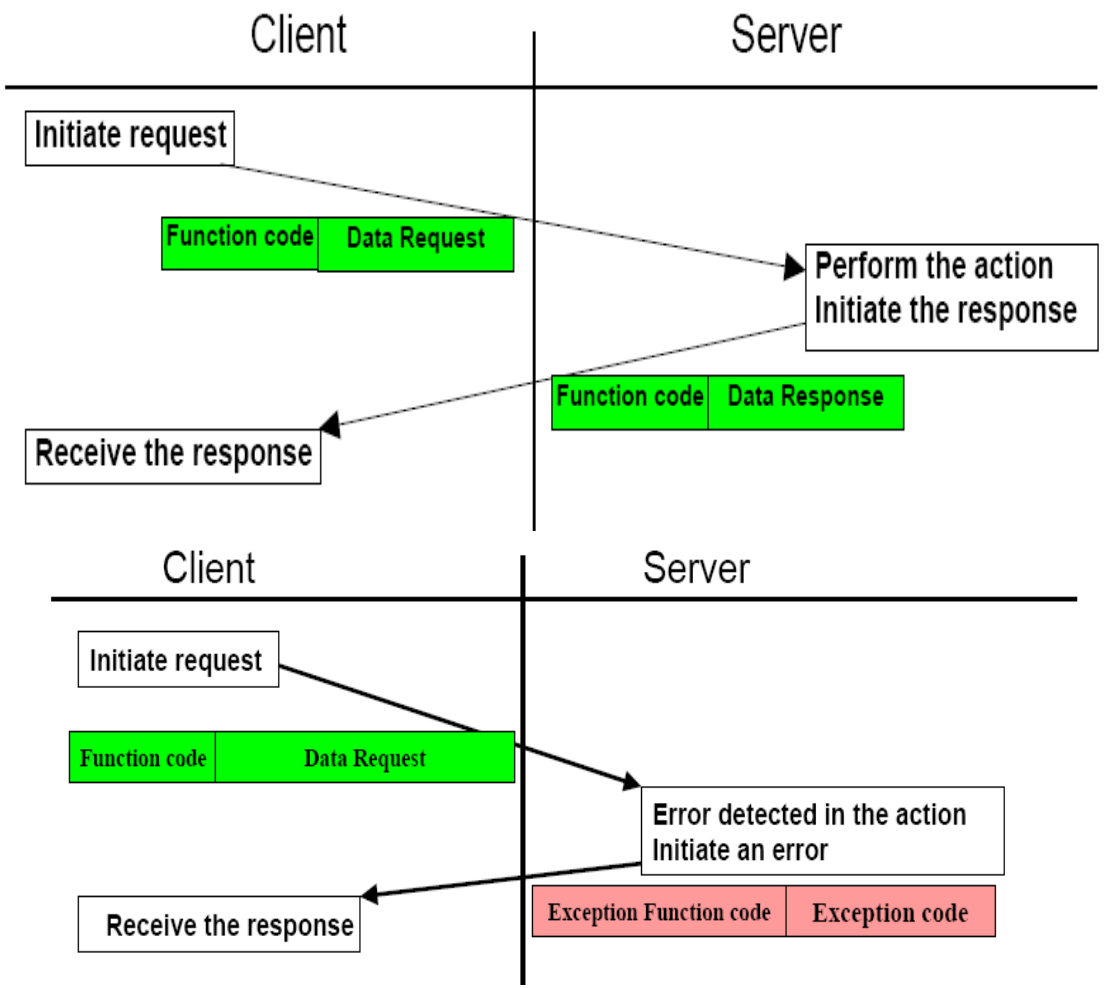
Address	Content	Explanation
1000H	Process value (PV)	Measuring unit is 0.1, updated one time in 0.4 second The following reading value display indicates error occurs: 8002H: temperature not acquired yet 8003H: temperature sensor not connected 8004H: wrong sensor type 8006H: unable to acquire temperature, ADC input error 8007H: unable to read/write the memory
1001H	Set point (SV)	Unit is 0.1, ₀C or ₀F
1002H	Upper-limit of temperature range	The data content should not be higher than the temperature range
1003H	Lower-limit of temperature range	The data content should not be lower than the temperature range
1004H	Input temperature sensor type	Please refer to the contents of the “Temperature Sensor Type and Temperature Range” for detail
1005H	Control method	0: PID, 1: ON/OFF, 2: manual tuning, 3: PID grogram control
1006H	Heating/Cooling control selection	0: Heating, 1: Cooling
1009H	PB Proportional band value	0.1 ~ 999.9
100AH	Ti Integral time	0~9999
100BH	Td Derivative time	0~9999

1001H ⟶ 9C41 H(40001) + 1001 H= AC42 H (44098)

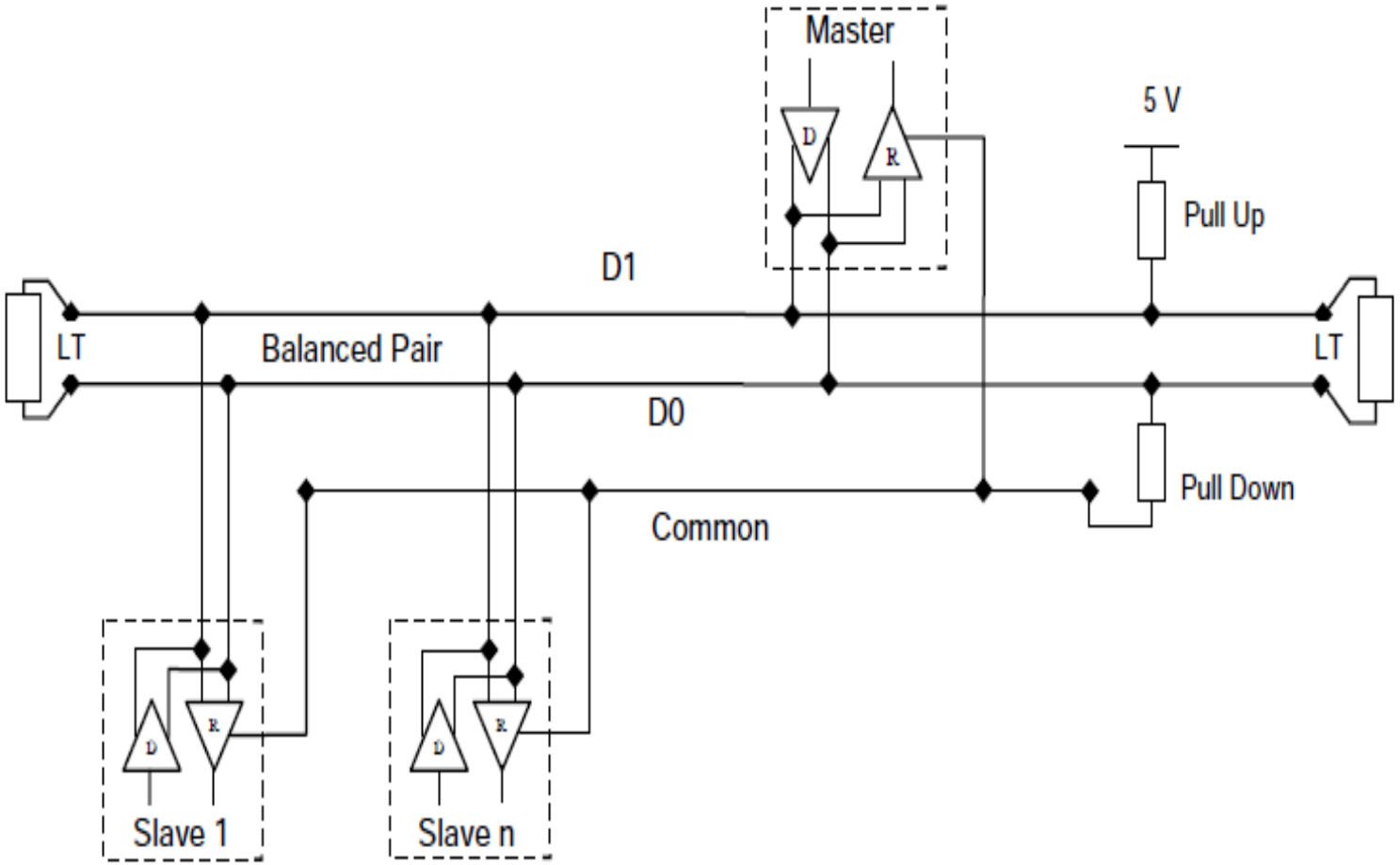
مثال :آدرس دهی حافظه درایو

محتویات	آدرس	کاربردها	
خواندن / نوشتن فرمان	2000 H	بیت 0-1	00: بدون کاربرد 01: توقف 10: اجراء 11: اجراء + jog
		بیت 2-3	ذخیره
		بیت 4-5	00: بدون کاربرد 01: استگرد 10: جیگرد 11: تغییر جهت
		بیت 6-15	ذخیره
	2001 H	فرمان فرکانس	
	2002 H	بیت 0	1 : خطای خارجی
		بیت 1	1 : ری ست
		بیت 2-15	ذخیره
نمایش حالات فقط خواندنی	2100H	**کد خطا :** 00: خطائی اتفاق نیافتاده است 01: جریان اضافه (OC) 01: دمای اضافه (OH) 04: اضافه بار درایو (OL) 05: اضافه بار موتور (D1) 06: خطای خارجی (EF) 07: نقص CPU (CF1) 08: نقص CPU یا مدار آنالوگ (CF3) 09: نقص مدار محافظتی سخت افزار (HPF) 10: اضافه جریان نسبت به جریان درحین زمان افزایش شتاب (OCA) 11: اضافه جریان نسبت به جریان در حین زمان کاهش شتاب (OCD) 12: اضافه جریان نسبت به جریان در حین عملکرد ثابت (OCN) 13: خطای زمین (GF) 14: ولتاژ پایین (LV) 15: ذخیره 16: نقص CPU 1 (CF2) 17: Base Block 18: اضافه بار (OL2) 19: نقص در افزایش /کاهش اتوماتیک شتاب (CFA) 20: فعال شدن مدار محافظتی نرم افزار (CODE)	

نحوه ارتباطات بین Client/Server



شماتیک سیم بندی در استاندارد RS 485 دو سیمه



طول شبکه

ماکزیمم طول شبکه وابسته است به:

الف) سرعت انتقال baud rate

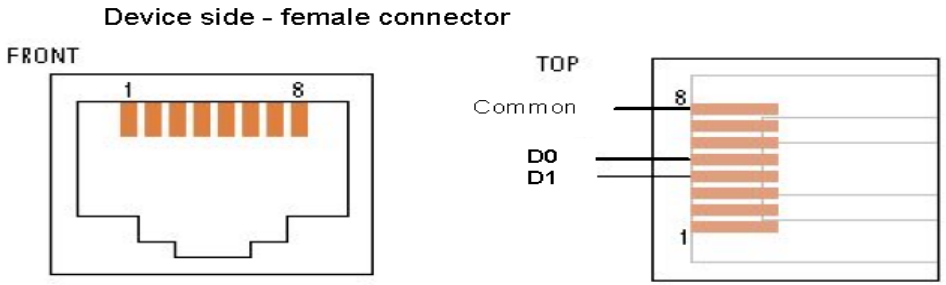
ب) نوع کابل (مشخصه امپدانس)

ج) تعداد ایستگاه ها (هر ایستگاه به عنوان یک بار جریانی محسوب می شود)

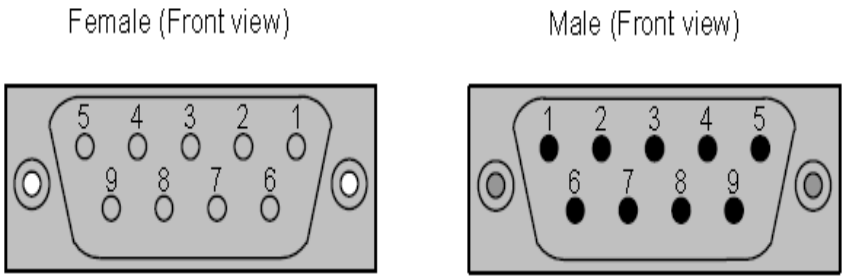
د) پیکربندی شبکه (۲سیمه یا ۴ سیمه)

کانکتور ها

- در MODBUS سریال از کانکتورهای RJ 45 و DB-9 استفاده می شود که در این کانکتورها استفاده از چند پایه الزامی است و استفاده از بقیه پایه ها اختیاری می باشد.



RJ 45



DB-9

رنگ بندی سیم ها

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

SD-GEM Modbus RTU / Ethernet gateway

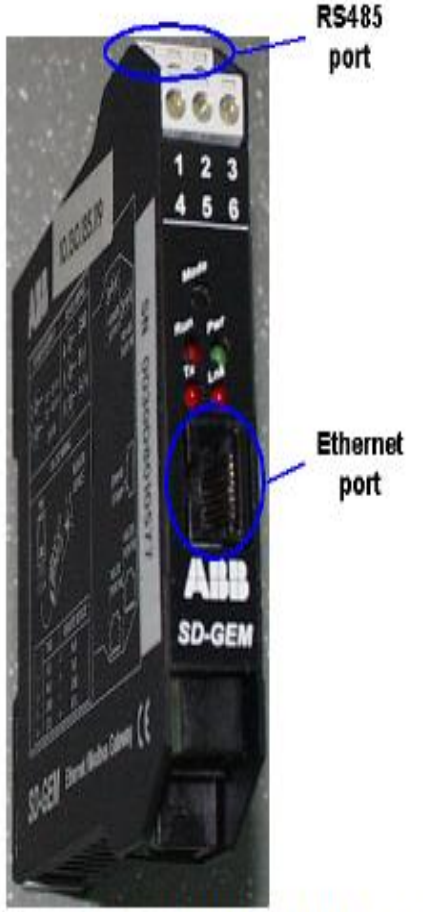


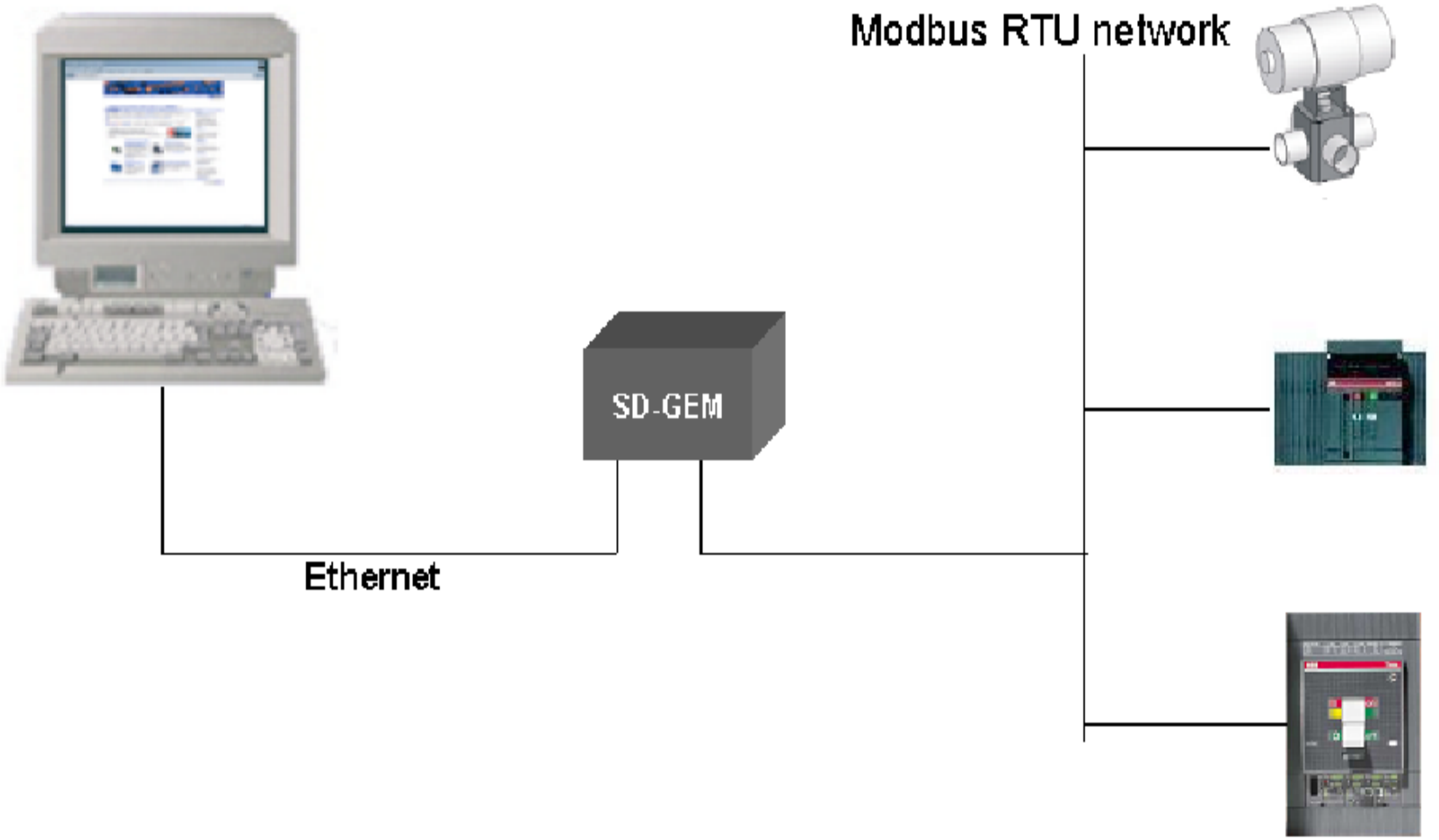
Figure 1: SD-GEM Ethernet and RS-485 port

- برای اتصال بین شبکهmodbus RTU
وشبکه modbus Tcp/IPاستفاده می شود.
SD-GEM اطلاعات را از شبکه modbus گرفته
فریم بندی مجدد کرده وآن را دوباره ارسال می کند.
این ماژول با نرم افزار / Windows 2000
Windows XP and Internet Explorer
می تواند کار کند.

SD-GEM terminals	
2	+24V DC power supply
3	0V DC power supply
4	ground
5	RS-485 DATA+
6	RS-485 DATA-

MODBUS

طریقه اتصال SD-GEM



ماژولهای I/O



- یک راه آسان برای وصل کردن تجهیزات به یک سبستم کنترل فرایند ،PLC یا کامپیوترهای دیجیتال استفاده از کانکتورهای دیجیتال وآنالوگ I/O است.

- به عنوان مثال NCS (NET concentrator system) که برای اتصال تجهیزات در فاصله دور استفاده می شود که چندین NCS در چند محل نصب می شوند.

- یک سیستم توزیع شده I/O تطبیق می دهد تمام I/O که وجود دارد یا اطلاعات را به صورت عا دلانه به تجهیزات بفرستد.

MODBUS

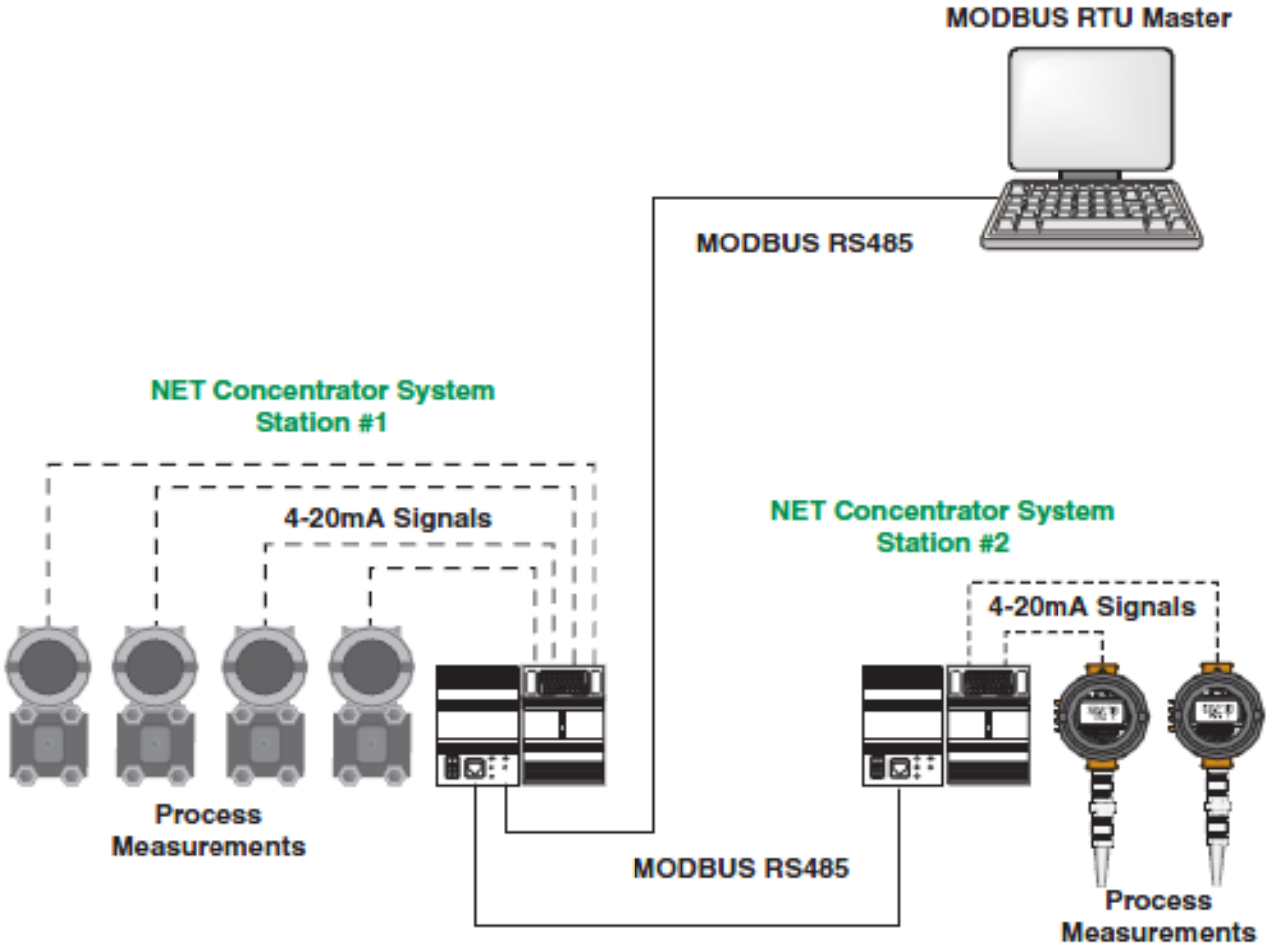
Modbus-RTU I/O Modules



- **Analog Input**
- DC current
- DC voltage
- DC millivolts
- RTD/resistance
- AC current
- **Analog output**
- DC voltage
- DC current
- Open drain MOSFETs
- **Inputs**
- Active-high inputs, 0 to 35V DC
- Active-low inputs, 0 to 35V DC
- **Outputs**
- Sourcing outputs, 5.5 to 35V DC, 250mA
- Sinking outputs, 0 to 35V DC, up to 1A

MODBUS

Modbus- I/O مثالی از Modules

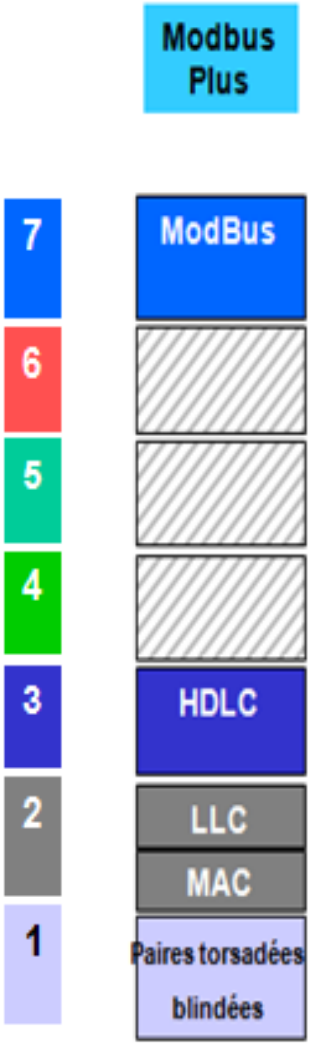


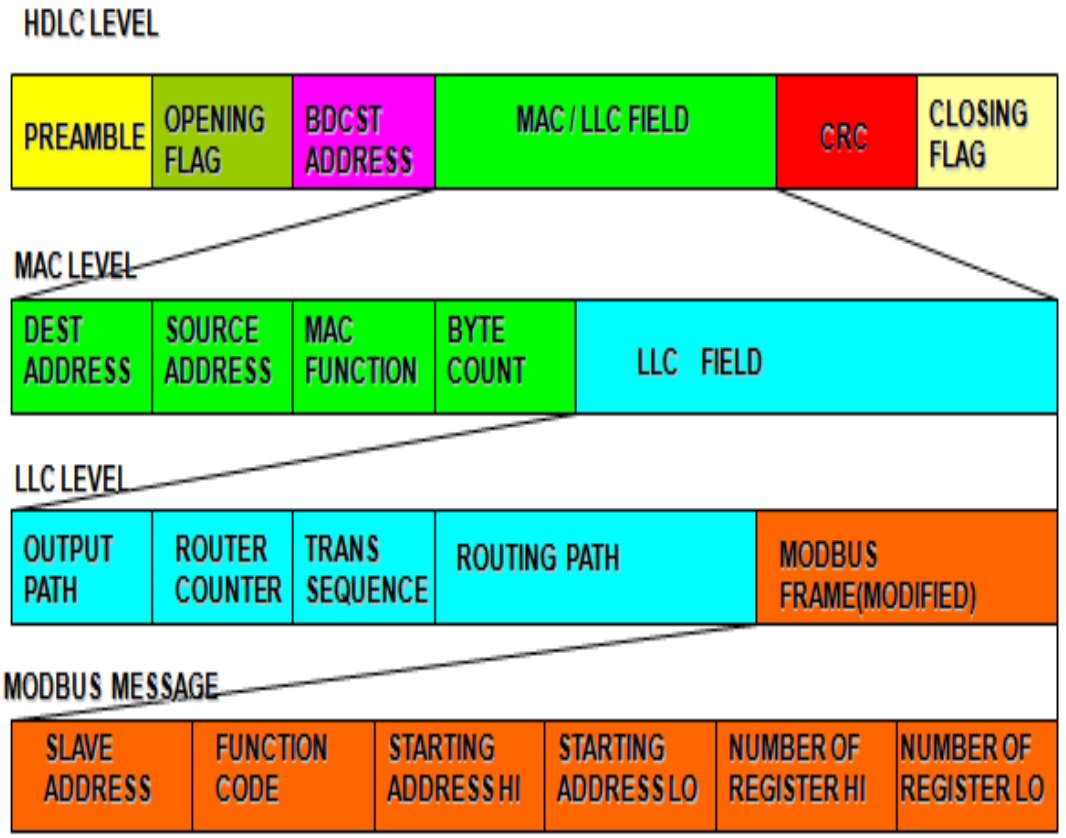
MODBUS PLUS

MODBUS PLUS

- این شبکه یک شبکه اختصاصی و در انحصار شرکت MODICON است و بیشتر برای شبکه کردن تجهیزات این شرکت و اشنایدر الکتریک مورد استفاده قرار می گیرد.

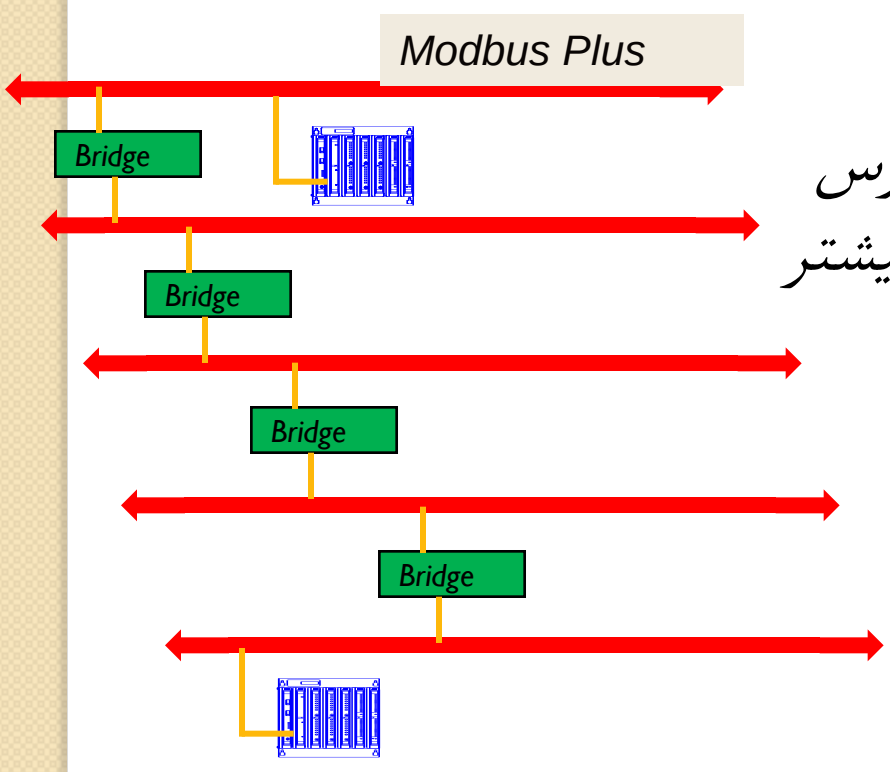
MODBUS PLUS در مدل OSI





خصوصیات modbus plus

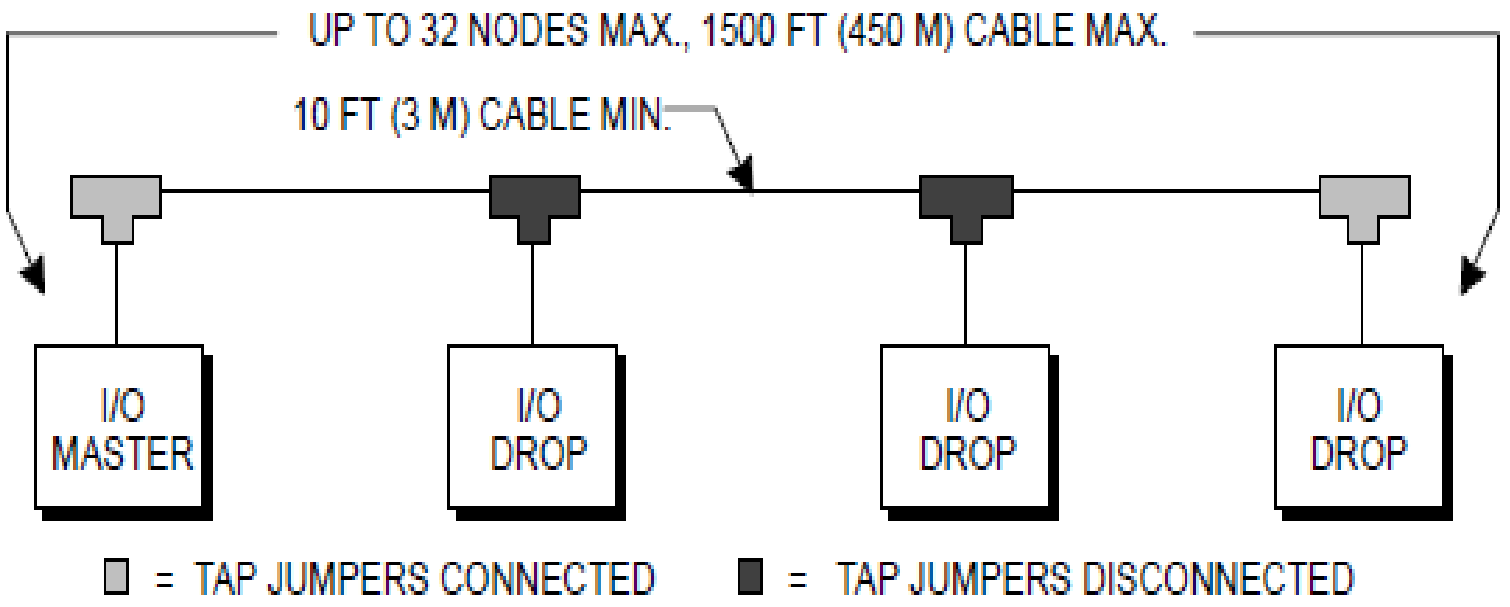
- پیاده سازی ساده
- قابلیت multi master
- سرعت انتقال 1Mbit/s
- برای هر خط ۶۴ گره را آدرس دهی می کند که از ۳۲ گره بیشتر نیاز به ریپیتر دارد.
- بوسیله bridge ۵ سطح را ساپورت می کند.
- قابلیت peer-to-peer



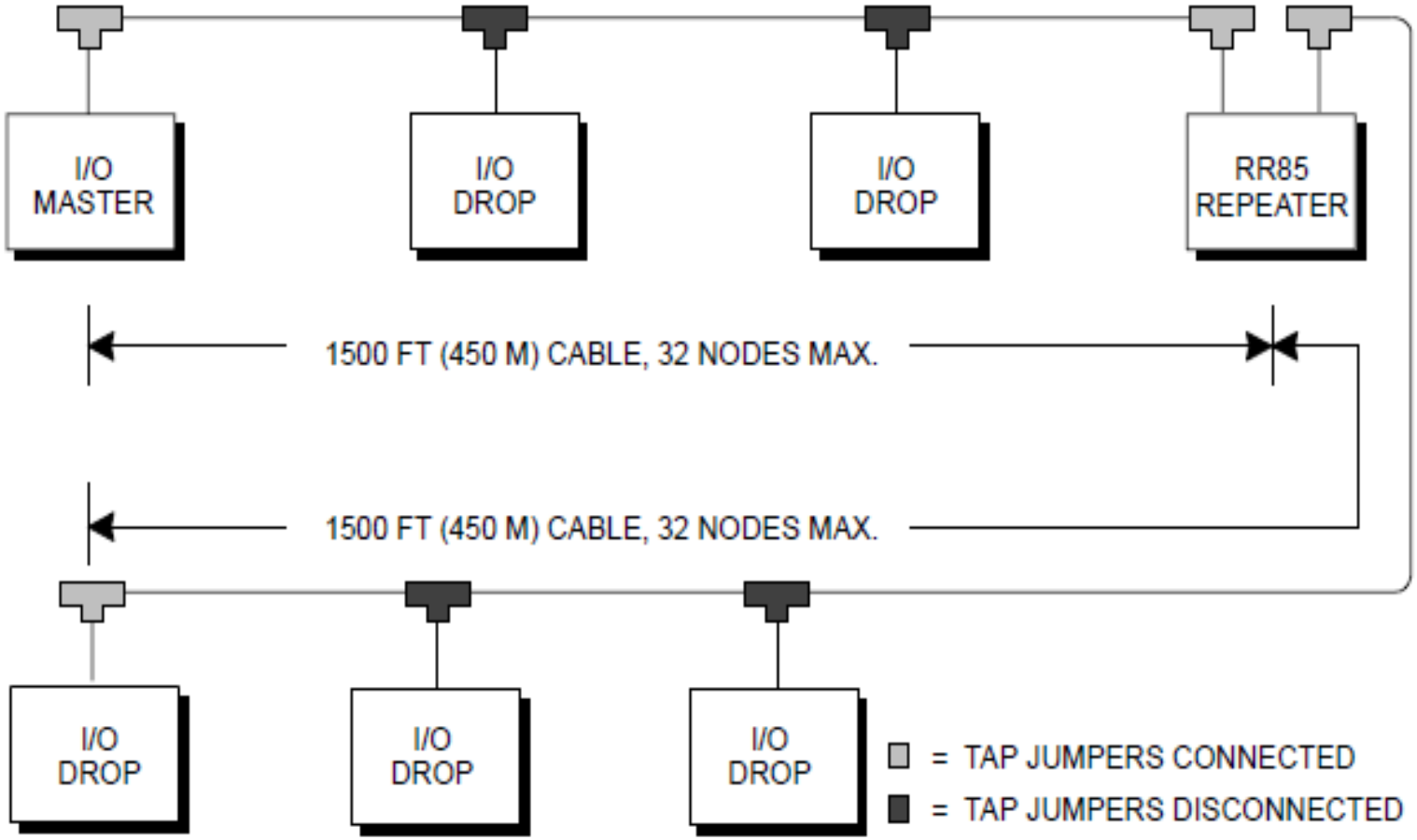
کابل کشی

کابل اصلی (Trunk Cable)

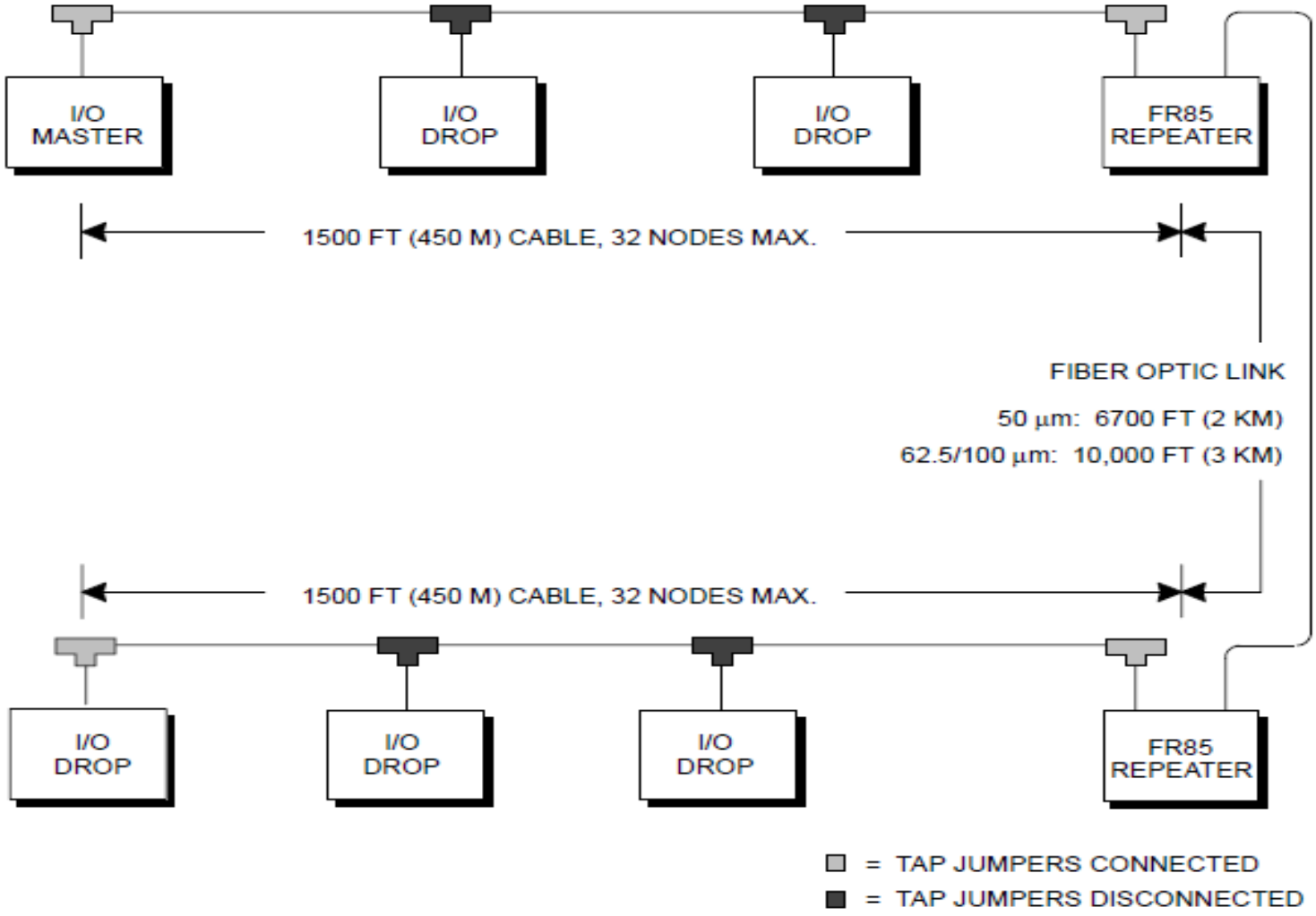
- کابل Trunkدر یک شبکه که از یک کابل دو سیمه (Twisted-Pair) با شیلد که بر روی یک مسیر مستقیم بین نودهای متوالی اجرا می شود این شبکه شامل یک یا چند بخش هست که هر بخش تا ۳۲ نود را پشتیبانی می کند که ماکزیمم طول کابل آن ۴۵۰ متر است.



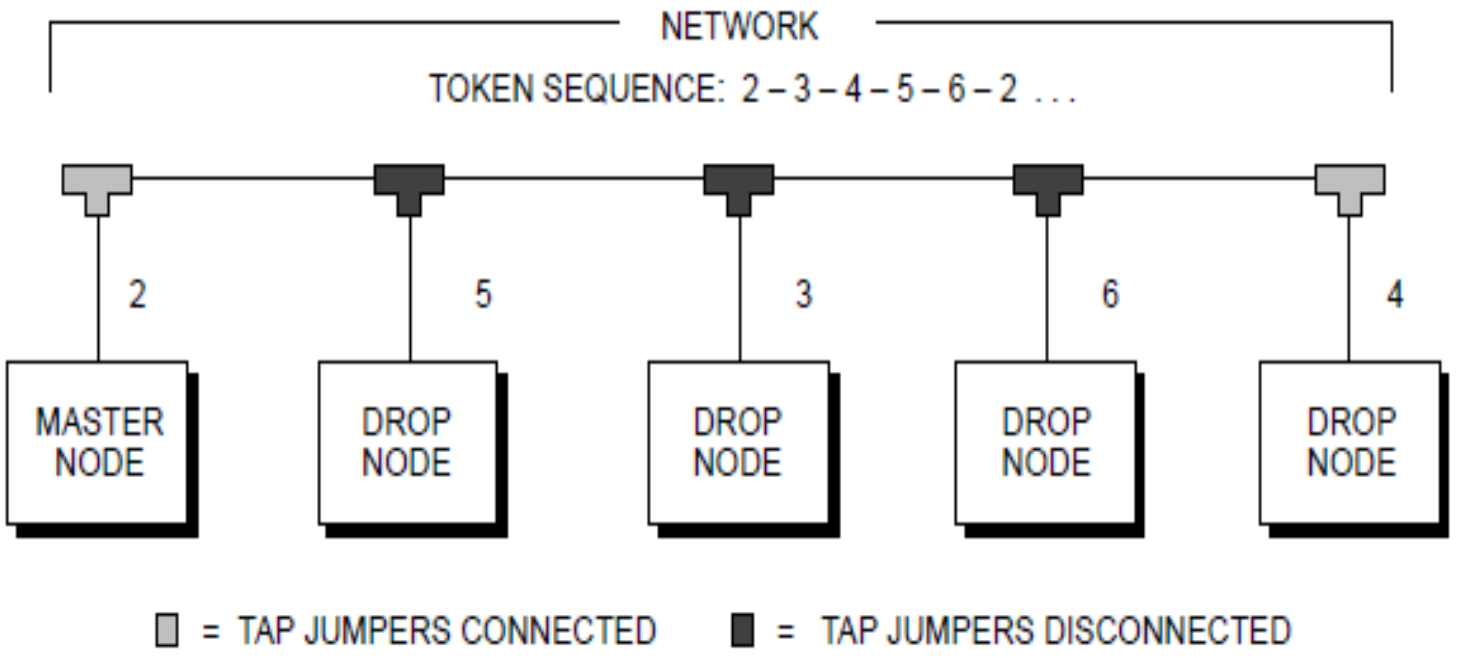
ریپیتر


I/O MASTER
I/O DROP
I/O DROP
RR85 REPEATER
1500 FT (450 M) CABLE, 32 NODES MAX.
1500 FT (450 M) CABLE, 32 NODES MAX.
I/O DROP
I/O DROP
I/O DROP
= TAP JUMPERS CONNECTED
= TAP JUMPERS DISCONNECTED

فیبر نوری


I/O MASTER
I/O DROP
I/O DROP
FR85 REPEATER
1500 FT (450 M) CABLE, 32 NODES MAX.
FIBER OPTIC LINK
50 µm: 6700 FT (2 KM)
62.5/100 µm: 10,000 FT (3 KM)
1500 FT (450 M) CABLE, 32 NODES MAX.
I/O DROP
I/O DROP
I/O DROP
FR85 REPEATER
= TAP JUMPERS CONNECTED
= TAP JUMPERS DISCONNECTED

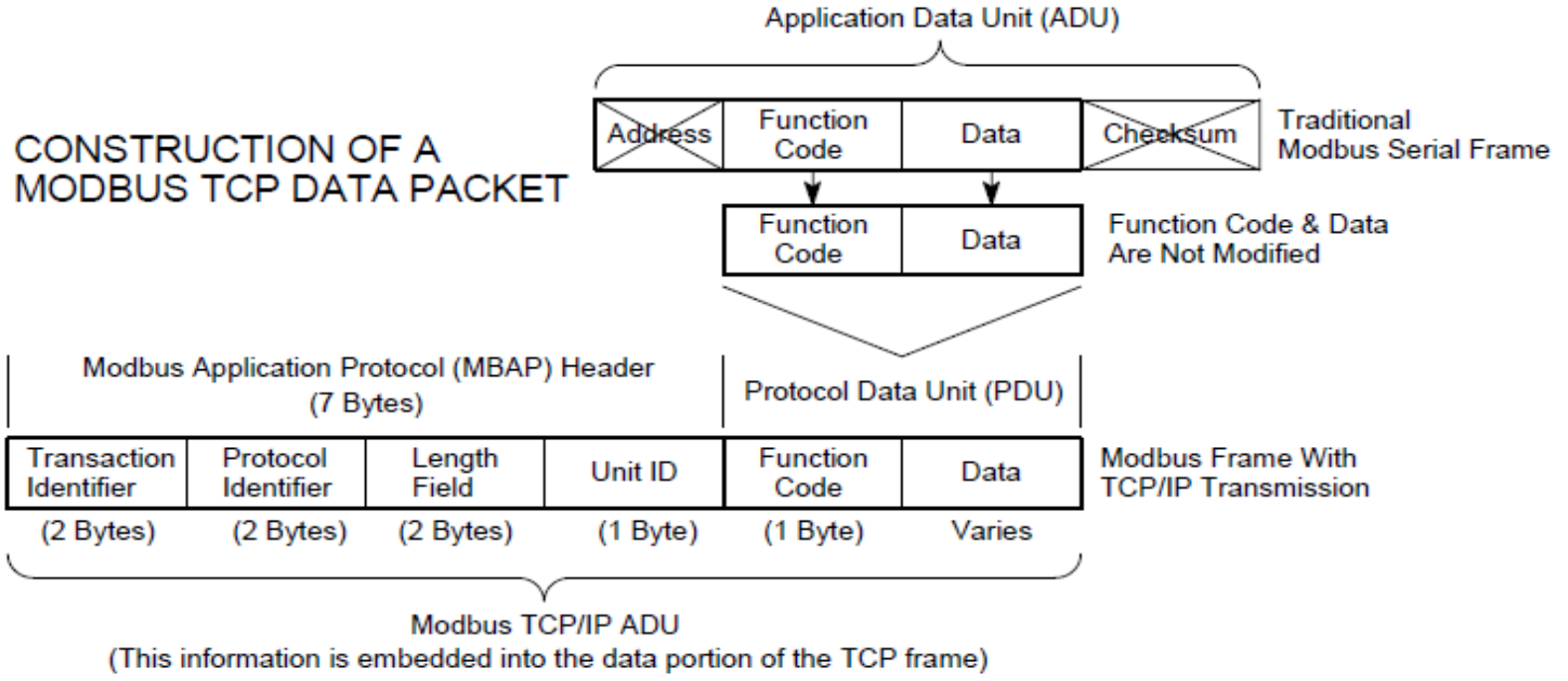
استفاده از Token passing در زیر لایه MAC



MODBUS TCP/IP

MODBUS TCP/IP چیست؟

- MODBUS TCP/IP به سادگی پروتکل MODBUS RTU است که با یک واسط TCP که بر روی اترنت اجرا می شود. ساختار انتقال پیام MODBUS که یک پروتکل برنامه کاربردی است با قوانینی برای سازمان دادن داده ها قطع نظر از ارسال داده در محیط معیین می شود.
- عملا MODBUS TCP/IP فرو می برد یک فریم استاندارد MODBUS را داخل یک فریم TCP بدون فریم چکسام و فریم آدرس



چرا MODBUS با اترنت ترکیب شده است؟

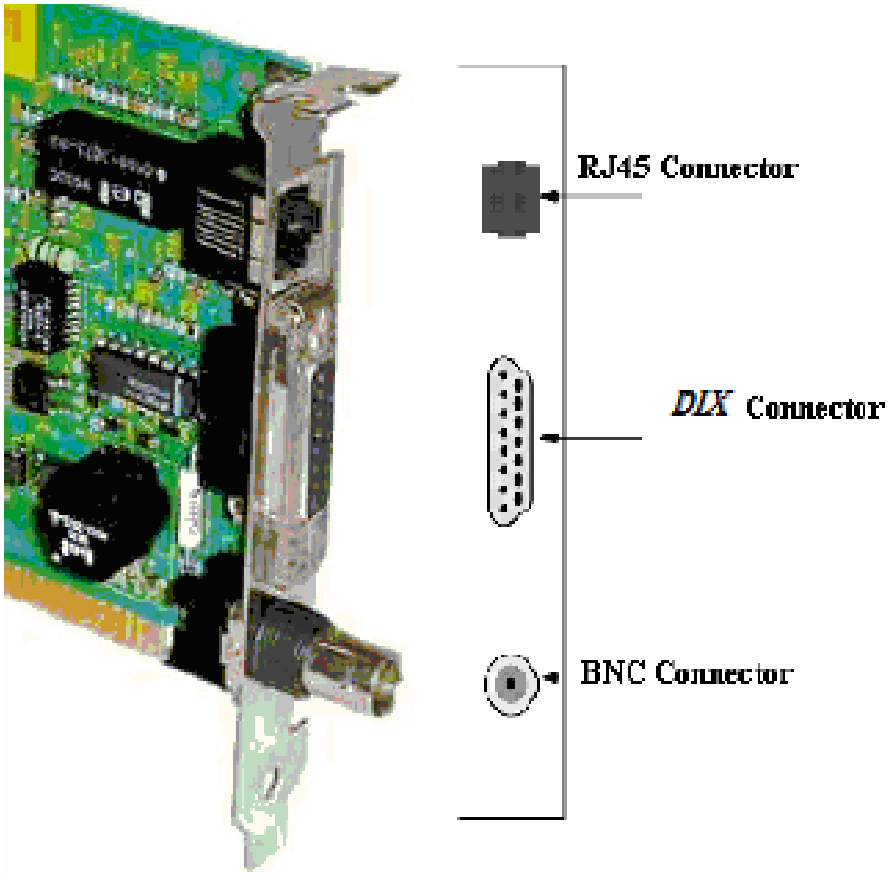
- IEEE 802.3 به عنوان استاندارد اترنت یاد می شود و یک پروتکل و روش جاری برای شبکه بندی است. که در جهان مورد پذیرش قرار دارد. فقط MODBUS به وسیله اترنت به طور آزاد و نامحدود در دسترس است و بسیاری از کارخانه های سازنده تجهیزات صنعتی از آن حمایت می کنند. همچنین فهمیدن آن آسان است و یک نامزد برای بنا کردن ارتباطات صنعتی استاندارد است.

- MODBUS TCP/IP از لایه فیزیکی و دیتا لینک مبنی بر اترنت سهم می برد و از دنباله TCP/IP و پروتکل هایش به طور یکسان استفاده می کند و کاملا با زیر بنای اترنت در نصب کابل ها، کانکتورها، واسط های شبکه، هاب ها و سوئیچ ها سازگار است.

کابل کشی اترنت و اجزاء آن

اترنت از سه رسانه انتقال مختلف استفاده می کند

- 10 Base5
- 10 Base 2
- 10Base T

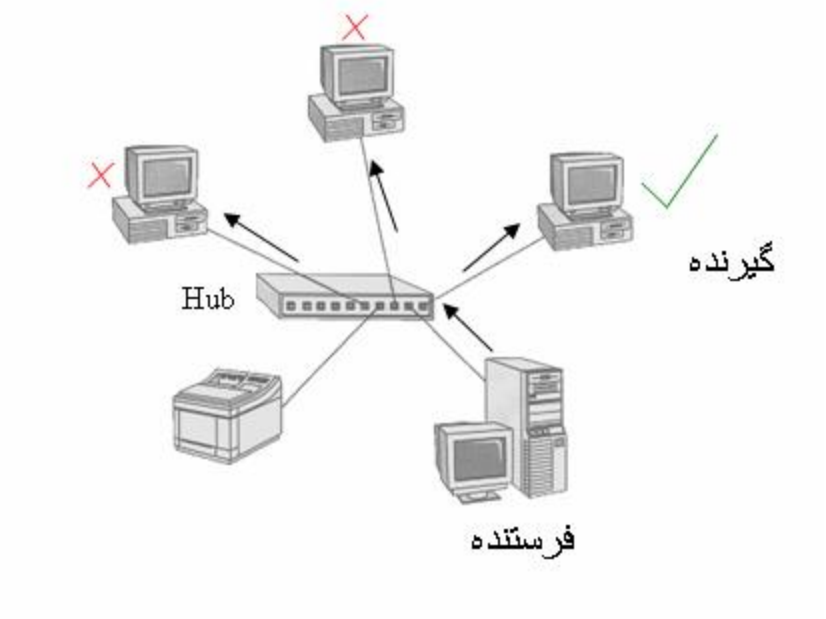


تجهیزات شبکه MODBUS TCP

- HUB های صنعتی
- پل ها
- Getaway
- مسیر یاب ها
- کارت شبکه

HUB

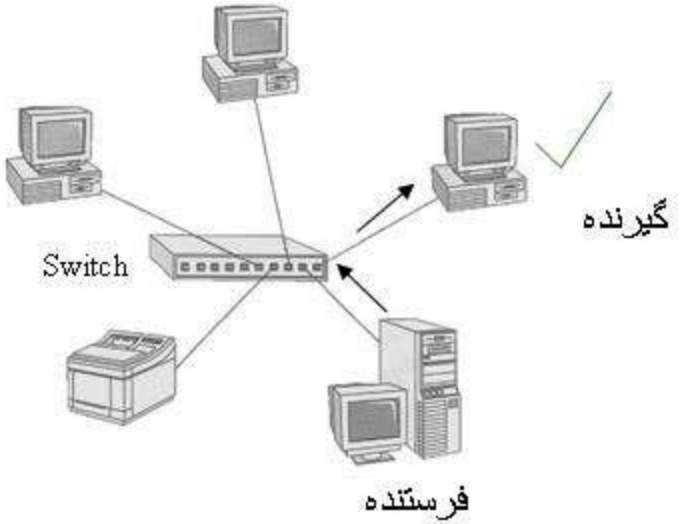




سویچ

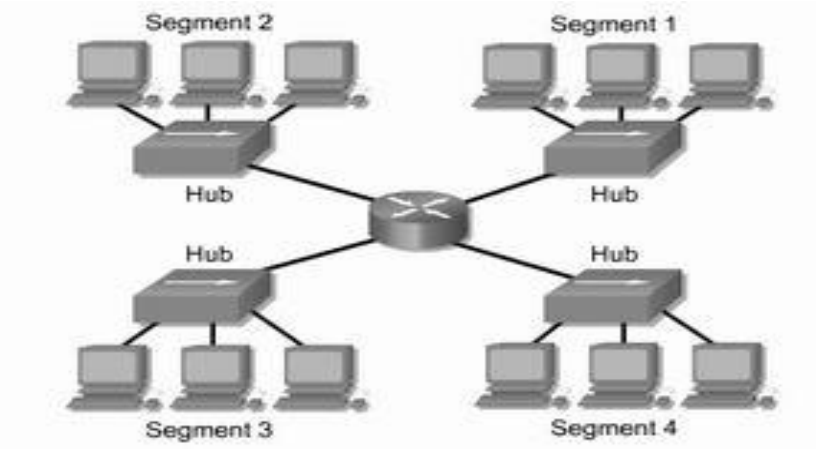




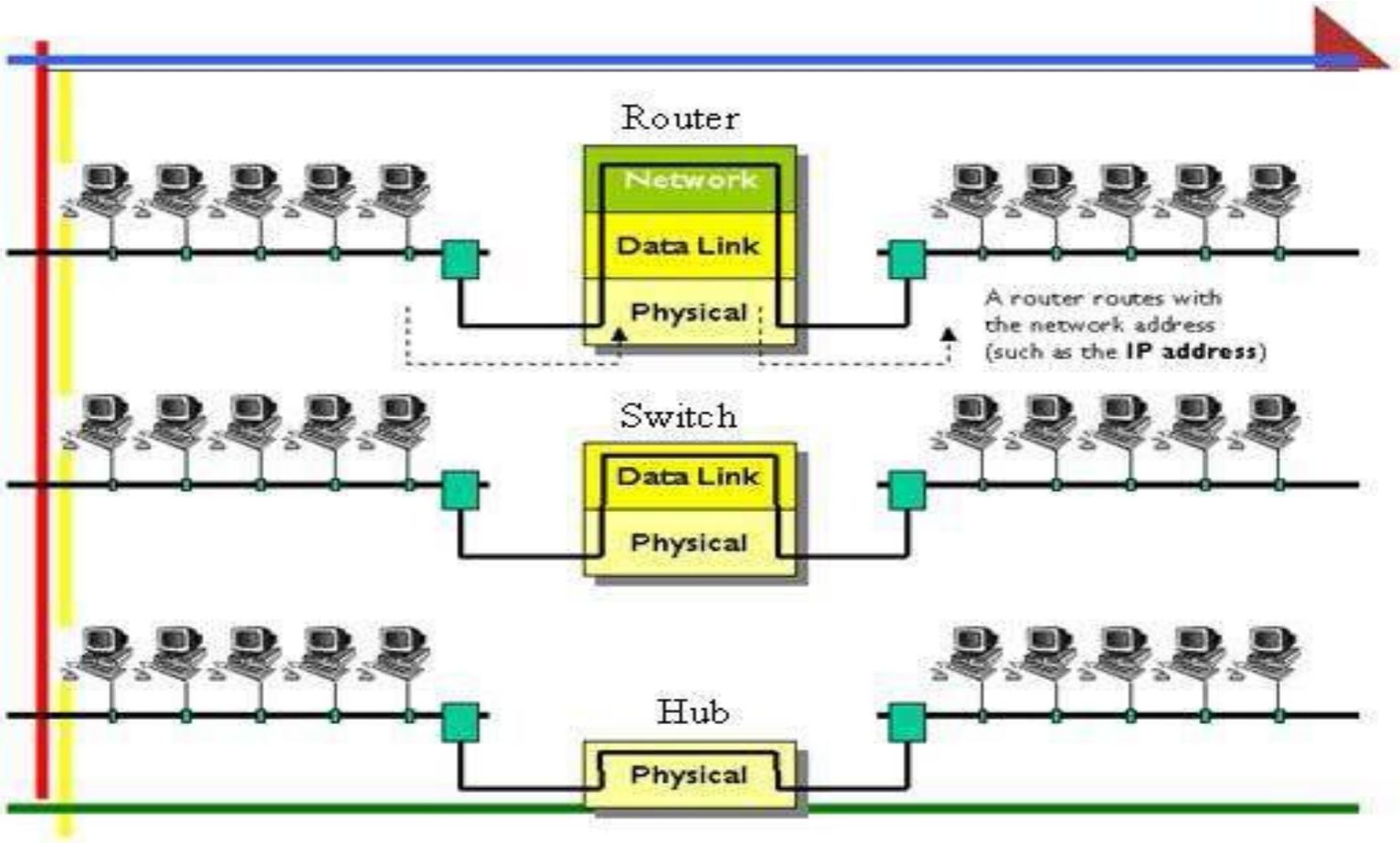


روتر (مسیر یاب)

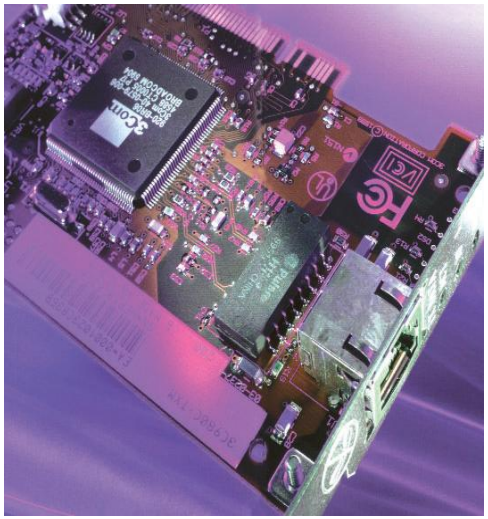




تفاوت بین تجهیزات شبکه



کارت شبکه

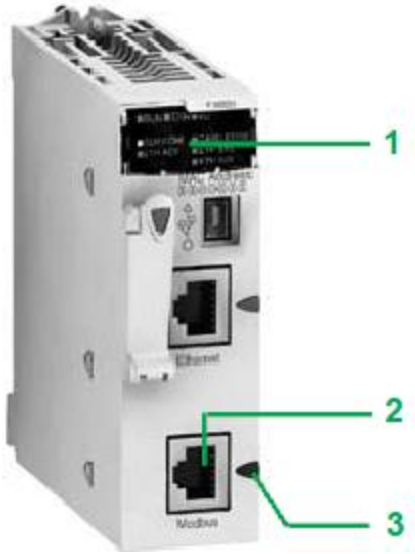




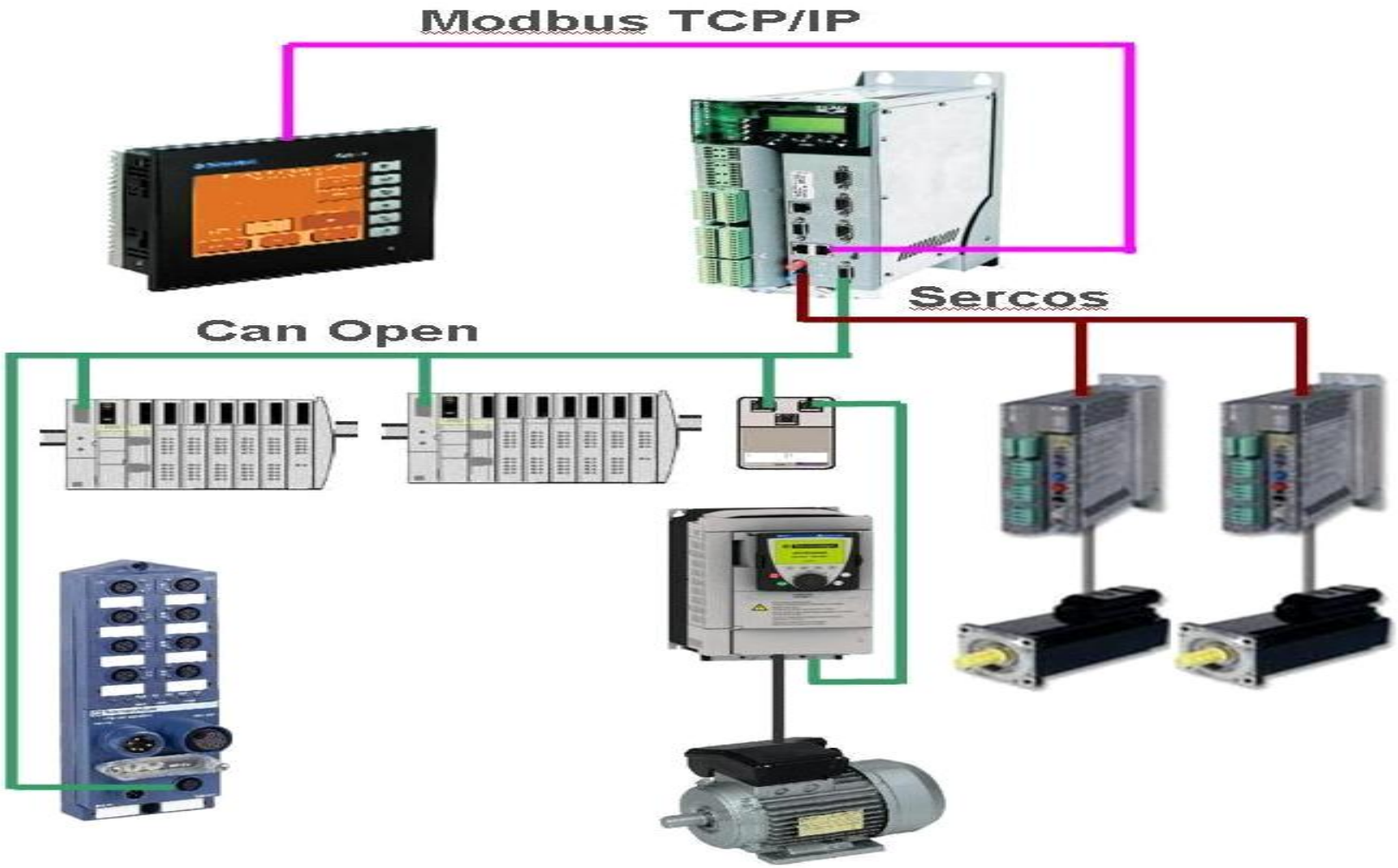
۱-کارت شبکه که در PC نصب می شود.

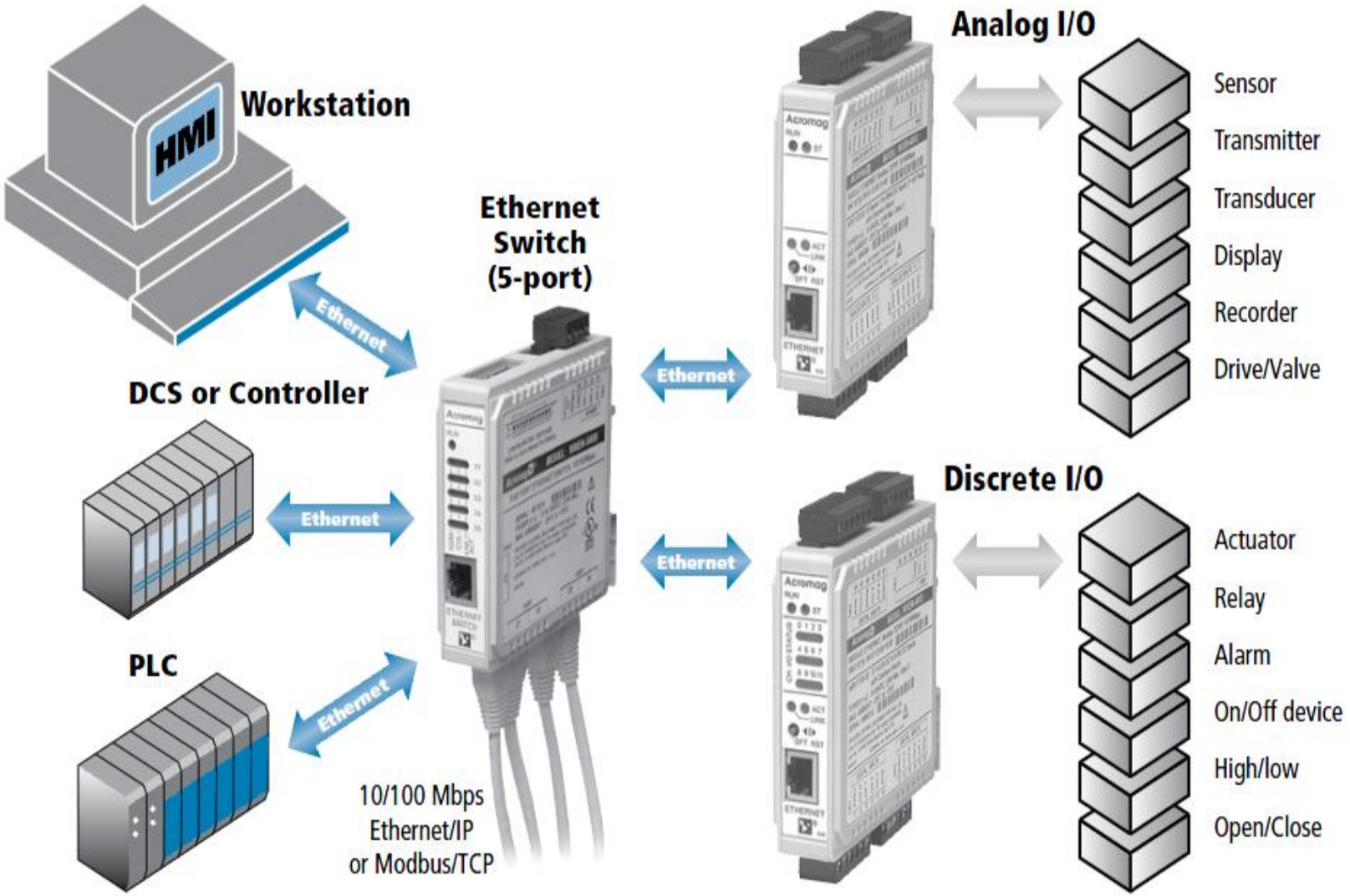
۲- کارت شبکه که بر روی PLC نصب می شود.

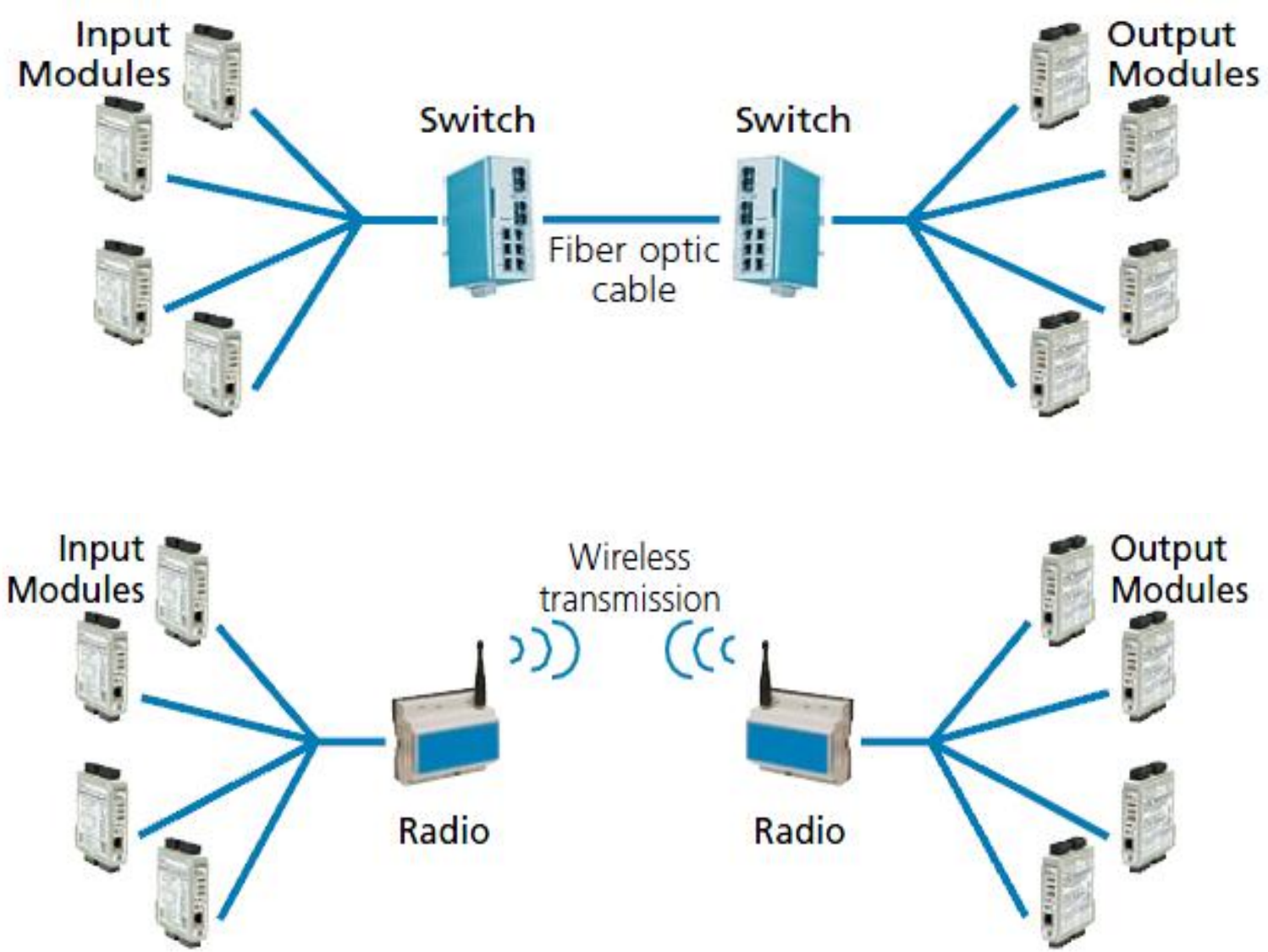




چند مثال




Workstation
HMI
Ethernet
Ethernet Switch (5-port)
DCS or Controller
Ethernet
Ethernet
PLC
Ethernet
10/100 Mbps
Ethernet/IP
or Modbus/TCP
Ethernet
Ethernet
Analog I/O
Sensor
Transmitter
Transducer
Display
Recorder
Drive/Valve
Discrete I/O
Actuator
Relay
Alarm
On/Off device
High/low
Open/Close

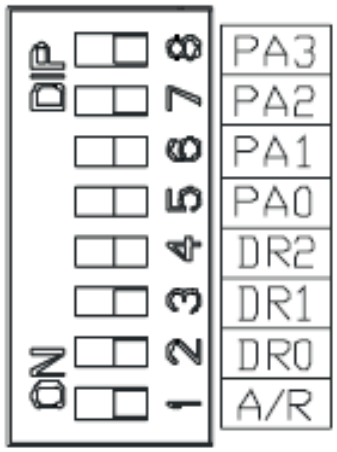

Input Modules
Switch
Switch
Output Modules
Fiber optic cable
Input Modules
Wireless transmission
Output Modules
Radio
Radio

پیکربندی شبکه

- پیکربندی شبکه
  - پیکربندی نرم افزاری
    - پیکربندی نرم افزاری تجهیزات شبکه
      - توسط نرم افزار
        - ✓تعیین آدرس
        - ✓سرعت انتقال
        - ✓مد انتقال
        - ✓انتخاب بیت پریتی
        - ✓....
      - توسط دیپ سوئیچ
    - برنامه نویسی شبکه
  - پیکربندی سخت افزاری
    - تجهیزات شبکه
      - MODBUS RTU/ASCII
        - واسط شبکه
        - ریپیترها
        - مبدل RS 232 به RS 485
      - MODBUS TCP/IP
        - کارت شبکه
        - Switch
        - HUB
    - کابل کشی

دیپ سوئیچ

- با این وسیله آدرس دهی و تنظیمات شبکه را انجام می دهیم معمولا بر روی Slave نصب شده و با تنظیم کردن آن پیکربندی مربوط به شبکه را انجام می دهیم.



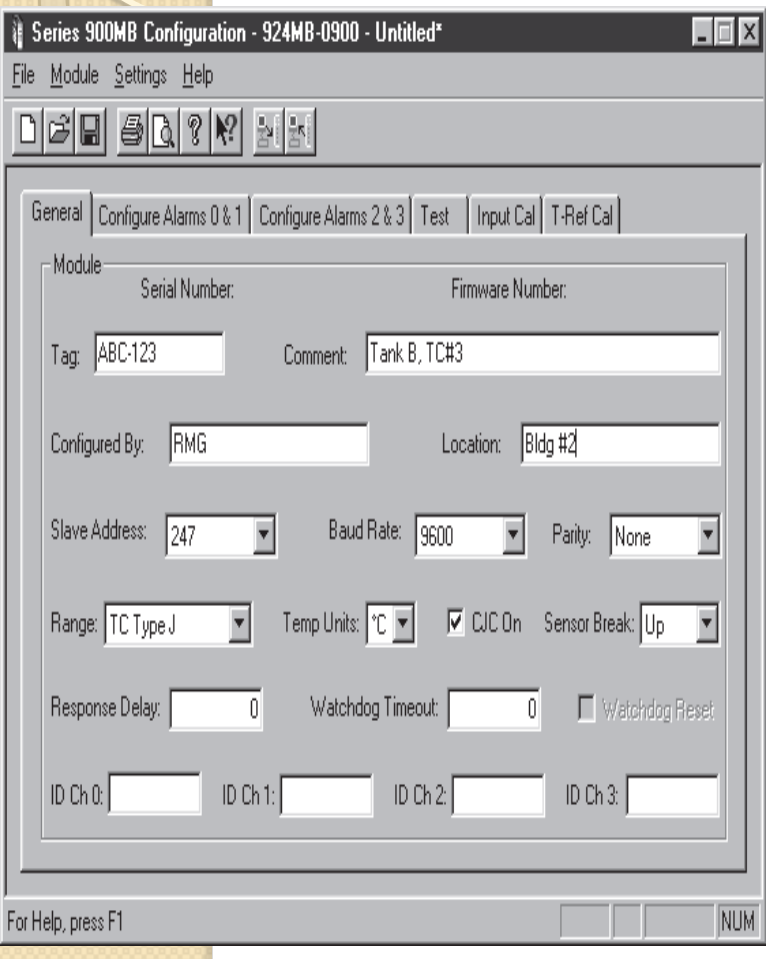
MODBUS

Modbus-RTU I/O Modules



- **Analog Input**
- DC current
- DC voltage
- DC millivolts
- RTD/resistance
- AC current
- **Analog output**
- DC voltage
- DC current
- Open drain MOSFETs
- **Inputs**
- Active-high inputs, 0 to 35V DC
- Active-low inputs, 0 to 35V DC
- **Outputs**
- Sourcing outputs, 5.5 to 35V DC, 250mA
- Sinking outputs, 0 to 35V DC, up to 1A

Module configuration



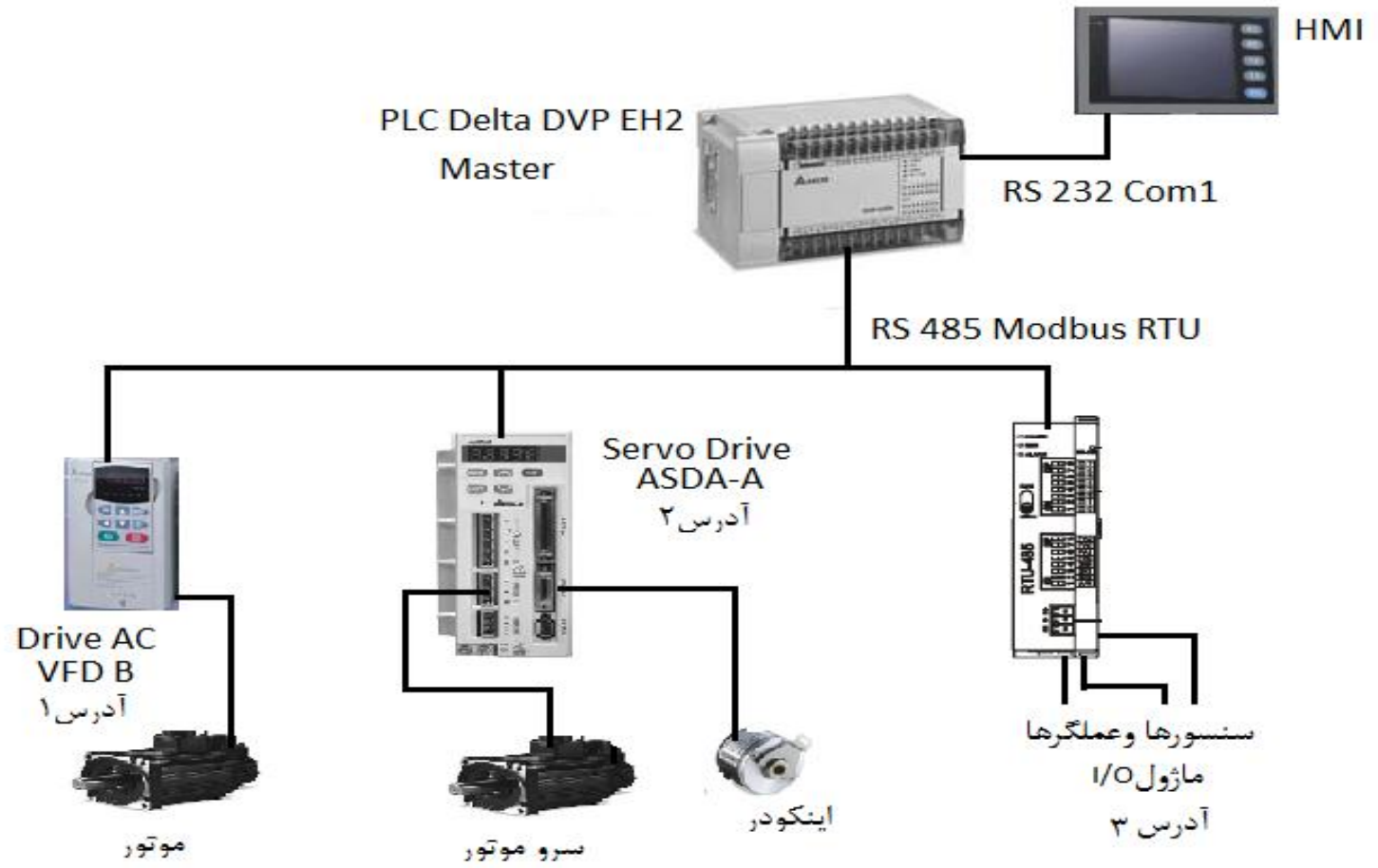
- برای پیکر بندی تنظیمات زیر را انجام می دهیم.
- **Boad rate** که بر اساس طول خط تغییر میکند.
- انتخاب بیت پایان ۱ یا ۱/۵یا ۲
- بیت **Parity** بدون انتخاب یا زوج(**Even**) یا فرد(**Odd**)

  اگر حاصل جمع بیت ها زوج شود(**Even**)

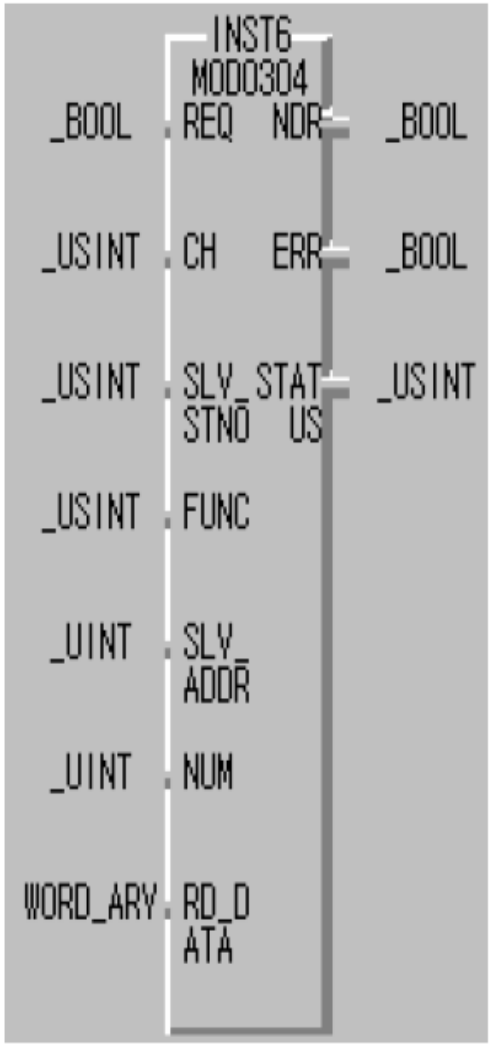
  اگر حاصل جمع بیت ها فرد شود(**Odd**)
- **Watch dog timeout**
- آدرس **Slave**
- انتخاب**ID** کانال های خروجی و رودی

  Id ch.0 ,id ch.1 ,id ch.2 ,id ch.3

مثال: کنترل و مانیتورینگ اطلاعات در MODBUS RTU



برنامه نویسی توسط بلوک های MODBUS

Function block		Description
	**Input**	REQ: Execute function block when it's 1(rising edge) CH : Set communication channel (0 ~ 1) SLV_STNO: Input the number of the slave station FUNC: Input the function code. It supports function code 03 and 04 SLV_ADDR: The address to read from the slave station NUM: The data size to read from the slave station
	Output	RD_DATA: A variable name to save the data that is read (The number of array is to be declared as same as or bigger than data size.). NDR: If it ends without error, output 1 and keep the value till the call for the next function block. ERR: If an error occurs, output 1 and keep the value till the call for the next function block. STATUS: When an error occurs, output an error code.

پایان

جهت دریافت فایل می توان به آدرس زیر مراجعه نمود و اطلاعات کافی را بدست آورید.

www.ecm50.blogfa.com