Giao thức (Protocol)

- Giao thức thiết lập một tiêu chuẩn chung cho việc trao dữ liệu giữa phần thu và phát trên mạng.
- Nó thường kết hợp với gói tin.
- Giao thức điều khiển một khung bản tin chung cho tất cả các thiết bị trên mạng.
- Giao thức thiết lập hoạt động đúng cho hệ thông tin

Giao thức (Protocol)

Các đặc điểm của giao thức:

- Khởi động: Khởi động các thông số của giao thức để bắt đầu truyền số liệu qua kênh liên lạc.
- Tạo khung và đồng bộ khung.
- Điều khiển luồng dữ liệu.
- Điều khiển truy nhập đường truyền.
- Phát hiện và sửa lỗi.
- Kiểm soát Time-out.

Các yêu cầu riêng cho giao thức CN

- Đơn giản nhất có thể để dễ khắc phục sự cố:
  - + CN là nơi có sự hiểu biết về mạng thông tin CN ít.
  - + Đòi hỏi hoạt động liên tục.
  - + Có ý thức lựa chọn giao thức đơn giản nhất có thể.
- Độ đảm bảo dữ liệu truyền cao:
  - + Hoạt động trong môi trường có nhiễu điện lớn.
  - + Các thiết bị công suất lớn tập trung với mật độ cao.
  - + Đòi hỏi không có lỗi khi truyền.
  - + Chọn giao thức có mức độ cao của việc kiểm tra lỗi.

Các yêu cầu riêng cho giao thức CN

- Chuẩn hoá giao thức:

  + Có thể có nhu cầu cho việc kết nối giữa các thiết bị của các nhà SX khác nhau hay các hệ khác nhau.

  + Cần phải chuẩn hoá giao thức.

- Tốc độ cập nhật thông số cao:

  + Không đòi hỏi số lượng thông số lớn.

  + Yêu cầu cập nhật một loạt các setpoint cho một loạt các thiết bị gần như đồng thời.

  + Mộ số giao thức Field Bus mới có thể đáp ứng yêu cầu này.

Modbus

Mô tả chung về Modbus:

+ Modbus được phát triển bởi Modicon (AEG) cho hệ thống điều khiển các quá trình

ModBus

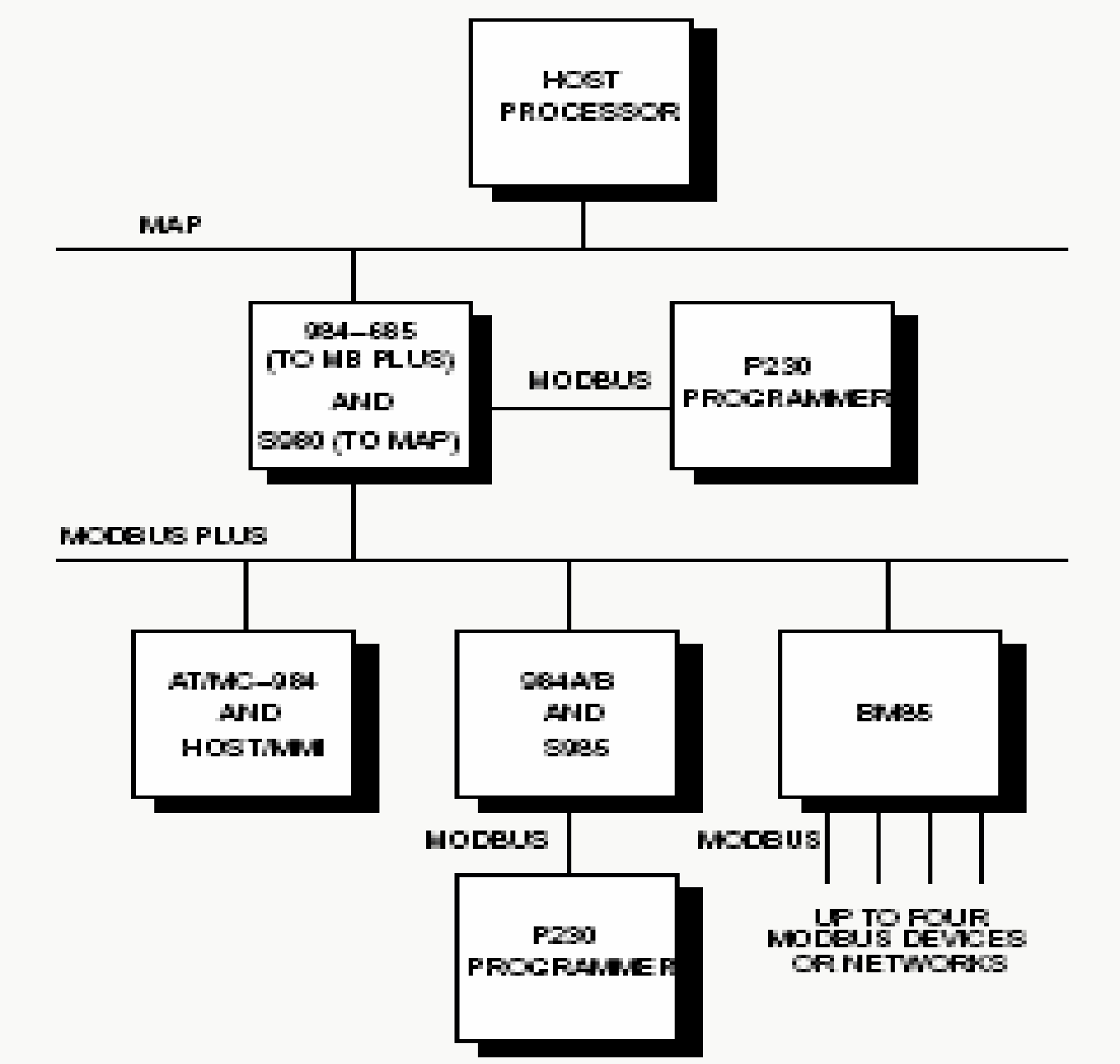


Figure 1 Overview of Modbus Protocol Application

ModBus

+ Modbus chuẩn của bộ điều khiển Modicon sử dụng cổng RS-232. Bộ điều khiển có thể nối mạng trực tiếp hay qua Modem.

+ Người dùng có thể lựa chọn các chuẩn RS-422, RS-485, 20mA Current loop, tất cả các chuẩn trên đều tương thích với tốc độ truyền của giao thức.

+ Thông tin giữa các bộ điều khiển sử dụng kỹ thuật Master-Slave. Chỉ có Master mới có quyền khởi động việc truyền dữ liệu, các thiết bị khác là Slave trả lời bằng cách cung cấp các dữ liệu được yêu cầu từ Master hoặc đáp lại các hoạt động.

+ Master có thể là các máy chủ, PC hay các Panel lập trình.

+ Slave là các bộ điều khiển có tối đa 247 Slave.

ModBus

+ Master có thể địa chỉ từng Slave riêng hay gửi một bản tin quảng bá tới tất cả các Slave.

+ Khi có yêu cầu bởi địa chỉ riêng thì sẽ có bản tin trả lời. Không có bản tin trả lời với yêu cầu quảng bá.

+ Modbus cung cấp một định dạng khung bản tin chung cho các bản tin truyền giữa Master và Slave. Bản tin bao gồm địa chỉ của thiết bị, mã chức năng định nghĩa các hoạt động yêu cầu, số liệu cần gửi và trường kiểm tra lỗi.

+ Slave trả lời bằng một bản tin nó chính là kết quả của hoạt động. Nếu có lỗi thì nó cũng báo lỗi nào đã xảy ra.

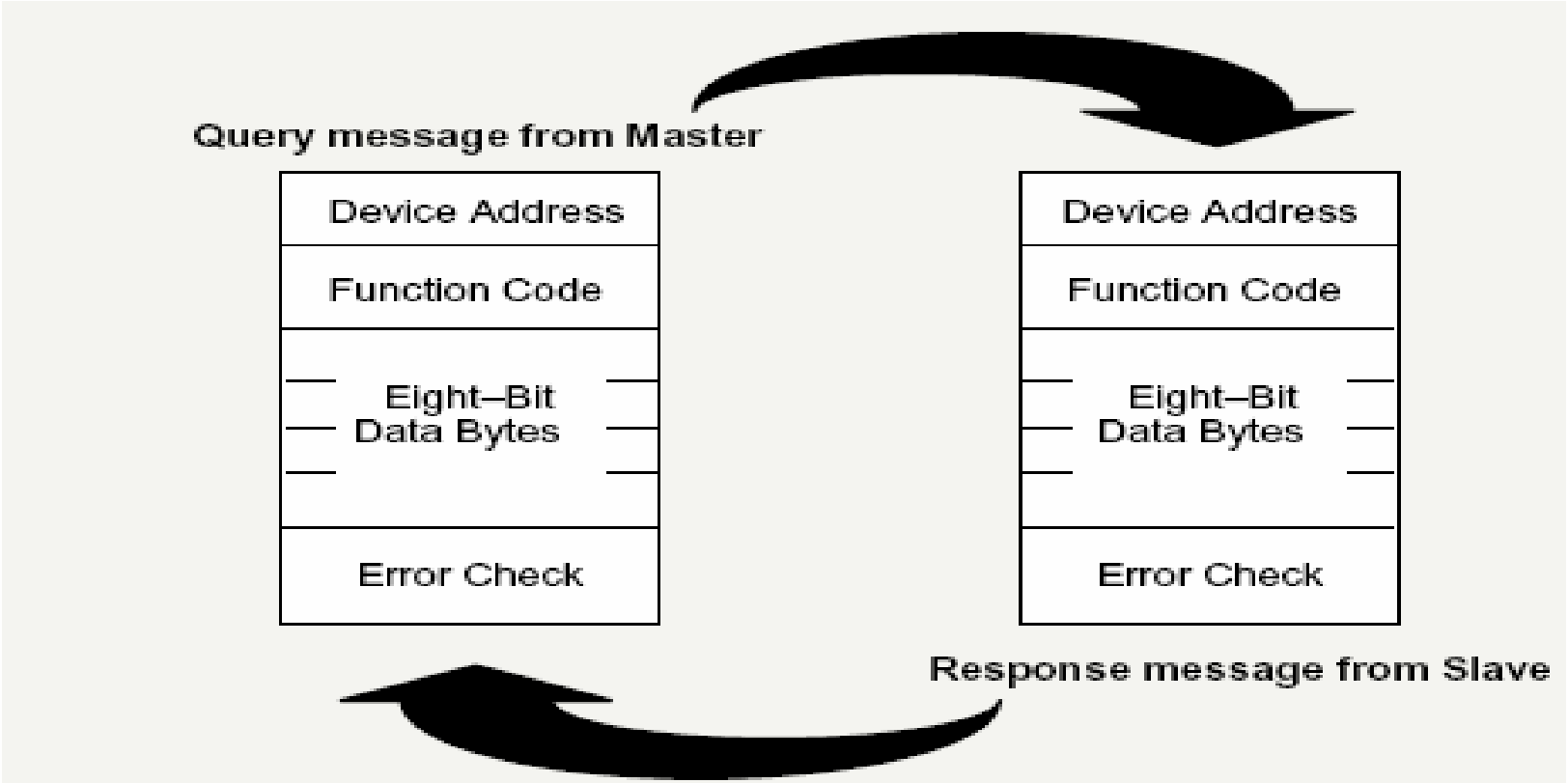
ModBus

+ Ngoài ra các bộ điều khiển Modbus có thể thông tin trên Modbus Plus sử dụng cổng thông tin có sẵn hay cộng mạng và truyền trên MAP.

+ ở đay thông tin giữa các bộ điều khiển dùng kỹ thuật Pear-Pear.(ứng dụng vẫn là Master-Slave).

ModBus

The Query–Response Cycle



ModBus - Hai chế độ truyền

+ Bộ điều khiển trên mạng Modbus có thể truyền ở hai chế độ: ASCII và RTU.

+ Ta có thể chọn chế độ truyền cũng như các thông số của cổng thông tin nhưng nó phải như nhau ở tất cả các bộ điều khiển.

ModBus - ASCII Mode

+ Khi các bộ điều khiển sử dụng chế độ ASCII mỗi một byte-8bits truyền như là 2 ký tự ASCII.

+ Ưu điểm chính là cho thời gian truyền giữa các ký tự lên đến 1s mà không gây ra lỗi

+ Mã: Hexadecimal, ASCII 0-9,A-F. 1 Hexa ->ASCII

+ Bit trên ký tự: 1 Start bit; 7 data bit; 1,0 Parity bit; 1,2 Stop bit (10 bit).

+ Kiểm tra lỗi: LRC

ModBus - RTU Mode

+ Khi các bộ điều khiển hoạt động ở chế đọ RTU mỗi một Byte-8bit gửi như là hai số Hexadecimal -4 bit.

+ Ưu điểm của phương pháp này là có mật độ ký tự lớn cho phép truyền tốt hơn chế độ ASCII với cùng một tốc độ bit.

+ Mỗi một bản tin cần phải truyền thành một chuỗi liên tục.

+ Mã: 8 bit, Hexa 0-9,A-F. Hai số Hexa chứa trong một trường 8 bit.

+ Số bit trên Byte: 1 Start bit; 8 data bit; 1,0 Parity bit; 1,2 Stop bit (11 bit).

+ Kiểm tra lỗi: CRC

ModBus – Cấu trúc khung bản tin

+ Trong cả hai chế độ truyền bản tin Modbus được bên phát đặt trong một khung có điểm bắt đầu, kết thúc.

+ Bên thu nhận bản tin định vị các trường khác và phát hiện ra lỗi có trong bản tin.

+ Có hai chế độ truyền có hai kiểu khung bản tin

ModBus - ASCII Frame

START	ADDRESS	FUNCTION	DATA	LRC CHECK	END
1 CHAR :	2 CHARS	2 CHARS	*n* CHARS	2 CHARS	2 CHARS CRLF

ModBus - ASCII Frame

+ Tất cả các thiết bị nối vào mạng sẽ kiểm tra bus liên tục cho đến khi nhận được ký tự ':' . Nó sẽ giải mã trường địa chỉ. Nếu gửi cho nó thì nó nhận và xử lý các trường tiết theo.

+ Thời gian cho phép giữa các ký tự có thể lên đến 1 s-> không gây ra lỗi.

ModBus - RTU Frame

START	ADDRESS	FUNCTION	DATA	CRC CHECK	END
T1-T2-T3-T4	8 BITS	8 BITS	*n* x 8 BITS	16 BITS	T1-T2-T3-T4

ModBus - RTU Frame

+ Các thiết bị nối vào mạng sẽ kiểm tra bus trong suốt quá trình rỗi của bus. Trường đầu tiên nhận được sẽ là trường địa chỉ và nó sẽ so sánh với địa chỉ của nó.

+ Nếu thời gian nghỉ > 3.5 lần thười gian truyền 1 byte thì kết thúc bản tin.

ModBus – Cấu trúc khung bản tin

Trường địa chỉ:

+ Chứa 2 ký tự ASCII hay 8 bit.

+ Giá trị từ 0-247.

+ Từng Slave địa chỉ hoá từ 1-247.

+ Master địa chỉ hoá Slave bằng cách đặt địa chỉ của nó vào trường địa chỉ.

+ Slave trả lời báo cho Master biết Slave nào đã trả lời.

+ Địa chỉ 0 sử dụng ở chế độ quảng bá.

ModBus – Cấu trúc khung bản tin

Trường chức năng:

+ Bao gồm 2 ký tự ASCII hay 1 byte.

+ Giá trị từ 1-255.

+ Một vài mã áp dụng cho các bộ điều khiển. Một vài mã chỉ áp dụng cho một mô hình nào đó. Một số dành cho tương lai.

+ Master->Slave chỉ ra Slave phải làm gì?

+ Slave->Master báo là hoạt động bình thường hay báo lỗi. Nếu bình thường thì phản hồi về mã chức năng ban đầu. Nếu có lỗi thì phản hồi về mã chức năng ban đầu với bít cao nhất bằng 1.

ModBus – Cấu trúc khung bản tin

Trường dữ liệu:

- Master->Slave các dữ liệu cần cho hoạt động được định nghĩa bởi mã chức năng.

- Slave->Master nếu không có lỗi nó chức các dữ liệu trả về. Nếu có lỗi nó chứa mã lỗi.

- Trường dữ liệu có thể không có trong một số bản tin.

ModBus – Cấu trúc khung bản tin

Kiểm tra lỗi:

+ ASCII mode: kết quả kiểm tra theo LRC -> 1byte -> 2 ký tự ASCII.

+ RTU mode: kiểm tra theo PP CRC nội dung bản tin. 16 bit -> 2 byte

ModBus – Cấu trúc khung bản tin

- Khi truyền ở chế độ Modbus chuẩn các ký tự hay các byte được truyền các bít thấp trước, cao sau.

With ASCII character framing, the bit sequence is:

With Parity Checking

Start	1	2	3	4	5	6	7	Par	Stop

Without Parity Checking

Start	1	2	3	4	5	6	7	Stop	Stop

ModBus – Cấu trúc khung bản tin

With RTU character framing, the bit sequence is:

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

ModBus – Các phương pháp kiểm tra lỗi

- Modbus chuẩn được áp dụng hai phương pháp kiểm tra lỗi. Kiểm tra chẵn lẻ áp dụng cho từng ký tự. Kiểm tra khung (LRC, CRC) được áp dụng cho toàn bộ khung bản tin.
- Cả hai phương pháp này sẽ được Master thực hiện trước khi truyền khung bản tin và được Slave kiểm tra trong quá trình nhận bản tin.
- Nếu Slave phát hiện ra lỗi trong bản tin thì bản tin sẽ bị bỏ đi, không có đáp ứng cho Master. Master đợi quá thời gian Time-out để bỏ quá trình truyền. Thời gian Time-out đủ lớn để cho bất kỳ Slave nào có thể trả lời bình thường được. Như vậy khi Time-out chương trình ứng dụng trên Master biết có một lỗi xảy ra.

ModBus – Các phương pháp kiểm tra lỗi

Kiểm tra chẵn lẻ:

- Ta có thể đặt là kiểm tra chẵn, kiểm tra lẻ hay không kiểm tra chẵn lẻ.

- Khi truyền các bit chẵn lẻ sẽ được tính toán và truyền cùng với ký tự. Bên thu sẽ kiểm tra lại. Tất cả các thiết bị phải dùng chung một phương pháp.

ModBus - Các phương pháp kiểm tra lỗi

Kiểm tra LRC:

Kiểm tra CRC:

ModBus -Các chức năng của Modbus

Modbus cung cấp một loạt các chức năng sau:

Code	Name	384	484	584	884	M84	984
01	Read Coil Status	Y	Y	Y	Y	Y	Y
02	Read Input Status	Y	Y	Y	Y	Y	Y
03	Read Holding Registers	Y	Y	Y	Y	Y	Y
04	Read Input Registers	Y	Y	Y	Y	Y	Y
05	Force Single Coil	Y	Y	Y	Y	Y	Y
06	Preset Single Register	Y	Y	Y	Y	Y	Y
07	Read Exception Status	Y	Y	Y	Y	Y	Y
08	Diagnostics (see Chapter 3)						

ModBus -Các chức năng của Modbus

09	Program 484	N	Y	N	N	N	N
10	Poll 484	N	Y	N	N	N	N
11	Fetch Comm. Event Ctr.	Y	N	Y	N	N	Y
12	Fetch Comm. Event Log	Y	N	Y	N	N	Y
13	Program Controller	Y	N	Y	N	N	Y
14	Poll Controller	Y	N	Y	N	N	Y
15	Force Multiple Coils	Y	Y	Y	Y	Y	Y
16	Preset Multiple Registers	Y	Y	Y	Y	Y	Y
17	Report Slave ID	Y	Y	Y	Y	Y	Y
18	Program 884/M84	N	N	N	Y	Y	N
19	Reset Comm. Link	N	N	N	Y	Y	N
20	Read General Reference	N	N	Y	N	N	Y
21	Write General Reference	N	N	Y	N	N	Y

ModBus -Các chức năng của Modbus

Code	Name	384	484	584	884	M84	984
22	Mask Write 4X Register	N	N	N	N	N	(1)
23	Read/Write 4X Registers	N	N	N	N	N	(1)
24	Read FIFO Queue	N	N	N	N	N	(1)

ModBus -Các chức năng của Modbus

QUERY			
Field Name	Example (Hex)	ASCII Characters	RTU 8–Bit Field
Header		: (colon)	None
Slave Address	06	0 6	0000 0110
Function	03	0 3	0000 0011
Starting Address Hi	00	0 0	0000 0000
Starting Address Lo	6B	6 B	0110 1011
No. of Registers Hi	00	0 0	0000 0000
No. of Registers Lo	03	0 3	0000 0011
Error Check		LRC (2 chars.)	CRC (16 bits)
Trailer		CR LF	None
	Total Bytes:	17	8

ModBus -Các chức năng của Modbus

RESPONSE

Field Name	Example (Hex)	ASCII Characters	RTU 8–Bit Field
Header		: (colon)	None
Slave Address	06	0 6	0000 0110
Function	03	0 3	0000 0011
Byte Count	06	0 6	0000 0110
Data Hi	02	0 2	0000 0010
Data Lo	2B	2 B	0010 1011
Data Hi	00	0 0	0000 0000
Data Lo	00	0 0	0000 0000
Data Hi	00	0 0	0000 0000
Data Lo	63	6 3	0110 0011
Error Check		LRC (2 chars.)	CRC (16 bits)
Trailer		CR LF	None
	Total Bytes:	23	11

ModBus -Các kiểu dữ liệu của Modbus

- Modbus sử dụng 4 kiểu dữ liệu khác nhau:
    + Đầu vào số.
    + Đầu ra số (Coil).
    + Thanh ghi vào (Input Register).
    + Thanh ghi giữ (Holding Register)
- Các biến đầu vào và ra sô là 1 bit.
- Các biến thanh ghi là 2 byte.
- Mỗi một chức năng gắn liền với một kiểu dữ liệu.
- Địa chỉ mà khung bản tin sử dụng là địa chỉ offset tương đối với địa chỉ thấp nhất của kiểu dữ liệu.

ModBus -Mô tả chi tiết các mã chức năng

QUERY

Field Name	Example (Hex)
Slave Address	11
Function	01
Starting Address Hi	00
Starting Address Lo	13
No. of Points Hi	00
No. of Points Lo	25
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

RESPONSE

Field Name	Example (Hex)
Slave Address	11
Function	01
Byte Count	05
Data (Coils 27–20)	CD
Data (Coils 35–28)	6B
Data (Coils 43–36)	B2
Data (Coils 51–44)	0E
Data (Coils 56–52)	1B
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

QUERY

Field Name	Example (Hex)
Slave Address	11
Function	02
Starting Address Hi	00
Starting Address Lo	C4
No. of Points Hi	00
No. of Points Lo	16
Error Check (LRC or CRC)	--

ModBus -Mô tả chi tiết các mã chức năng

RESPONSE

Field Name	Example (Hex)
Slave Address	11
Function	02
Byte Count	03
Data (Inputs 10204–10197)	AC
Data (Inputs 10212–10205)	DB
Data (Inputs 10218–10213)	35
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

QUERY

Field Name	Example (Hex)
Slave Address	11
Function	05
Coil Address Hi	00
Coil Address Lo	AC
Force Data Hi	FF
Force Data Lo	00
Error Check (LRC or CRC)	—

ModBus -Mô tả chi tiết các mã chức năng

RESPONSE

Field Name	Example (Hex)
Slave Address	11
Function	05
Coil Address Hi	00
Coil Address Lo	AC
Force Data Hi	FF
Force Data Lo	00
Error Check (LRC or CRC)	—

ModBus -Function 08 Diagnostics

QUERY

Field Name	Example (Hex)
Slave Address	11
Function	08
Subfunction Hi	00
Subfunction Lo	00
Data Hi	A5
Data Lo	37
Error Check (LRC or CRC)	—

ModBus -Function 08 Diagnostics

RESPONSE

Field Name	Example (Hex)
Slave Address	11
Function	08
Subfunction Hi	00
Subfunction Lo	00
Data Hi	A5
Data Lo	37
Error Check (LRC or CRC)	—

ModBus -Function 08 Diagnostics

Code	Name	384	484	584	884	M84	984
00	Return Query Data	Y	Y	Y	Y	Y	Y
01	Restart Comm Option	Y	Y	Y	Y	Y	Y
02	Return Diagnostic Register	Y	Y	Y	Y	Y	Y
03	Change ASCII Input Delimiter	Y	Y	Y	N	N	Y
04	Force Listen Only Mode	Y	Y	Y	Y	Y	Y
05–09	Reserved						
10	Clear Ctrs and Diagnostic Reg.	Y	Y	(1)	N	N	(1)
11	Return Bus Message Count	Y	Y	Y	N	N	Y
12	Return Bus Comm. Error Count	Y	Y	Y	N	N	Y

ModBus -Function 08 Diagnostics

13	Return Bus Exception Error Cnt	Y	Y	Y	N	N	Y
14	Return Slave Message Count	Y	Y	Y	N	N	N
15	Return Slave No Response Cnt	Y	Y	Y	N	N	N
16	Return Slave NAK Count	Y	Y	Y	N	N	Y
17	Return Slave Busy Count	Y	Y	Y	N	N	Y
18	Return Bus Char. Overrun Cnt	Y	Y	Y	N	N	Y
19	Return Overrun Error Count	N	N	N	Y	N	N
20	Clear Overrun Counter and Flag	N	N	N	Y	N	N
21	Get/Clear Modbus Plus Statistics	N	N	N	N	N	Y
22–up	Reserved						

ModBus -Trả lời báo lỗi

Ngoại trừ bản tin quảng bá. Khi Master gửi một bản tin tới hỏi Slave thì có 4 trường hợp có thể xảy ra:

+ Slave nhận bản tin không có lỗi và có thể trả lời bản tin. Trả lời thường.

+ Nếu Slave không nhận được bản tin hỏi vì lỗi thông tin, sẽ không có bản tin trả lời.Master sử lý sự kiện Time-out.

+ Nếu Slave nhận được bản tin hỏi nhưng có lỗi thông tin (Parity, LRC,CRC), sẽ không có bản tin trả lời.Master sử lý sự kiện Time-out.

+Nếu Slave nhận được bản tin không bị lỗi thông tin nhưng không thể thực hiện được thì nó sẽ trả lời bản tin báo lỗi. Nó báo cho Master lỗi nào đã xảy ra.

ModBus -Trả lời báo lỗi

Bản tin báo lỗi bao gồm:

+ Trường địa chỉ báo thiết bị nào trả lời.
+ Trường chức năng với bit cao nhất bằng 1.
+ Trường dữ liệu báo lỗi nào đã xảy ra.
+ Trường kiểm tra lỗi.

ModBus -Trả lời báo lỗi

QUERY

Byte	Contents	Example
1	Slave Address	0A
2	Function	01
3	Starting Address Hi	04
4	Starting Address Lo	A1
5	No. of Coils Hi	00
6	No. of Coils Lo	01
7	LRC	4F

EXCEPTION RESPONSE

Byte	Contents	Example
1	Slave Address	0A
2	Function	81
3	Exception Code	02
4	LRC	73

ModBus -Trả lời báo lỗi

Code	Name	Meaning
01	ILLEGAL FUNCTION	The function code received in the query is not an allowable action for the slave. If a Poll Program Complete command was issued, this code indicates that no program function preceded it.
02	ILLEGAL DATA ADDRESS	The data address received in the query is not an allowable address for the slave.
03	ILLEGAL DATA VALUE	A value contained in the query data field is not an allowable value for the slave.

ModBus -Trả lời báo lỗi

04	SLAVE DEVICE FAILURE	An unrecoverable error occurred while the slave was attempting to perform the requested action.
05	ACKNOWLEDGE	The slave has accepted the request and is processing it, but a long duration of time will be required to do so. This response is returned to prevent a timeout error from occurring in the master. The master can next issue a Poll Program Complete message to determine if processing is completed.
06	SLAVE DEVICE BUSY	The slave is engaged in processing a long–duration program command. The master should retransmit the message later when the slave is free.

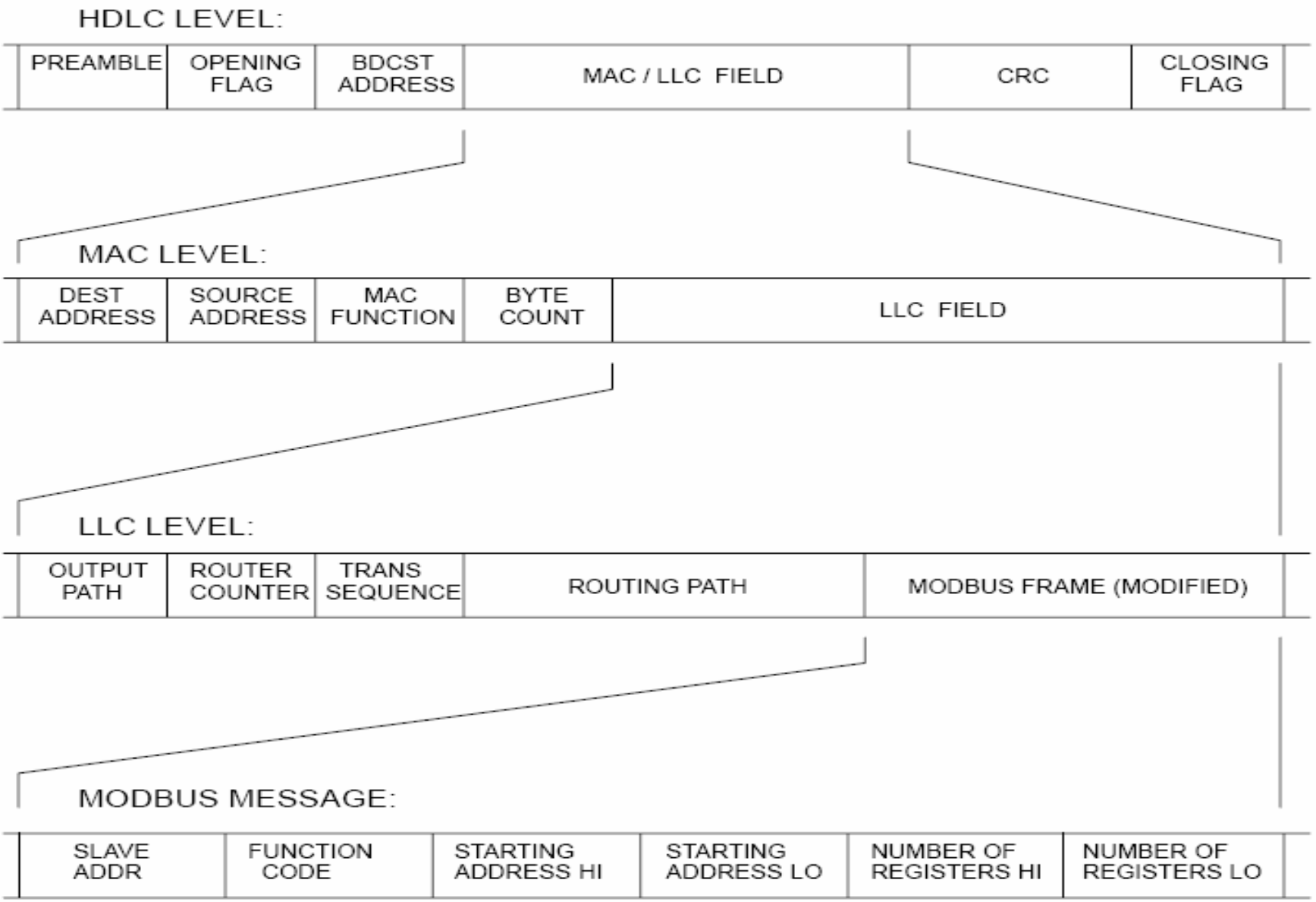
ModBus -Trả lời báo lỗi

07	NEGATIVE ACKNOWLEDGE	The slave cannot perform the program function received in the query. This code is returned for an unsuccessful programming request using function code 13 or 14 decimal. The master should request diagnostic or error information from the slave.
08	MEMORY PARITY ERROR	The slave attempted to read extended memory, but detected a parity error in the memory. The master can retry the request, but service may be required on the slave device.

ModBus Plus

- Là một hệ thống Bus dựa trên Modbus nhưng có giá thành thấp, dễ láp đặt, cài đặt.
- Cho phép đành địa chỉ 64 nút trên mạng, tốc độ truyền 1 Mbps.
- Mạng Peer-to-peer, sử dung MAC là Token passing.

ModBus Plus


HDLC LEVEL:
PREAMBLE
OPENING FLAG
BDCST ADDRESS
MAC / LLC FIELD
CRC
CLOSING FLAG
MAC LEVEL:
DEST ADDRESS
SOURCE ADDRESS
MAC FUNCTION
BYTE COUNT
LLC FIELD
LLC LEVEL:
OUTPUT PATH
ROUTER COUNTER
TRANS SEQUENCE
ROUTING PATH
MODBUS FRAME (MODIFIED)
MODBUS MESSAGE:
SLAVE ADDR
FUNCTION CODE
STARTING ADDRESS HI
STARTING ADDRESS LO
NUMBER OF REGISTERS HI
NUMBER OF REGISTERS LO

ModBus Plus

- Output Path (1 byte):Đường dẫn đầu ra chỉ một kênh logic của trạm chủ, có vai trò trong việc dồn kênh/phân kênh.
- Router counter (1 byte): đếm số router mà khung bản tin đã đi qua.
- Transaction Sequence Number: Mã số giao dịch
- Routing Path (5 byte): Mã số đường dẫn chức thông tin chọn đường tối ưu trong liên mạng.
- DA (1 byte): địa chit trạm đích.
- SA (1 byte): Địa chỉ trạm nguồn.
- MAC Function (1 byte): mã hàm điều khiển truy nhập đường truyền.

ModBus Plus

- Byte Count (2 byte) số lượng byte trong phần LLC được truyền.
- Preamble (1 byte): dãy bit báo hiệu đầu khung.
- Opening Flag (1 byte): Cờ mở đầu khung.
- Broadcast Address (1 byte): địa chỉ gửi đồng loạt.
- CRC (2 byte): kiểm tra lỗi CRC.
- Closing Flag (1 byte): cờ báo kết thúc