目　录

一. 概述

此次 Modbus RTU 通讯协议标准的制定参照 GB/T 19582—2008《基于 Modbus 协议的工业自动化网络规范》。协议中规定了功能码的使用和数据地址的分配, Modbus 通讯协议的实现请参照 GB/T 19582—2008《基于 Modbus 协议的工业自动化网络规范》 。

GB/T 19582—2008 分为三部分：

——第 1 部分： Modbus 应用协议；

——第 2 部分： Modbus 协议在串行链路上的实现指南；

——第 3 部分： Modbus 协议在 TCP/IP 上的实现指南。

第 1 部分描述了 Modbus 事物处理；第 2 部分提供了有助于开发者在串行链路上实现 Modbus 应用层的参考信息；第 3 部分提供了有助于开发者在 TCP/IP 上实现 Modbus 应用层的参考信息。

GB/T 19582—2008 包括两个通信规程中使用的 Modbus 应用层协议和服务规范：

——串行链路上的 Modbus 基于 TIA/EIA 标准： 232—E 和 485—A ；

—— TCP/IP 上的 Modbus 基于 IETF 标准： RFC793 和 RFC791。

Modbus 是一种请求 /应答协议，并提供功能码规定的服务。协议定义了一个与基础通信层无关的简单协议数据单元（ PDU）。特定总线或网络上的 Modbus 协议映射能够在数据单元（ADU ）上引入一些附加字段，如图 1.1 所示。

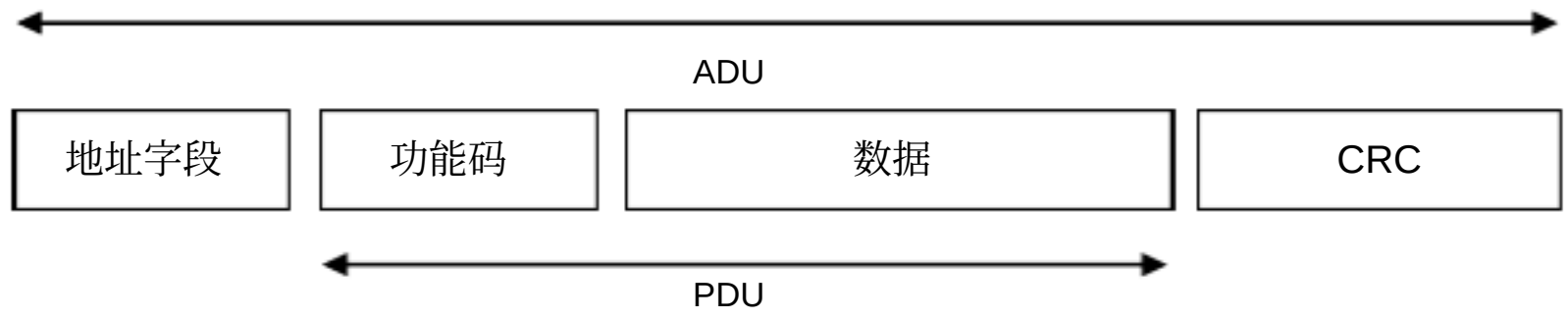


图 1.1 通用 Modbus 通讯帧

在一个正确接收的 Modbus ADU 中，如果不出现与请求的 Modbus 功能有关的差错，那么设备至上位机的相应数据字段包括所要求的数据。如果出现与所要求的 Modbus 功能有关的差错，那么该字段包括一个异常码。当设备对上位机响应时，它使用功能码字段来只是正常(无差错)响应(见图 1.2)或出现某中差错 (异常响应，见图 1.3)。

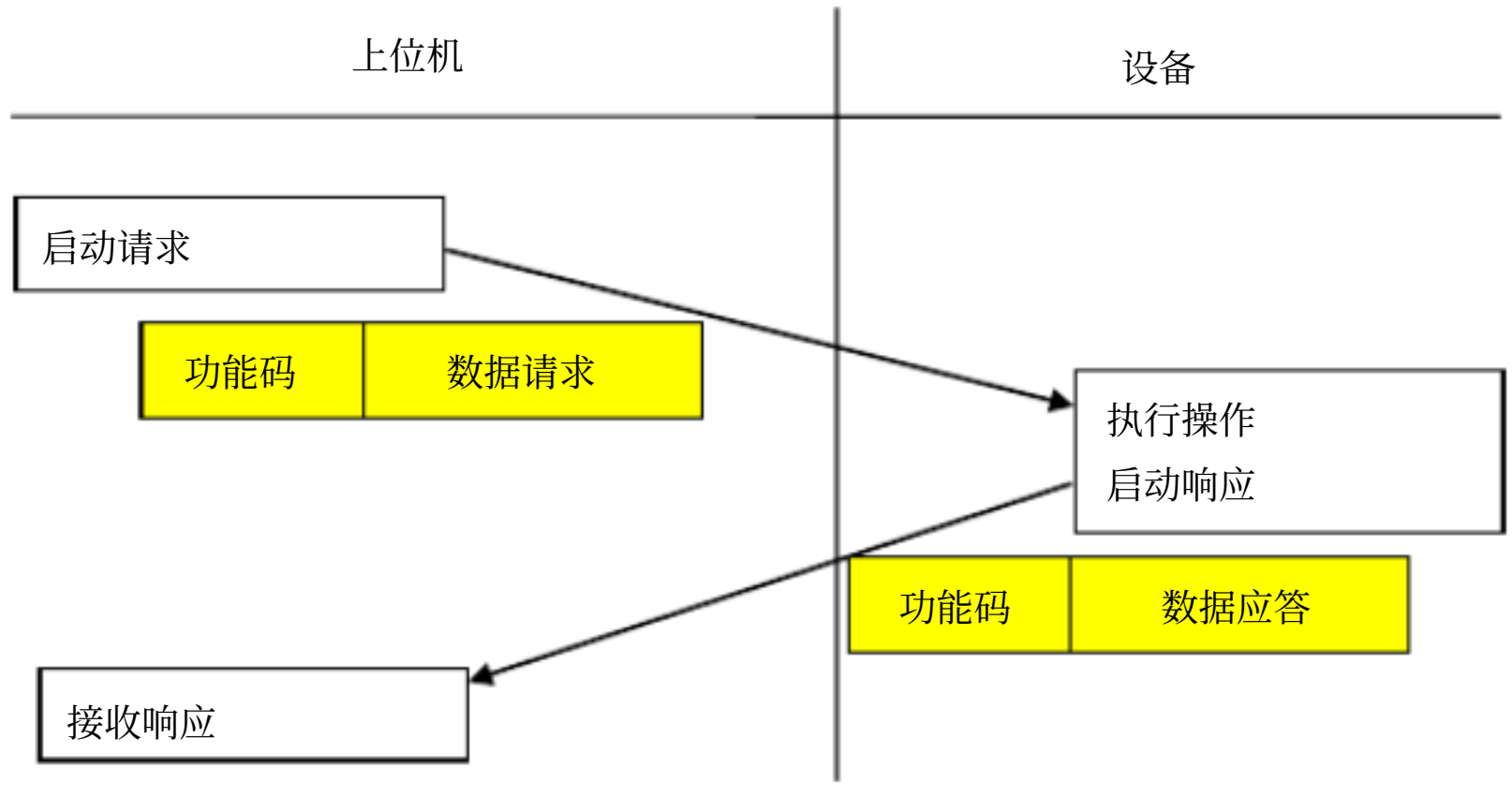


图 1.2 Modbus 事务处理 (无差错)

对于正常响应，设备仅复制原始功能码。对于异常响应，设备将请求　　PDU 中的原始功能的最高有效位设置逻辑　1 后返回。

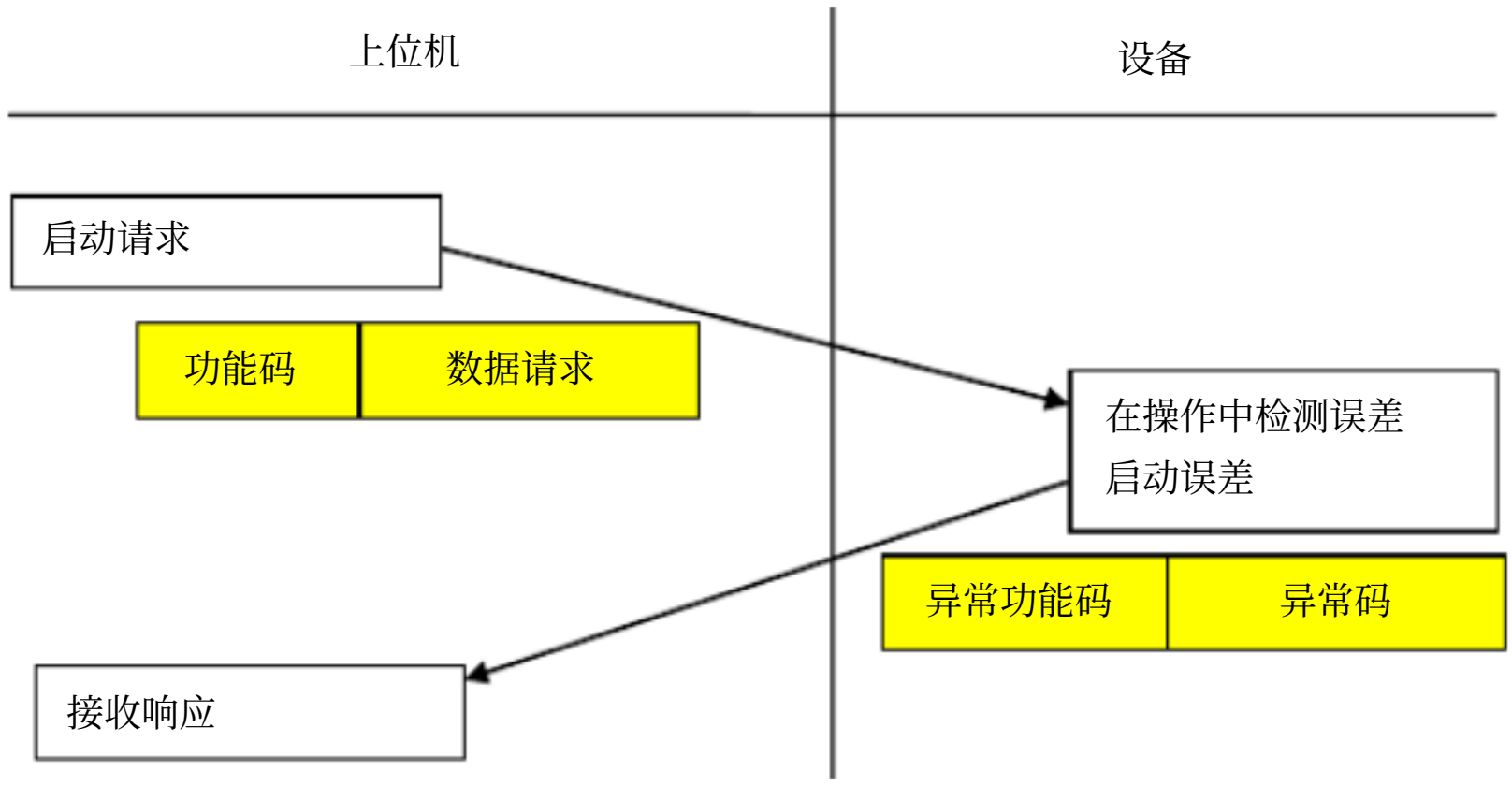


图 1.3 Modbus 事务处理（异常响应 ）

注意：需要超时管理，以免无期限的等待可能不会出现的应答。

串行通讯链路上　Modbus ADU 的长度最大为　256 字节，则 Modbus PDU=256-设备地址（1 字节） -CRC（2 字节） =253 字节。

Modbus 事务处理：

图 1.4 是 Modbus 事务处理状态图，描述了在设备上　Modbus 事务处理的一般过程。一旦设备处理请求，　就使用相应的　Modbus 事务处理生成　Modbus 响应。根据处理结果，　可以建立两种类型的响应：

——一个正常的　Modbus 响应：响应功能码　=请求功能码。

——一个异常的　Modbus 响应：

1)用来为上位机提供处理过程中与所发现的差错相关的信息；

2)异常功能码 =请求功能码 +0x80；

3)提供一个异常码来指示差错原因。

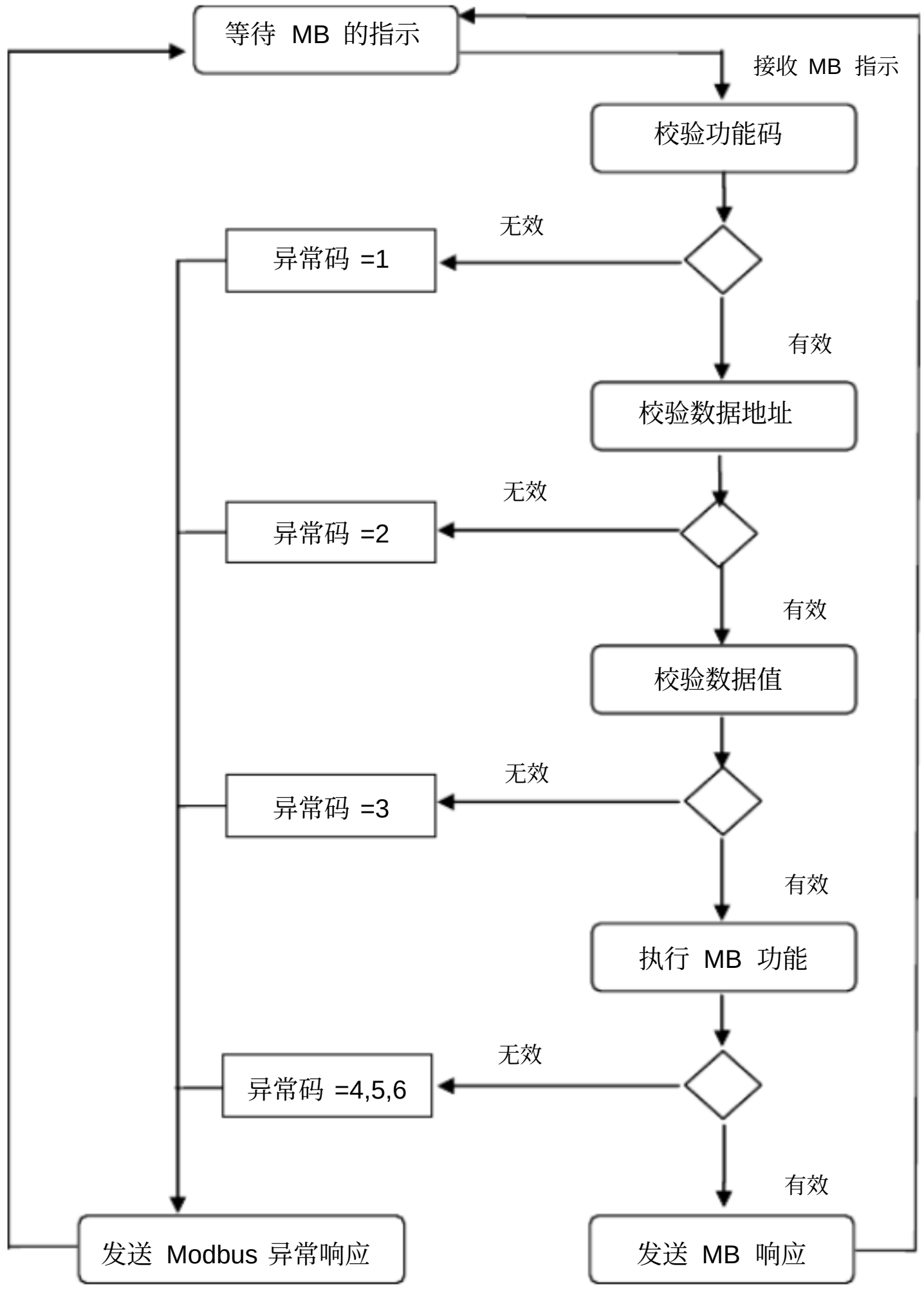


图 1.4 Modbus 事务处理的状态图

注：MB(Modbus Protocol) —— Modbus 协议。

二. 功能码分类

本协议中规定了 11 种功能码，其功能如表 2.1 所示：

表 2.1 功能码分类表

功能码	功能	备注
01(0x01)	读线圈	读开关量输出状态
02(0x02)	读离散量输入	读开关量输入状态、报警标志
03(0x03)	读保持寄存器	读系统参数、模拟量输出值
04(0x04)	读输入寄存器	读模拟量输入值、报警标志
05(0x05)	写单个线圈	写单个开关量输出状态
06(0x06)	写单个寄存器	写单个系统参数、模拟量输出值
15(0x0F)	写多个线圈	写多个开关量输出状态
16(0x10)	写多个寄存器	写多个系统参数、模拟量输出值
43/13(0x2B/0x0E)	读设备标识	读设备标识信息
65(0x41)	自定义	读标定参数及相关系统参数
66(0x42)	自定义	写多个标定参数及相关系统参数

三. 地址分配及功能码使用

3.1 开关量输出： 功能码 **0x01(**读**)**、**0x05(**写单个**)**、**0x0F(**写多个**)** 对外公布

0x0000H	第 1 路开关量输出通道状态	0 表示 OFF, 1 表示 ON
0x0001H	第 2 路开关量输出通道状态	0 表示 OFF, 1 表示 ON
0x0002H	第 3 路开关量输出通道状态	0 表示 OFF, 1 表示 ON
0x0003H	第 4 路开关量输出通道状态	0 表示 OFF, 1 表示 ON
0x0004H	第 5 路开关量输出通道状态	0 表示 OFF, 1 表示 ON
……	……	
0x002FH	第 48 路开关量输出通道状态	0 表示 OFF, 1 表示 ON

3.2 开关量输入： 功能码 **0x02(**读**)** 对外公布

0x0000H	第 1 路开关量输入通道状态	0 表示 OFF/低电平, 1 表示 ON/高电平
0x0001H	第 2 路开关量输入通道状态	0 表示 OFF/低电平, 1 表示 ON/高电平
0x0002H	第 3 路开关量输入通道状态	0 表示 OFF/低电平, 1 表示 ON/高电平
0x0003H	第 4 路开关量输入通道状态	0 表示 OFF/低电平, 1 表示 ON/高电平
0x0004H	第 5 路开关量输入通道状态	0 表示 OFF/低电平, 1 表示 ON/高电平
……	……	
0x002FH	第 48 路开关量输入通道状态	0 表示 OFF/低电平, 1 表示 ON/高电平
0x0030H	第 1 路开关量输入报警标志	0 表示正常, 1 表示报警
0x0031H	第 2 路开关量输入报警标志	0 表示正常, 1 表示报警
0x0032H	第 3 路开关量输入报警标志	0 表示正常, 1 表示报警
0x0033H	第 4 路开关量输入报警标志	0 表示正常, 1 表示报警
0x0034H	第 5 路开关量输入报警标志	0 表示正常, 1 表示报警
……	……	
0x005FH	第 48 路开关量输入报警标志	0 表示正常, 1 表示报警

3.3 模拟量输入： 功能码 **0x04(**读**)** 对外公布

0x0000H	第 1 路模拟量输入通道值	16 位整型
0x0001H	第 2 路模拟量输入通道值	16 位整型
0x0002H	第 3 路模拟量输入通道值	16 位整型
0x0003H	第 4 路模拟量输入通道值	16 位整型
0x0004H	第 5 路模拟量输入通道值	16 位整型
……	……	
0x002FH	第 48 路模拟量输入通道值	16 位整型
0x0030H	第 1 路模拟量输入报警标志	00 —— 无报警； 01 —— 上限报警； 02 —— 下限报警； 03 —— 上上限报警； 04 —— 下下限报警。
0x0031H	第 2 路模拟量输入报警标志	
0x0032H	第 3 路模拟量输入报警标志	
……	……	
0x005FH	第 8 路模拟量输入报警标志	

3.4 设备标识信息： 功能码 **0x2B/0x0E** 对外公布

0x00	厂商名称“ ColliHigh ”	ASII 字符串
0x01	产品代码，即序列号	ASII 字符串
0x02	版本号，如“ V1.0 ”	ASII 字符串
0x03	厂商网址“ www.klha.cn ”	ASII 字符串
0x04	产品名称，如“ KL-N4000 Series ”	ASII 字符串
0x05	型号名称，如“ KL-N4118-20mA-232 ”	ASII 字符串

3.5 模拟量输出及系统参数 对外公布

功能码 **0x03(**读**)**、**0x06(**写单个 **)**、 **0x10(**写多个 **)**

0x0000H	第 1 路模拟量输出通道值	16 位整型
0x0001H	第 2 路模拟量输出通道值	16 位整型
0x0002H	第 3 路模拟量输出通道值	16 位整型
0x0003H	第 4 路模拟量输出通道值	16 位整型
0x0004H	第 5 路模拟量输出通道值	16 位整型
……	……	
0x002FH	第 48 路模拟量输出通道值	16 位整型

0x0030H~0x0032H 串口通讯参数：

0x0030H	设备地址	地址范围： 1~247
0x0031H	通讯波特率	编码 01 —— 300bps；02 —— 600bps； 03 —— 1200bps；04 —— 2400bps； 05 —— 4800bps；06 —— 9600bps； 07 —— 19200bps；08 —— 38400bps； 09 —— 57600bps；0A —— 115200bps
0x0032H	串口通讯帧格式	编码 00 —— 偶检验 (默认)；01 —— 奇校验； 02 —— 无校验， 2 个停止位； 03 —— 无校验， 1 个停止位。

0x0033H~0x003FH 网络通讯参数：

0x0033H	设备网关低两位	低位在前高位在后
0x0034H	设备网关高两位	低位在前高位在后 例如：网关为 192.168.0.1 0x0033H 中的内容为 0x0100 0x0034H 中的内容为 0xA8C0
0x0035H	设备子网掩码低两位	低位在前高位在后
0x0036H	设备子网掩码高两位	低位在前高位在后 例如：子网掩码为 123.111.211.1 0x0035H 中的内容为 0x01D3 0x0036H 中的内容为 0x6F7B
0x0037H	设备 IP 低两位	低位在前高位在后
0x0038H	设备 IP 高两位	低位在前高位在后 例如：网关为 192.168.47.123 0x0037H 中的内容为 0x7B2F 0x0038H 中的内容为 0xA8C0
0x0039H	服务器 IP 低两位	低位在前高位在后
0x003AH	服务器 IP 高两位	低位在前高位在后 例如：网关为 211.100.8.14 0x0039H 中的内容为 0x0E08 0x003AH 中的内容为 0x64D3
0x003BH	服务器端口	16 位整型
0x003CH	设备通讯模式	0 —— TCP；1 —— UDP。
0x003DH	APN	0 —— CMNET ；1 —— CMWAP。
0x003EH	预留	
0x003FH	预留	

0x0040H	AD 滤波参数	16 位整型
0x0041H	系统睡眠时间	16 位整型
0x0042H	系统工作时间	16 位整型
0x0043H	系统参数恢复出厂设置	0 — 不恢复参数； 1 — 恢复参数。
0x0044H	预留	
.....		
0x005FH	预留	

0x0060H~0x065FH 模拟量输入通道参数：

0x0060H	第 1 路模拟量输入通道量程零点	16 位整型
0x0061H	第 2 路模拟量输入通道量程零点	16 位整型
0x0062H	第 3 路模拟量输入通道量程零点	16 位整型
0x0063H	第 4 路模拟量输入通道量程零点	16 位整型
.....	.....	
0x008FH	第 48 路模拟量输入通道量程零点	16 位整型
0x0090H	第 1 路模拟量输入通道量程满度	16 位整型
0x0091H	第 2 路模拟量输入通道量程满度	16 位整型
0x0092H	第 3 路模拟量输入通道量程满度	16 位整型
0x0093H	第 4 路模拟量输入通道量程满度	16 位整型
.....	.....	
0x00BFH	第 48 路模拟量输入通道量程满度	16 位整型
0x00C0H	第 1 路模拟量输入通道报警上限	16 位整型
0x00C1H	第 2 路模拟量输入通道报警上限	16 位整型
0x00C2H	第 3 路模拟量输入通道报警上限	16 位整型
0x00C3H	第 4 路模拟量输入通道报警上限	16 位整型
.....	.....	
0x00EFH	第 48 路模拟量输入通道报警上限	16 位整型
0x00F0H	第 1 路模拟量输入通道报警下限	16 位整型
0x00F1H	第 2 路模拟量输入通道报警下限	16 位整型
0x00F2H	第 3 路模拟量输入通道报警下限	16 位整型
0x00F3H	第 4 路模拟量输入通道报警下限	16 位整型
.....	.....	
0x011FH	第 48 路模拟量输入通道报警下限	16 位整型

0x0120H	第 1 路模拟量输入通道报警上上限	16 位整型
0x0121H	第 2 路模拟量输入通道报警上上限	16 位整型
0x0122H	第 3 路模拟量输入通道报警上上限	16 位整型
0x0123H	第 4 路模拟量输入通道报警上上限	16 位整型
……	……	
0x014FH	第 48 路模拟量输入通道报警上上限	16 位整型
0x0150H	第 1 路模拟量输入通道报警下下限	16 位整型
0x0151H	第 2 路模拟量输入通道报警下下限	16 位整型
0x0152H	第 3 路模拟量输入通道报警下下限	16 位整型
0x0153H	第 4 路模拟量输入通道报警下下限	16 位整型
……	……	
0x017FH	第 48 路模拟量输入通道报警下下限	16 位整型
0x0180H	第 1 路模拟量输入通道报警回差值	16 位整型
0x0181H	第 2 路模拟量输入通道报警回差值	16 位整型
0x0182H	第 3 路模拟量输入通道报警回差值	16 位整型
0x0183H	第 4 路模拟量输入通道报警回差值	16 位整型
……	……	
0x01AFH	第 48 路模拟量输入通道报警回差值	16 位整型
0x01B0H	第 1 路模拟量输入通道报警使能	0 — 不使能；1 — 使能报警。
0x01B1H	第 2 路模拟量输入通道报警使能	0 — 不使能；1 — 使能报警。
0x01B2H	第 3 路模拟量输入通道报警使能	0 — 不使能；1 — 使能报警。
0x01B3H	第 4 路模拟量输入通道报警使能	0 — 不使能；1 — 使能报警。
……	……	
0x01DFH	第 48 路模拟量输入通道报警使能	0 — 不使能；1 — 使能报警。
0x01E0H	第 1 路模拟量输入通道报警锁存	0 — 不锁存；1 — 锁存报警。
0x01E1H	第 2 路模拟量输入通道报警锁存	0 — 不锁存；1 — 锁存报警。
0x01E2H	第 3 路模拟量输入通道报警锁存	0 — 不锁存；1 — 锁存报警。
0x01E3H	第 4 路模拟量输入通道报警锁存	0 — 不锁存；1 — 锁存报警。
……	……	
0x020FH	第 48 路模拟量输入通道报警锁存	0 — 不锁存；1 — 锁存报警。

0x0210H	第 1 路模拟量输入通道偏移量	16 位整型
0x0211H	第 2 路模拟量输入通道偏移量	16 位整型
0x0212H	第 3 路模拟量输入通道偏移量	16 位整型
0x0213H	第 4 路模拟量输入通道偏移量	16 位整型
……	……	
0x023FH	第 48 路模拟量输入通道偏移量	16 位整型

0x0240H	第 1 模拟量输入通道上限报警联动	1~16 路继电器 0 表示联动； 1 表示不联动 低通道号对应低位： 低字节位 0 代表第 1 通道；位 7 代表第 8 通道，高字节位 0 代表第 9 通道；位 7 代表第 16 通道。
0x0241H	第 2 模拟量输入通道上限报警联动	1~16 路继电器
0x0242H	第 3 模拟量输入通道上限报警联动	1~16 路继电器
0x0243H	第 4 模拟量输入通道上限报警联动	1~16 路继电器
……	……	
0x026FH	第 48 模拟量输入通道上限报警联动	1~16 路继电器

0x0270H	第 1 模拟量输入通道上限报警联动	17~32 路继电器 0 表示联动； 1 表示不联动 低通道号对应低位： 低字节位 0 代表第 17 通道；位 7 代表第 24 通道，高字节位 0 代表第 25 通道；位 7 代表第 32 通道。
0x0271H	第 2 模拟量输入通道上限报警联动	17~32 路继电器
0x0272H	第 3 模拟量输入通道上限报警联动	17~32 路继电器
0x0273H	第 4 模拟量输入通道上限报警联动	17~32 路继电器
……	……	
0x029FH	第 48 模拟量输入通道上限报警联动	17~32 路继电器

0x02A0H	第 1 模拟量输入通道上限报警联动	33~48 路继电器 0 表示联动； 1 表示不联动 低字节位 0 代表第 33 通道；位 7 代表第 40 通道，高字节位 0 代表第 41 通道；位 7 代表第 48 通道。
0x02A1H	第 2 模拟量输入通道上限报警联动	33~48 路继电器
0x02A2H	第 3 模拟量输入通道上限报警联动	33~48 路继电器

0x02A3H　第 4 模拟量输入通道上限报警联动　33~48 路继电器
…… ……
0x02CFH　第 48 模拟量输入通道上限报警联动　33~48 路继电器

0x02D0H　第 1 模拟量输入通道下限报警联动　1~16 路继电器
0x02D1H　第 2 模拟量输入通道下限报警联动　1~16 路继电器
0x02D2H　第 3 模拟量输入通道下限报警联动　1~16 路继电器
0x02D3H　第 4 模拟量输入通道下限报警联动　1~16 路继电器
…… ……
0x02FFH　第 48 模拟量输入通道下限报警联动　1~16 路继电器

0x0300H　第 1 模拟量输入通道下限报警联动　17~32 路继电器
0x0301H　第 2 模拟量输入通道下限报警联动　17~32 路继电器
0x0302H　第 3 模拟量输入通道下限报警联动　17~32 路继电器
0x0303H　第 4 模拟量输入通道下限报警联动　17~32 路继电器
…… ……
0x032FH　第 48 模拟量输入通道下限报警联动　17~32 路继电器

0x0330H　第 1 模拟量输入通道下限报警联动　33~48 路继电器
0x0331H　第 2 模拟量输入通道下限报警联动　33~48 路继电器
0x0332H　第 3 模拟量输入通道下限报警联动　33~48 路继电器
0x0333H　第 4 模拟量输入通道下限报警联动　33~48 路继电器
…… ……
0x035FH　第 48 模拟量输入通道下限报警联动　33~48 路继电器

0x0360H　第 1 模拟量输入通道上上限报警联动　1~16 路继电器
0x0360H　第 2 模拟量输入通道上上限报警联动　1~16 路继电器
0x0360H　第 3 模拟量输入通道上上限报警联动　1~16 路继电器
0x0360H　第 4 模拟量输入通道上上限报警联动　1~16 路继电器
…… ……
0x038FH　第 48 模拟量输入通道上上限报警联动　1~16 路继电器

0x0390H　第 1 模拟量输入通道上上限报警联动　17~32 路继电器
0x0391H　第 2 模拟量输入通道上上限报警联动　17~32 路继电器
0x0392H　第 3 模拟量输入通道上上限报警联动　17~32 路继电器
0x0393H　第 4 模拟量输入通道上上限报警联动　17~32 路继电器
…… ……
0x03BFH　第 48 模拟量输入通道上上限报警联动　17~32 路继电器

0x03C0H	第 1 模拟量输入通道上上限报警联动	33~48 路继电器
0x03C1H	第 2 模拟量输入通道上上限报警联动	33~48 路继电器
0x03C2H	第 3 模拟量输入通道上上限报警联动	33~48 路继电器
0x03C3H	第 4 模拟量输入通道上上限报警联动	33~48 路继电器
……	……	
0x03EFH	第 48 模拟量输入通道上上限报警联动	33~48 路继电器
0x03F0H	第 1 模拟量输入通道下下限报警联动	1~16 路继电器
0x03F1H	第 2 模拟量输入通道下下限报警联动	1~16 路继电器
0x03F2H	第 3 模拟量输入通道下下限报警联动	1~16 路继电器
0x03F3H	第 4 模拟量输入通道下下限报警联动	1~16 路继电器
……	……	
0x041FH	第 48 模拟量输入通道下下限报警联动	1~16 路继电器
0x0420H	第 1 模拟量输入通道下下限报警联动	17~32 路继电器
0x0421H	第 2 模拟量输入通道下下限报警联动	17~32 路继电器
0x0422H	第 3 模拟量输入通道下下限报警联动	17~32 路继电器
0x0423H	第 4 模拟量输入通道下下限报警联动	17~32 路继电器
……	……	
0x044FH	第 48 模拟量输入通道下下限报警联动	17~32 路继电器
0x0450H	第 1 模拟量输入通道下下限报警联动	33~48 路继电器
0x0451H	第 2 模拟量输入通道下下限报警联动	33~48 路继电器
0x0452H	第 3 模拟量输入通道下下限报警联动	33~48 路继电器
0x0453H	第 4 模拟量输入通道下下限报警联动	33~48 路继电器
……	……	
0x047FH	第 48 模拟量输入通道下下限报警联动	33~48 路继电器

0x0480H~0x065FH 预留

0x0660H~0x095FH 开关量输入通道参数：

0x0660H	第 1 路开关量输入通道报警状态	0—闭合 /低电平报警； 1—断开 /高电平报警
0x0661H	第 2 路开关量输入通道报警状态	0—闭合 /低电平报警； 1—断开 /高电平报警
0x0662H	第 3 路开关量输入通道报警状态	0—闭合 /低电平报警； 1—断开 /高电平报警
0x0663H	第 4 路开关量输入通道报警状态	0—闭合 /低电平报警； 1—断开 /高电平报警
……	……	
0x068FH	第 48 路开关量输入通道报警状态	0—闭合 /低电平报警； 1—断开 /高电平报警

0x0690H	第 1 路开关量输入通道报警使能	0—不使能报警； 1—使能报警
0x0691H	第 2 路开关量输入通道报警使能	0—不使能报警； 1—使能报警
0x0692H	第 3 路开关量输入通道报警使能	0—不使能报警； 1—使能报警
0x0693H	第 4 路开关量输入通道报警使能	0—不使能报警； 1—使能报警
……	……	
0x06BFH	第 48 路开关量输入通道报警使能	0—不使能报警； 1—使能报警

0x06C0H	第 1 路开关量输入通道报警锁存	0—不锁存报警； 1—锁存报警
0x06C1H	第 2 路开关量输入通道报警锁存	0—不锁存报警； 1—锁存报警
0x06C2H	第 3 路开关量输入通道报警锁存	0—不锁存报警； 1—锁存报警
0x06C3H	第 4 路开关量输入通道报警锁存	0—不锁存报警； 1—锁存报警
……	……	
0x06EFH	第 48 路开关量输入通道报警锁存	0—不锁存报警； 1—锁存报警

0x06F0H	第 1 路开关量输入通道报警联动	1~16 路继电器 0 表示联动； 1 表示不联动 低通道号对应低位： 低字节位 0 代表第 1 通道；位 7 代表第 8 通道，高字节位 0 代表第 9 通道；位 7 代表第 16 通道。
0x06F1H	第 2 路开关量输入通道报警联动	1~16 路继电器
0x06F2H	第 3 路开关量输入通道报警联动	1~16 路继电器
0x06F3H	第 4 路开关量输入通道报警联动	1~16 路继电器
……	……	
0x071FH	第 48 路开关量输入通道报警联动	1~16 路继电器

0x0720H	第 1 路开关量输入通道报警联动	17~32 路继电器 0 表示联动； 1 表示不联动 低通道号对应低位： 低字节位 0 代表第 17 通道；位 7 代表第

24 通道，高字节位　0 代表第 25 通道；
位 7 代表第 32 通道。

0x0721H　第 2 路开关量输入通道报警联动　17~32 路继电器
0x0722H　第 3 路开关量输入通道报警联动　17~32 路继电器
0x0723H　第 4 路开关量输入通道报警联动　17~32 路继电器
……　……
0x074FH　第 48 路开关量输入通道报警联动　17~32 路继电器

0x0750H　第 1 路开关量输入通道报警联动　33~48 路继电器
0 表示联动； 1 表示不联动
低字节位 0 代表第 33 通道；位 7 代表第 40 通道，高字节位　0 代表第 41 通道；
位 7 代表第 48 通道。
0x0751H　第 2 路开关量输入通道报警联动　33~48 路继电器
0x0752H　第 3 路开关量输入通道报警联动　33~48 路继电器
0x0753H　第 4 路开关量输入通道报警联动　33~48 路继电器
……　……
0x077FH　第 48 路开关量输入通道报警联动　33~48 路继电器

0x0780H~0x095FH　预留

0x0960H~0x098FH 开关量输出通道参数：
0x0960H　第 1 路继电器输出控制标志　0 表示远程控制； 1 表示联动控制
0x0961H　第 2 路继电器输出控制标志　0 表示远程控制； 1 表示联动控制
0x0962H　第 3 路继电器输出控制标志　0 表示远程控制； 1 表示联动控制
0x0963H　第 4 路继电器输出控制标志　0 表示远程控制； 1 表示联动控制
……　……
0x098FH　第 48 路继电器输出控制标志　0 表示远程控制； 1 表示联动控制

0x0990H~0x09BFH 压力变送器专用： **48** 个
0x0990H　信道　16 位整型

0x09C0H~0x0A3FH 超声波变送器专用： **128** 个

0x09C0H	测量方式	0 表示测量物位高度； 1 表示测量物位距离。	
0x09C1H	修正值	16 位整型	
0x09C2H	滤波次数	16 位整型	3~9
0x09C3H	零点输出	16 位整型	
0x09C4H	满度输出	16 位整型	
0x09C5H	故障输出	16 位整型	
0x09C6H	温度显示选择	0 表示液晶不显示温度； 1 表示液晶显示温度。	
0x09C7H	波数显示选择	0 表示液晶不显示波数； 1 表示液晶显示波数。	
0x09C8H	波值显示选择	0 表示液晶不显示波值； 1 表示液晶显示波值。	
0x09C9H	接收范围选择	0 表示液晶不显示接收范围； 1 表示液晶显示接收范围。	
0x09CAH	近端距离	16 位整型	
0x09CBH	远端距离	16 位整型	
0x09CCH	通讯协议	16 位整型	
0x09CDH	接收模式	0 表示 “ 模式 1 ”；1 表示 “ 模式 2 ”。	
0x09CEH	发射频率	16 位整型	
0x09CFH	发射模式	0 表示 “ 模式 1 ”；1 表示 “ 模式 2 ”。	
0x09D0H	发射强度 1	16 位整型	0~16
0x09D1H	发射强度 2	16 位整型	0~16
0x09D2H	发射强度 3	16 位整型	0~16
0x09D3H	发射强度 4	16 位整型	0~16
0x09D4H	发射强度 5	16 位整型	0~16
0x09D5H	发射强度 6	16 位整型	0~16
0x09D6H	发射强度 7	16 位整型	0~16
0x09D7H	发射强度 8	16 位整型	0~16
0x09D8H	发射强度 9	16 位整型	0~16
0x09D9H	发射强度 10	16 位整型	0~16
0x09DAH	接收灵敏度 1	16 位整型	0~9
0x09DBH	接收灵敏度 2	16 位整型	0~9
0x09DCH	接收灵敏度 3	16 位整型	0~9
0x09DDH	接收灵敏度 4	16 位整型	0~9
0x09DEH	接收灵敏度 5	16 位整型	0~9
0x09DFH	接收灵敏度 6	16 位整型	0~9
0x09E0H	接收灵敏度 7	16 位整型	0~9
0x09E1H	接收灵敏度 8	16 位整型	0~9
0x09E2H	接收灵敏度 9	16 位整型	0~9
0x09E3H	接收灵敏度 10	16 位整型	0~9
0x09E4H	比较电平值	16 位整型	

0x09E5H	波形宽度	16 位整型
0x09E6H	测量介质	16 位整型
0x09E7H	背光延时时间	16 位整型
0x09E8H	安装高度	16 位整型
0x09E9H	高度设置	16 位整型
0x09EAH	低位设置	16 位整型
0x09EBH	预留	
……	……	
0x0A3FH	预留	

0x0A40H~0x0ABFH 油、水液面变送器专用： **128** 个

0x0A40H	输出方式	0 — 测量物位高度； 1 — 测量物位距离。	
0x0A41H	探极数量	16 位整型	0~40
0x0A42H	起始探极	16 位整型	0~40
0x0A43H	结束探极	16 位整型	0~40
0x0A44H	零点设置	16 位整型	
0x0A45H	满度设置	16 位整型	
0x0A46H	修正值	16 位整型	
0x0A47H	启动延时	16 位整型	
0x0A48H	峰值延时	16 位整型	
0x0A49H	均值延时	16 位整型	
0x0A4AH	整定延时	16 位整型	
0x0A4BH	滤波次数	16 位整型	0~99
0x0A4CH	测量介质	16 位整型	
0x0A4DH	油气正常值	16 位整型	
0x0A4EH	油气最小值	16 位整型	
0x0A4FH	油水正常值	16 位整型	
0x0A50H	油水最小值	16 位整型	
0x0A51H	一级增益	16 位整型	0~9
0x0A52H	二级增益	16 位整型	0~9
0x0A53H	探极长度	16 位整型	
0x0A54H	单个探极	16 位整型	
0x0A55H	中间探极	16 位整型	
0x0A56H	工作频率	16 位整型	
0x0A57H	工作模式	0 — “ 模式 1 ”；1 — “ 模式 2 ”。	

0x0A58H	系数修正值 1	16 位整型
0x0A59H	系数修正值 2	16 位整型
0x0A5AH	系数修正值 3	16 位整型
0x0A5BH	系数修正值 4	16 位整型
.....	.....	
0x0A7FH	系数修正值 40	16 位整型
0x0A80H	自整定使能	0 — 不使能自整定； 1 — 使能自整定。
0x0A81H	干扰探极	16 位整型 0~99
0x0A82H	空气电压值	16 位整型
0x0A83H	满油电压值	16 位整型
0x0A84H	背光延时时间	16 位整型
0x0A86H~0x0ABFH	预留	

0x0AC0H~0x0FFFH GPRS 数据采集模块专用： **1344** 个

0x0AC0H~0x0BBFH	服务器域名	16 位整型	256 字节
0x0BC0H	GPRS 最大在线时间	16 位整型	
0x0BC1H	GPRS 最大离线时间	16 位整型	
0x0BC2H	电话申请的时间长度	16 位整型	
0x0BC3H	设备工作模式	16 位整型	
0x0BC4H	设备自动操作和数据传输模式	16 位整型	
0x0BC5H	短信群发标志	0 表示按通道发送； 1 表示群发。	
0x0BC6H	群发模式下要处理的号码序号	16 位整型	
0x0BC7H	预留		
0x0BC8H	预留		
0x0BC9H	预留		
0x0BCAH	预留		
0x0BCBH	预留		
0x0BCCH	预留		
0x0BCDH	预留		
0x0BCEH	预留		
0x0BCFH	预留		
0x0BD0H	第 1 路模拟量输入通道基准零点	16 位整型	
0x0BD1H	第 1 路模拟量输入通道基准满度	16 位整型	
0x0BD2H	第 2 路模拟量输入通道基准零点	16 位整型	
0x0BD3H	第 2 路模拟量输入通道基准满度	16 位整型	
.....	.....		
0x0C2EH	第 48 路模拟量输入通道基准零点	16 位整型	
0x0C2FH	第 48 路模拟量输入通道基准满度	16 位整型	

0x0C30H~0x0C37H	短信号码 1	16 位整型
0x0C38H~0x0C3FH	短信号码 2	16 位整型
0x0C40H~0x0C47H	短信号码 3	16 位整型
0x0C48H~0x0C4FH	短信号码 4	16 位整型
0x0C50H~0x0C57H	短信号码 5	16 位整型
0x0C58H~0x0C5FH	短信号码 6	16 位整型
0x0C60H~0x0C67H	短信号码 7	16 位整型
0x0C68H~0x0C6FH	短信号码 8	16 位整型
0x0C70H~0x0C77H	语音电话号码 1	16 位整型
0x0C78H~0x0C7FH	语音电话号码 2	16 位整型
0x0C80H~0x0C87H	语音电话号码 3	16 位整型
0x0C88H~0x0C8FH	语音电话号码 4	16 位整型
0x0C90H~0x0CAFH	短信息内容 1	16 位整型
0x0CB0H~0x0CCFH	短信息内容 2	16 位整型
0x0CD0H~0x0CEFH	短信息内容 3	16 位整型
0x0CF0H~0x0D0FH	短信息内容 4	16 位整型
0x0D10H~0x0D2FH	短信息内容 5	16 位整型
0x0D30H~0x0D4FH	短信息内容 6	16 位整型
0x0D50H~0x0D6FH	短信息内容 7	16 位整型
0x0D70H~0x0D8FH	短信息内容 8	16 位整型
0x0D90H~0x0FFFH	预留	

0x1000H~0x10FFH 以太网数据采集模块专用： **256** 个

0x1100H~0x11FFH Zigbee 模块专用： **256** 个

0x1100H	无线频点	16 位整型
0x1101H	无线发射功率	16 位整型
0x1102H	网络类型	16 位整型
0x1103H	节点类型	16 位整型
0x1104H	网络编号	16 位整型

0x1200H~0x12FFH WiFi 模块专用： **256** 个

3.6 系统参数　　功能码　**0x41(**读**)**、**0x42(**写多个 **)**　　不对外公布

0x0000H	第 1 路模拟量输入通道　AD 标定点 1	16 位整型
0x0001H	第 2 路模拟量输入通道　AD 标定点 1	16 位整型
0x0002H	第 3 路模拟量输入通道　AD 标定点 1	16 位整型
0x0003H	第 4 路模拟量输入通道　AD 标定点 1	16 位整型
……	……	
0x002FH	第 48 路模拟量输入通道　AD 标定点 1	16 位整型
0x0030H	第 1 路模拟量输入通道　AD 标定点 2	16 位整型
0x0031H	第 2 路模拟量输入通道　AD 标定点 2	16 位整型
0x0032H	第 3 路模拟量输入通道　AD 标定点 2	16 位整型
0x0033H	第 4 路模拟量输入通道　AD 标定点 2	16 位整型
……	……	
0x005FH	第 48 路模拟量输入通道　AD 标定点 2	16 位整型

……

0x02D0H	第 1 路模拟量输入通道　AD 标定点 16	16 位整型
0x02D1H	第 2 路模拟量输入通道　AD 标定点 16	16 位整型
0x02D2H	第 3 路模拟量输入通道　AD 标定点 16	16 位整型
0x02D3H	第 4 路模拟量输入通道　AD 标定点 16	16 位整型
……	……	
0x02FFH	第 48 路模拟量输入通道　AD 标定点 16	16 位整型
0x0300H	第 1 路模拟量输出通道　DA 标定点 1	16 位整型
0x0301H	第 2 路模拟量输出通道　DA 标定点 1	16 位整型
0x0302H	第 3 路模拟量输出通道　DA 标定点 1	16 位整型
0x0303H	第 4 路模拟量输出通道　DA 标定点 1	16 位整型
……	……	
0x032FH	第 48 路模拟量输出通道　DA 标定点 1	16 位整型
0x0330H	第 1 路模拟量输出通道　DA 标定点 2	16 位整型
0x0331H	第 2 路模拟量输出通道　DA 标定点 2	16 位整型
0x0332H	第 3 路模拟量输出通道　DA 标定点 2	16 位整型
0x0333H	第 4 路模拟量输出通道　DA 标定点 2	16 位整型
……	……	
0x035FH	第 48 路模拟量输出通道　DA 标定点 2	16 位整型

.....		
0x05D0H	第 1 路模拟量输出通道 DA 标定点 16	16 位整型
0x05D1H	第 2 路模拟量输出通道 DA 标定点 16	16 位整型
0x05D2H	第 3 路模拟量输出通道 DA 标定点 16	16 位整型
0x05D3H	第 4 路模拟量输出通道 DA 标定点 16	16 位整型
.....	.....	
0x05FFH	第 48 路模拟量输出通道 DA 标定点 16	16 位整型
0x0600H	开关量输入通道数	16 位整型
0x0601H	开关量输出通道数	16 位整型
0x0602H	模拟量输入通道数	16 位整型
0x0603H	模拟量输出通道数	16 位整型
0x0604H	预留	
.....	.....	
0x061FH	预留	
0x0620H	第 1 路模拟量输入通道量程零点	16 位整型
0x0621H	第 2 路模拟量输入通道量程零点	16 位整型
0x0622H	第 3 路模拟量输入通道量程零点	16 位整型
0x0623H	第 4 路模拟量输入通道量程零点	16 位整型
.....	.....	
0x064FH	第 48 路模拟量输入通道量程零点	16 位整型
0x0650H	第 1 路模拟量输入通道量程满度	16 位整型
0x0651H	第 2 路模拟量输入通道量程满度	16 位整型
0x0652H	第 3 路模拟量输入通道量程满度	16 位整型
0x0653H	第 4 路模拟量输入通道量程满度	16 位整型
.....	.....	
0x067FH	第 48 路模拟量输入通道量程满度	16 位整型
0x0680H	第 1 路模拟量输入通道类型	编码 00 —— 4~20mA；01 —— 0~20mA； 02 —— 0~10mA；03 —— 0~5V； 04 —— 0~10V；05 —— PT100； 06 —— 0~100mV。
0x0681H	第 2 路模拟量输入通道类型	编码
0x0682H	第 3 路模拟量输入通道类型	编码
0x0683H	第 4 路模拟量输入通道类型	编码
.....	.....	

0x06AFH　　第 48 路模拟量输入通道类型　　编码
0x06B0H~0x06BFH　　产品系列号

0x1000H~0x10FFH　压力变送器专用：　**256** 个
0x1100H~0x11FFH　超声波变送器专用：　**256** 个
0x1200H~0x12FFH　油、水液面变送器专用：　**256** 个
0x1300H~0x13FFH　**GPRS** 采集模块专用：　**256** 个
0x1400H~0x14FFH　以太网专用：　**256** 个
0x1500H~0x15FFH　**Zigbee** 模块专用：　**256** 个
0x1600H~0x16FFH　**WiFi** 模块专用：　**256** 个

四. 功能码描述

4.1 01(0x01)读线圈

功能码 01(0x01)用于读开关量 (继电器)输出通道状态，如图 4.1 和表 4.1~4.3 所示：

表 4.1 读线圈请求

功能码	1 字节	0x01
起始地址	2 字节	0x0000~0xFFFF
线圈数量	2 字节	1~2000(0x7D0)

表 4.2 读线圈响应

功能码	1 字节	0x01
字节计数	1 字节	N
线圈状态	n 字节	n=N 或 N+1
N= 输出数量 /8，若余数不等于 0，则 N=N+1		

表 4.3 读线圈错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03 或 04

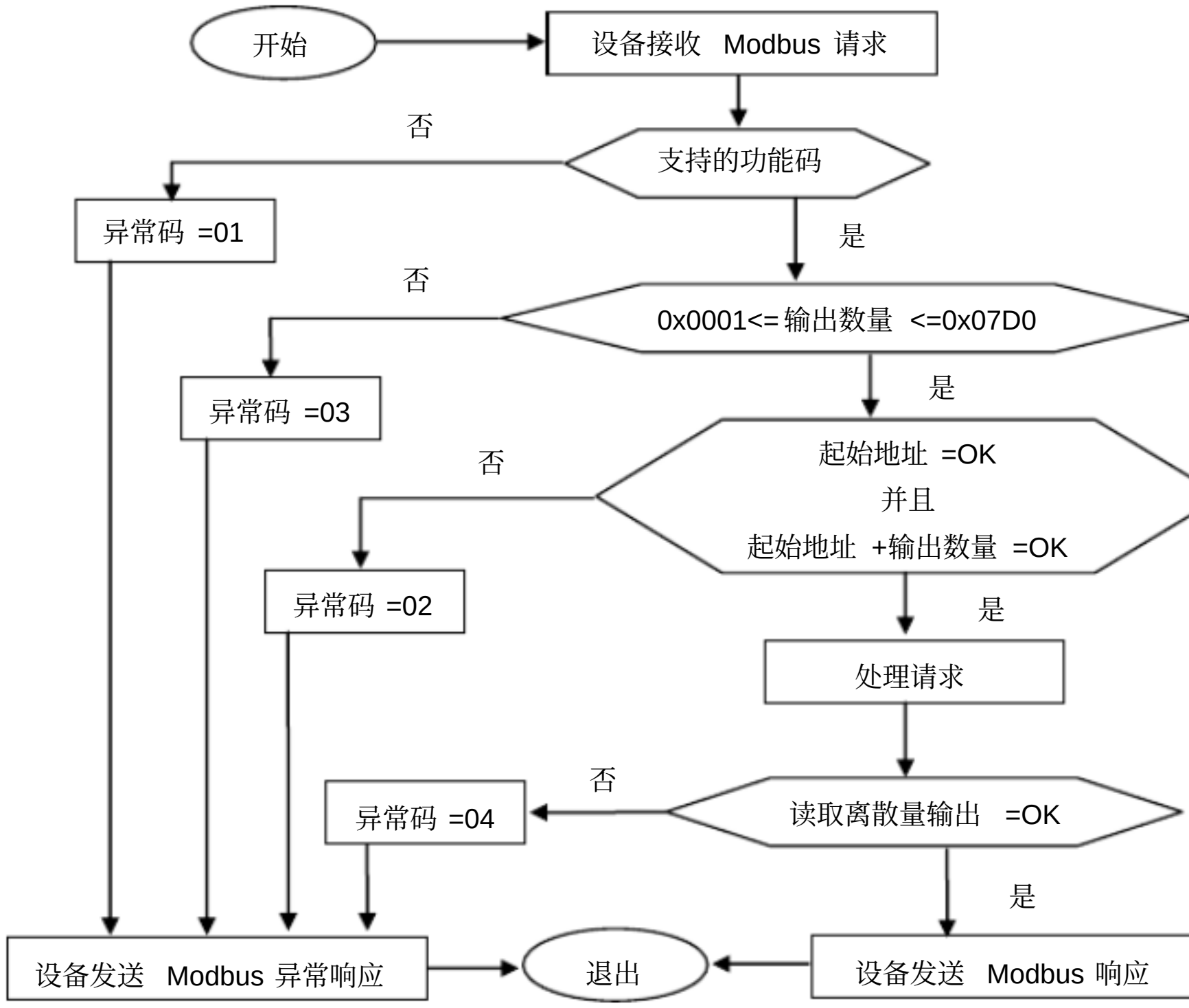


图 4.1 读线圈状态图

该功能码可从设备中读 1~2000 个连续的线圈状态。请求 PDU 指定了起始地址，即指定了第一个线圈地址和线圈数目。在 PDU 中，从零开始寻址线圈，因此编号为 1~16 的线圈寻址为 0~15。

响应报文中的线圈按数据字段的每位一个线圈进行打包。状态被表示成 1=ON/高电平和 0=OFF/低电平。第一个数据字节的 LSB(最低有效位)包含询问中所寻址的输出。其他线圈依次类推，一直到这个字节的高位端为止，并在后续字节中按照从低位到高位的顺序排列。

若返回的输出数量不是 8 的倍数，将用零填补最后数据字节中的剩余位 (一直到字节的高位端)。字节计数字段指定了数据的全部字节数。

表 4.4 是一个请求读数字量输出 20~38 的示例。

表 4.4 读数字量输出

请求		响应	
字段名	十六进制	字段名	十六进制
功能	01	功能	01
起始地址 Hi	00	字节计数	03
起始地址 Lo	13	输出状态 27~20	CD
输出数量 Hi	00	输出状态 35~28	6B
输出数量 Lo	13	输出状态 28~36	05

将输出 27~20 的状态表示为十六进制字节值 CD，或二进制 1100 1101。输出 27 是这个字节的 MSB(最高有效位)，输出 20 是 LSB(最低有效位)。

通常，一个字节的 MSB 位于左侧，LSB 位于右侧。第一个字节的输出从左到右为 27~20。下一个字节的输出从左到右为 35~28。当串行发送这些位时，从 LSB 向 MSB 传输：20~27、28~35 等等。

在最后的数据字节中，将输出 38~36 的状态表示为十六进制字节值 05，回二进制 0000 0101。输出 38 是左侧第六个位位置， 输出 36 是这个字节的 LSB。用零填充 5 个剩余高位位。

注：用零填充 5 个剩余位 (一直到高端)。

4.2 02(0x02)读离散量输入

功能码 02(0x02)用于读开关量输入通道状态，如图 4.2 和表 4.5~4.7 所示：

表 4.5 读线圈请求

功能码	1 字节	0x02
起始地址	2 字节	0x0000~0xFFFF
输入数量	2 字节	1~2000(0x7D0)

表 4.6 读线圈响应

功能码	1 字节	0x02
字节计数	1 字节	N
输入状态	N*1 字节	.....
N= 输出数量 /8，若余数不等于 0，则 N=N+1		

表 4.7 读线圈错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03 或 04

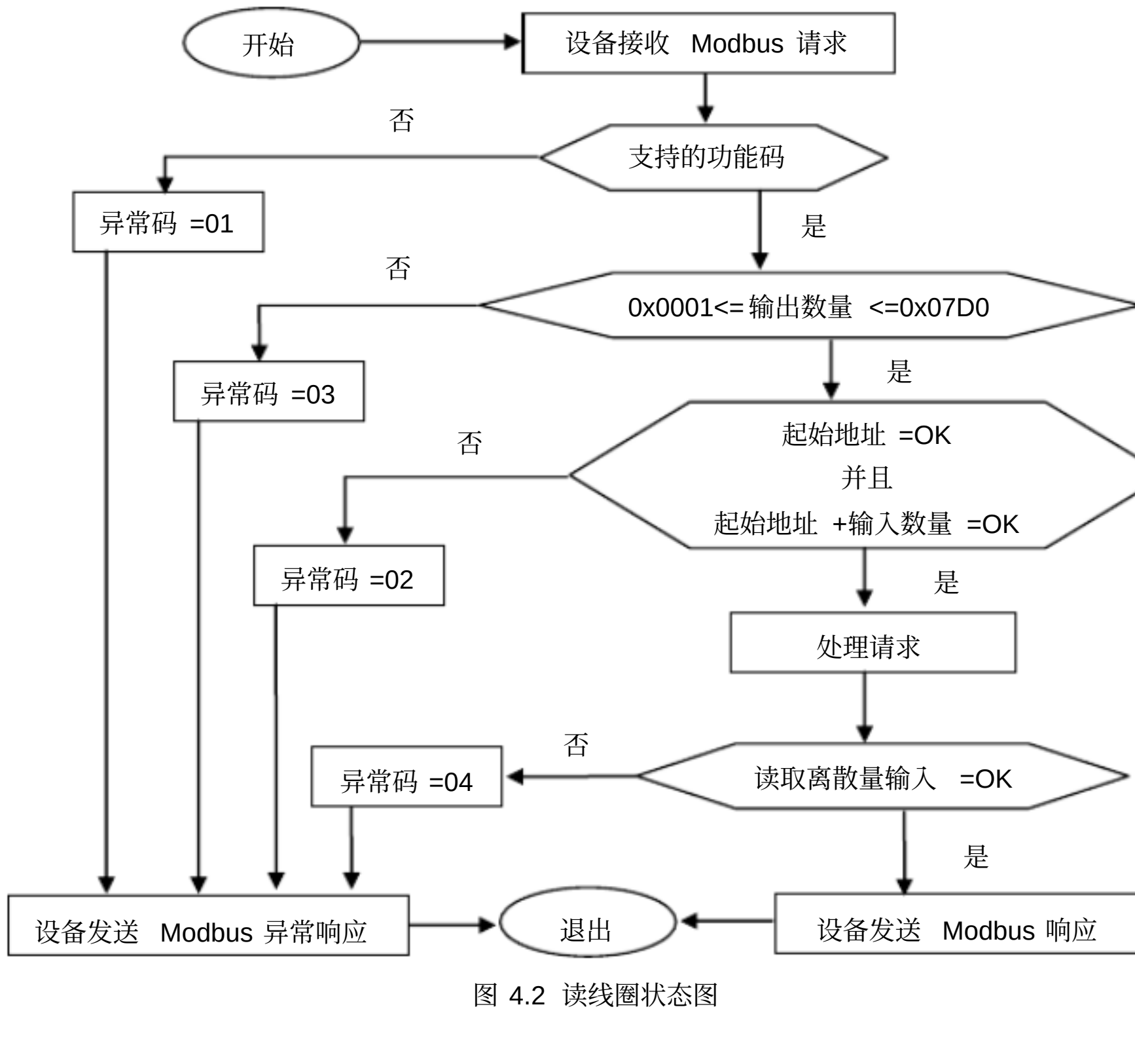


图 4.2 读线圈状态图

该功能码可从设备中读 1~2000 个连续的离散量输入状态。请求 PDU 指定了起始地址，即指定了第一个离散量输入地址和离散量输入数目。在 PDU 中，从零开始寻址离散量输入，因此编号为 1~16 的离散量输入寻址为 0~15。

响应报文中的离散量输入按数据字段的每位一个离散量输入进行打包。状态被表示成 1=ON/高电平和 0=OFF/低电平。第一个数据字节的 LSB(最低有效位)包含询问中所寻址的输入。其他离散量输入依次类推，一直到这个字节的高位端为止，并在后续字节中按照从低位到高位的顺序排列。

若返回的输入数量不是 8 的倍数，将用零填补最后数据字节中的剩余位 (一直到字节的高位端)。字节计数字段指定了数据的全部字节数。

表 4.8 是一个请求读离散量输入 197~218 的示例。

表 4.8 读离散量输入

请求		响应	
字段名	十六进制	字段名	十六进制
功能	02	功能	02
起始地址 Hi	00	字节计数	03
起始地址 Lo	C4	输入状态 204~197	AC
输出数量 Hi	00	输入状态 212~205	DB
输出数量 Lo	16	输入状态 218~213	35

将离散量输入 204~197 的状态表示为十六进制字节值 AC，或二进制 1010 1100。输入 204 是这个字节的 MSB，输入 197 是 LSB。

将离散量输入 218~213 的状态表示为十六进制字节值 35，或二进制 0011 0101。输入 218 位于左侧第 3 位，输入 213 是 LSB。

注：用零填充 2 个剩余位 (一直到高端)。

4.3 03(0x03)读保持寄存器

功能码 03(0x03)用于读系统参数、模拟量输出值，如图 4.3 和表 4.9~4.11 所示：

表 4.9 读保存寄存器

功能码	1 字节	0x03
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	1~125(0x07D)

表 4.10 读保存寄存器响应

功能码	1 字节	0x03
字节计数	1 字节	N*2
输入状态	N*2 字节	.....
N= 保持寄存器的数量		

表 4.11 读保持寄存器错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03 或 04

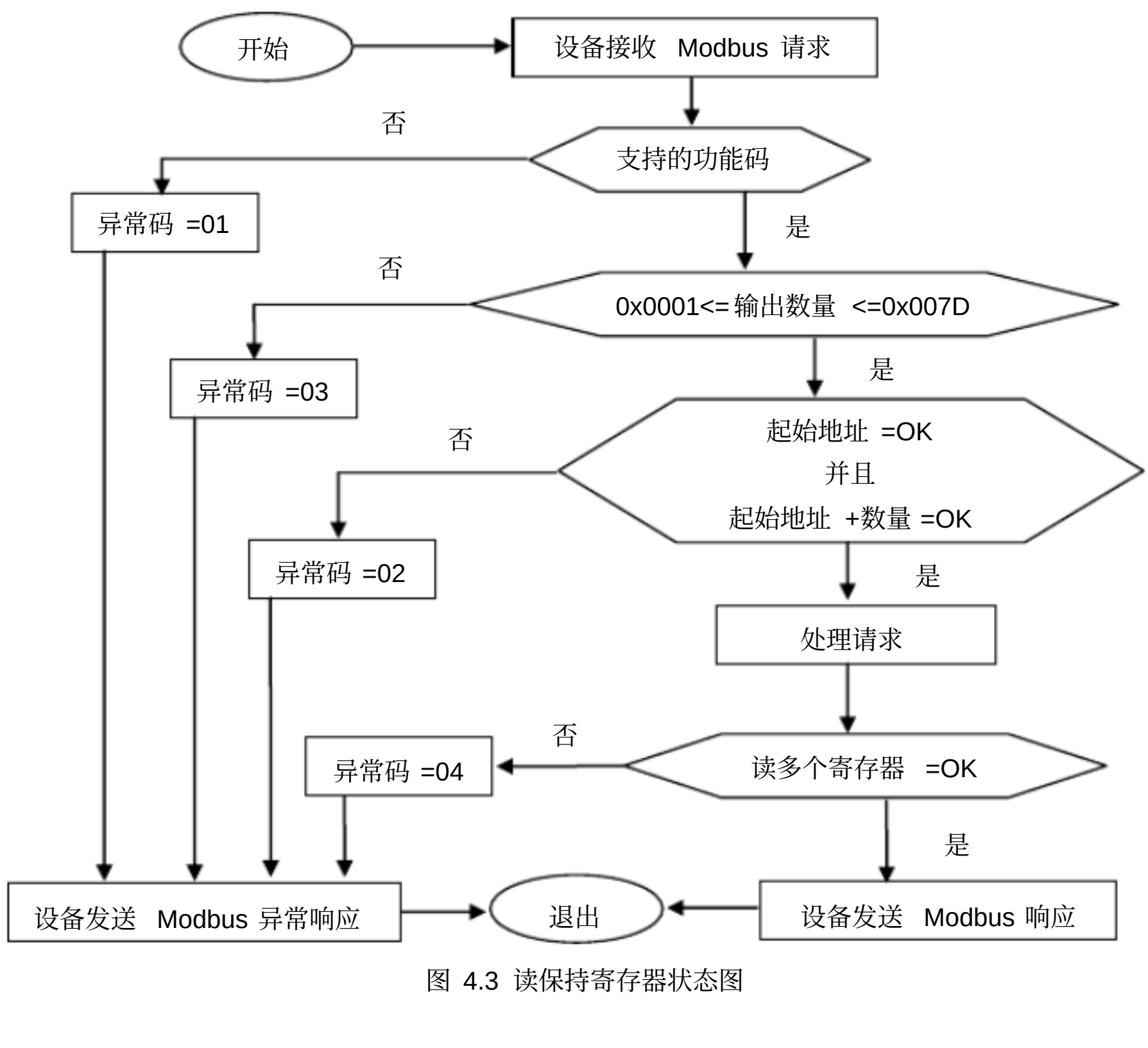


图 4.3 读保持寄存器状态图

该功能码可从设备中连续读 125 个保持寄存器的内容。 请求 PDU 指定了起始寄存器地址和寄存器数量。 在 PDU 中，从零开始寻址寄存器， 因此编号为 1~16 的寄存器被寻址为 0~15。

将响应报文中的寄存器数据按每个寄存器两字节进行打包，这个二进制内容正好填满每个字节。对于每个寄存器，第一个字节包括高位位，第二个字节包括低位位。

表 4.12 是一个请求读保存寄存器 108~110的示例。

表 4.12 读保存寄存器

请求		响应	
字段名	十六进制	字段名	十六进制
功能	03	功能	03
起始地址 Hi	00	字节计数	06
起始地址 Lo	6B	寄存器值 Hi(108)	02
输出数量 Hi	00	寄存器值 Lo(108)	2B
输出数量 Lo	03	寄存器值 Hi(109)	00
		寄存器值 Lo(109)	00
		寄存器值 Hi(110)	00
		寄存器值 Lo(110)	64

将寄存器 108 的内容表示为两个十六进制字节值 02 2B, 或十进制 555。将寄存器 109~110 的内容分别表示为十六进制字节值 00 00 和 00 64, 或十进制 0 和 100。

4.4 04(0x04)读输入寄存器

功能码 04(0x04)用于读模拟量输入值、报警标志，如图 4.4 和表 4.13~4.15所示：

表 4.13 读输入寄存器

功能码	1 字节	0x04
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	1~125(0x007D)

表 4.14 读输入寄存器响应

功能码	1 字节	0x04
字节计数	1 字节	N*2
输入状态	N*2 字节	.....
N= 输入寄存器的数量		

表 4.15 读输入寄存器错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03 或 04

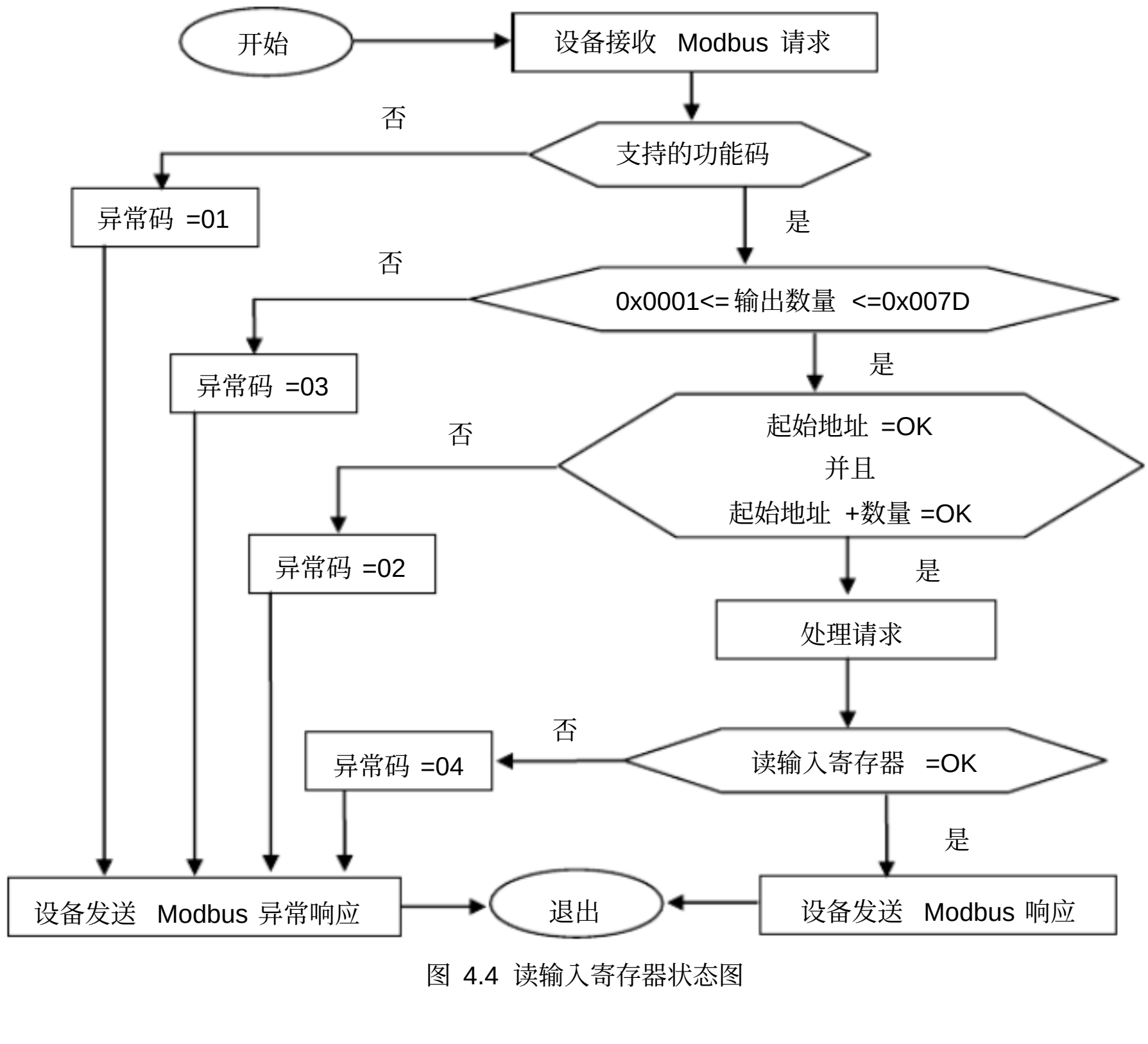


图 4.4 读输入寄存器状态图

该功能码可从设备中读　1~125 个连续输入寄存器的内容。

请求 PDU 指定了起始寄存器地址和寄存器数量。在　PDU 中，从零开始寻址寄存器，因此编号为 1~16 的寄存器被寻址为　0~15。

将响应报文中的寄存器数据按每个寄存器两字节进行打包，这个二进制内容正好填满每个字节。对于每个寄存器，第一个字节包括高位位，第二个字节包括低位位。

表 4.16 是一个请求读输入寄存器　9 的示例。

表 4.16 读输入寄存器

请求		响应	
字段名	十六进制	字段名	十六进制
功能	04	功能	04
起始地址 Hi	00	字节计数	02
起始地址 Lo	08	寄存器值 Hi(9)	00
输出数量 Hi	00	寄存器值 Lo(9)	0A
输出数量 Lo	01		

将输入寄存器 9 的内容表示为两个十六进制字节值　00 0A，或十进制 10。

4.5 05(0x05)写单个线圈

功能码 05(0x05)用于写单个开关量 (继电器)输出状态，如图 4.5 和表 4.17~4.19 所示：

表 4.17 写单个线圈请求

功能码	1 字节	0x05
起始地址	2 字节	0x0000~0xFFFF
输出值	2 字节	0x0000 或 0xFF00

表 4.18 写单个线圈响应

功能码	1 字节	0x05
起始地址	2 字节	0x0000~0xFFFF
输出值	2 字节	0x0000 或 0xFF00

表 4.19 写单个线圈错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03 或 04

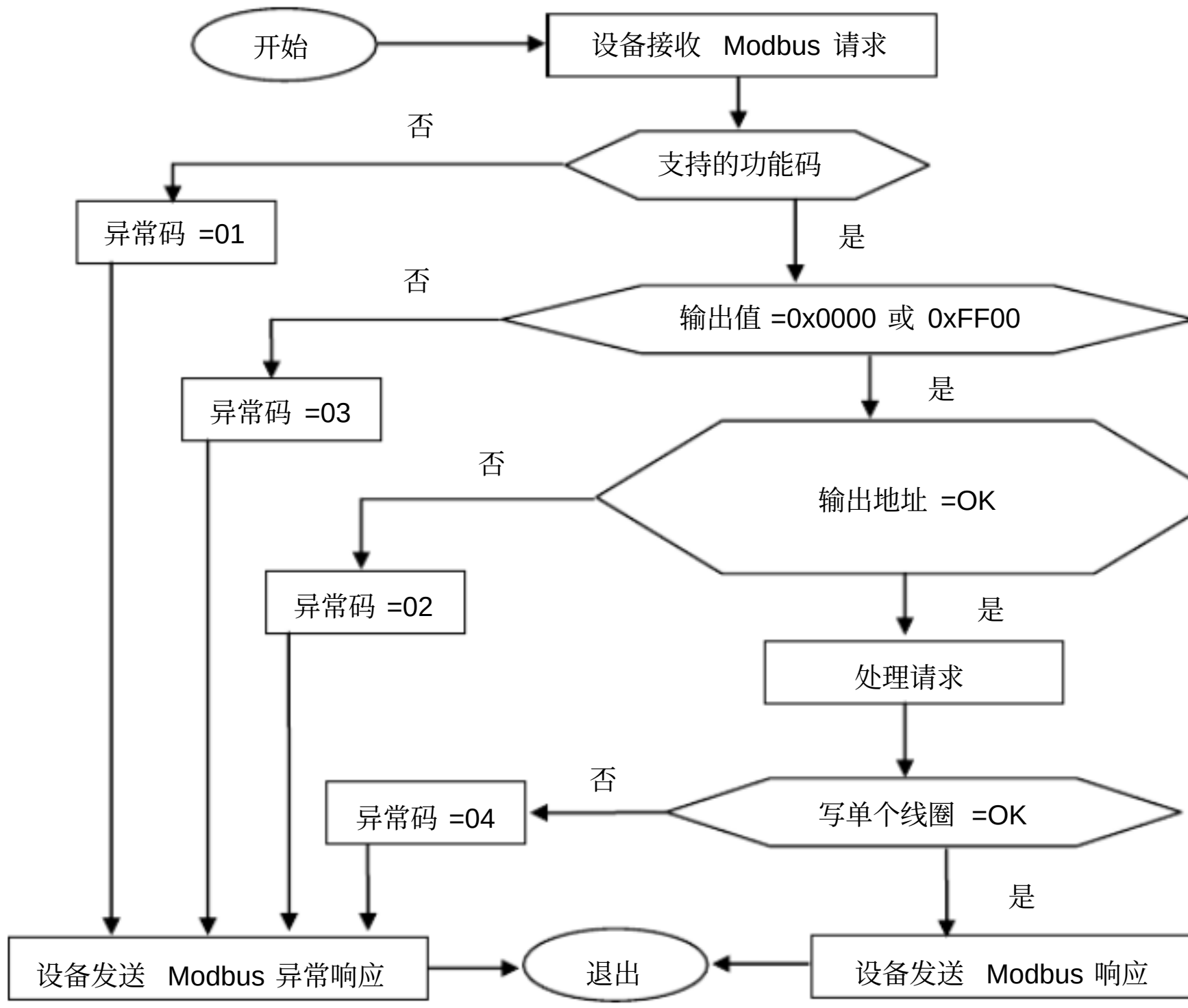


图 4.5 写单个线圈状态图

该功能码可将设备中的单个开关量 (继电器)输出状态写为 ON 或 OFF。

所请求的 ON/OFF 状态有请求数据字段中的常数指定。 十六进制值 FF 00 请求输出为 ON，十六进制值 00 00 请求输出为 OFF，其他所有值均是非法的，并且对输出不起作用。

请求 PDU 指定了被强制的线圈地址。在 PDU 中，从零开始寻址线圈，因此编号为 1 的线圈被寻址为 0。

正常的响应是请求的复制，在写入线圈状态后被返回。

表 4.20 是一个请求写线圈 173 为 ON 的示例。

表 4.20 写单个线圈

请求		响应	
字段名	十六进制	字段名	十六进制
功能	05	功能	05
起始地址 Hi	00	起始地址 Hi	00
起始地址 Lo	AC	起始地址 Lo	AC
输出数量 Hi	FF	输出数量 Hi	FF
输出数量 Lo	00	输出数量 Lo	00

4.6 06(0x06)写单个寄存器

功能码 06(0x06)用于写单个系统参数、模拟量输出值，如图 4.6 和表 4.21~4.23 所示：

表 4.21 写单个寄存器请求

功能码	1 字节	0x06
起始地址	2 字节	0x0000~0xFFFF
输出值	2 字节	0x0000~0xFFFF

表 4.22 写单个寄存器响应

功能码	1 字节	0x06
起始地址	2 字节	0x0000~0xFFFF
输出值	2 字节	0x0000~0xFFFF

表 4.23 写单个寄存器错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03 或 04

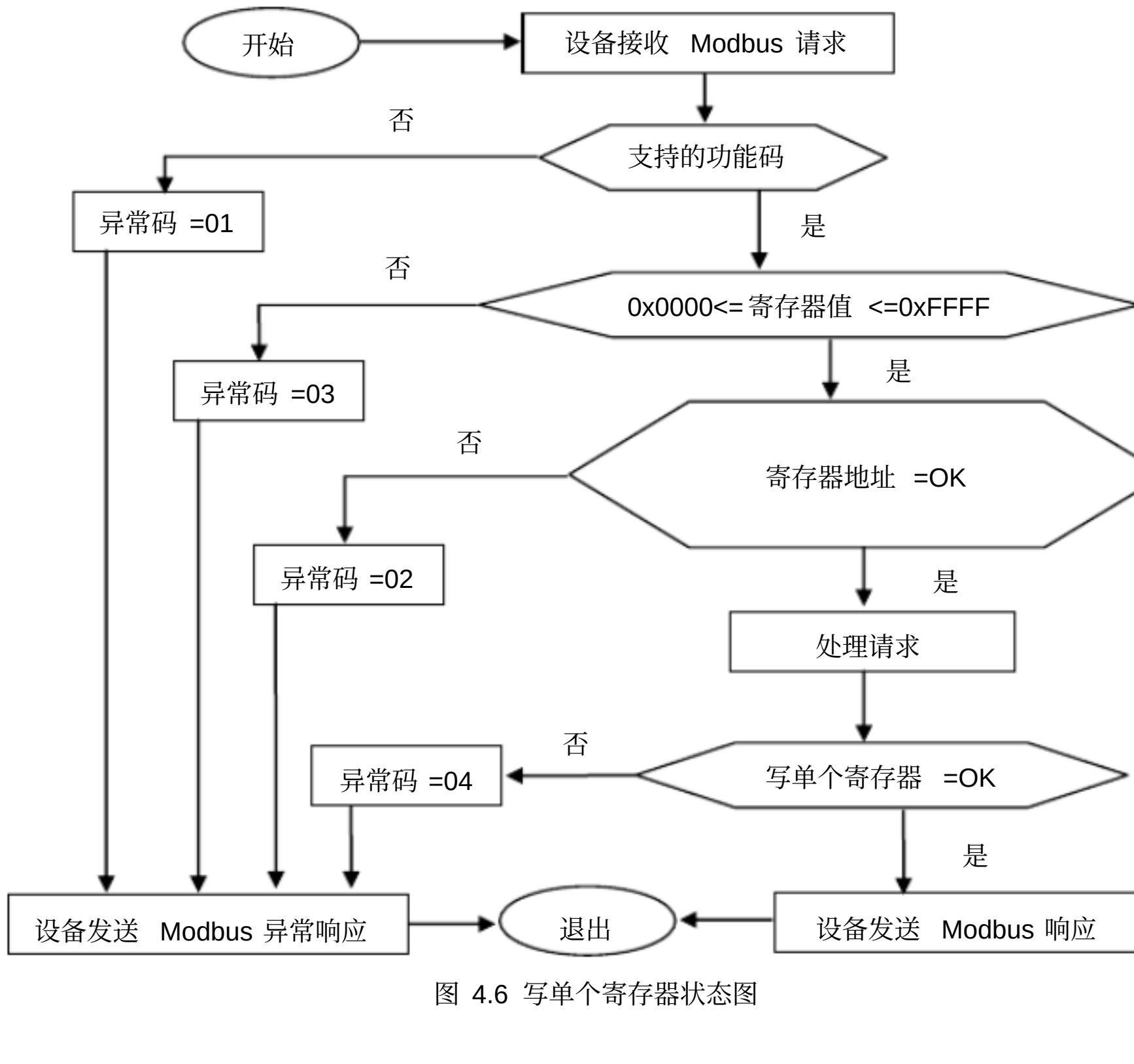


图 4.6 写单个寄存器状态图

该功能码可写设备中单个保持寄存器的内容。

请求 PDU 指定了被写入保持寄存器的地址。在 PDU 中，从零开始寻址寄存器，因此编号为 1 的保持寄存器被寻址为 0。

正常的响应是请求的复制，在写入保持寄存器后被返回。

表 4.24 是一个请求将十六进制 00 03 写保持寄存器 2 的示例。

表 4.24 写单个保持寄存器

请求		响应	
字段名	十六进制	字段名	十六进制
功能	06	功能	06
起始地址 Hi	00	起始地址 Hi	00
起始地址 Lo	01	起始地址 Lo	01
输出数量 Hi	00	输出数量 Hi	00
输出数量 Lo	03	输出数量 Lo	03

4.7 15(0x0F)写多个线圈

功能码 15(0x0F)用于写多个开关量 (继电器)输出状态，如图 4.7 和表 4.25~4.27 所示：

表 4.25 写多个线圈请求

功能码	1 字节	0x0F
起始地址	2 字节	0x0000~0xFFFF
输出数量	2 字节	0x0001~0x07B0
字节计数	1 字节	N
输出值	N*1 字节	
N=输出数量 /8，如果余数不等于 0，则 N=N+1。		

表 4.26 写多个线圈响应

功能码	1 字节	0x0F
起始地址	2 字节	0x0000~0xFFFF
输出数量	2 字节	0x0001~0x07B0

表 4.27 写多个线圈错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03 或 04

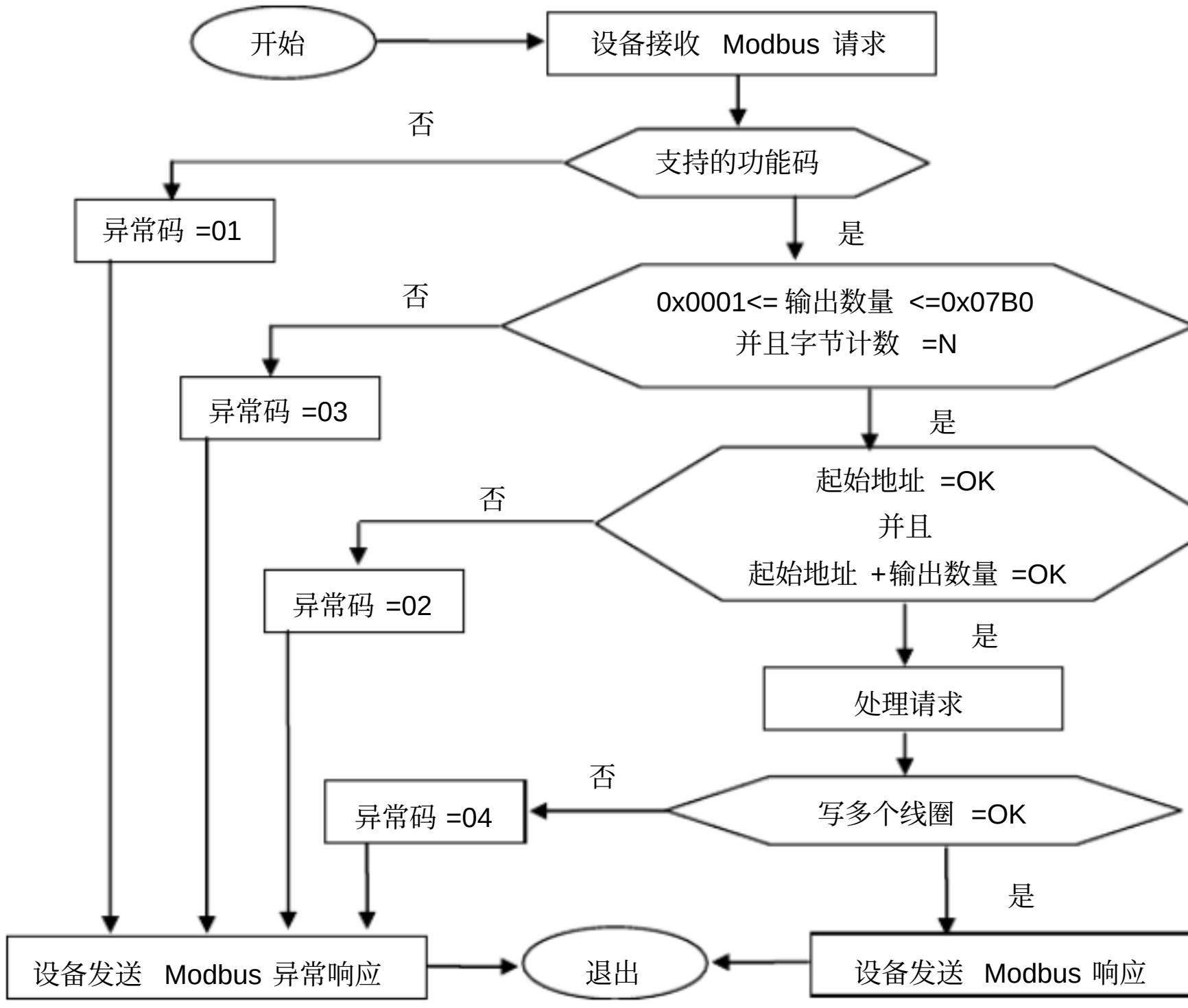


图 4.7 写多个线圈状态图

该功能码可将设备中的一个线圈状态序列的每一个线圈强制为 ON 或 OFF。

请求 PDU 指定了被强制的线圈引用， 且从零开始寻址线圈， 因此编号为 1 的线圈被寻址为 0。

请求数据字段中的内容指定了被请求线圈的 ON/OFF 状态。数据字段中为逻辑为 “ 1 ” 的位请求相应输出为 ON；为逻辑为 “ 1 ” 的位请求相应输出为 OFF。

正常的响应返回功能码、起始地址以及被强制的线圈数量。

表 4.28 是一个请求从线圈 20 开始写入 10 个线圈的示例。

表 4.28 写单个线圈

请求		响应	
字段名	十六进制	字段名	十六进制
功能	0F	功能	0F
起始地址 Hi	00	起始地址 Hi	00
起始地址 Lo	13	起始地址 Lo	13
输出数量 Hi	00	输出数量 Hi	00
输出数量 Lo	0A	输出数量 Lo	0A
字节计数	02		
输出值 Hi	CD		
输出值 Lo	01		

请求的数据内容为两个字节： 十六进制 CD 01(二进制 1100 1101 0000 0001)。二进制位按如下方式对应输出。

位	1	1	0	0	1	1	0	1	0	0	0	0	0	0	0	1
输出	27	26	25	24	23	22	21	20	-	-	-	-	-	-	29	28

传输的第一字节 (十六进制 CD)对应于输出 27~20， 最低有效位对应于最低输出 (20)。

传输的下一字节 (十六进制 01)对应于输出 29~28， 最低有效位对应于最低输出 (28)。应该用零填充最后数据字节中的未使用位。

4.8 16(0x10)写多个保持寄存器

功能码 16(0x10)用于写多个系统参数、模拟量输出值，如图 4.8 和表 4.29~4.31 所示：

表 4.29 写多个保持寄存器请求

功能码	1 字节	0x10
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	0x0001~0x007B
字节计数	1 字节	N*2
寄存器值	N*2 字节	值
N=寄存器数量		

表 4.30 写多个保持寄存器响应

功能码	1 字节	0x0F
起始地址	2 字节	0x0000~0xFFFF
寄存器数量	2 字节	1~123(0x007B)

表 4.31 写多个保持寄存器错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03 或 04

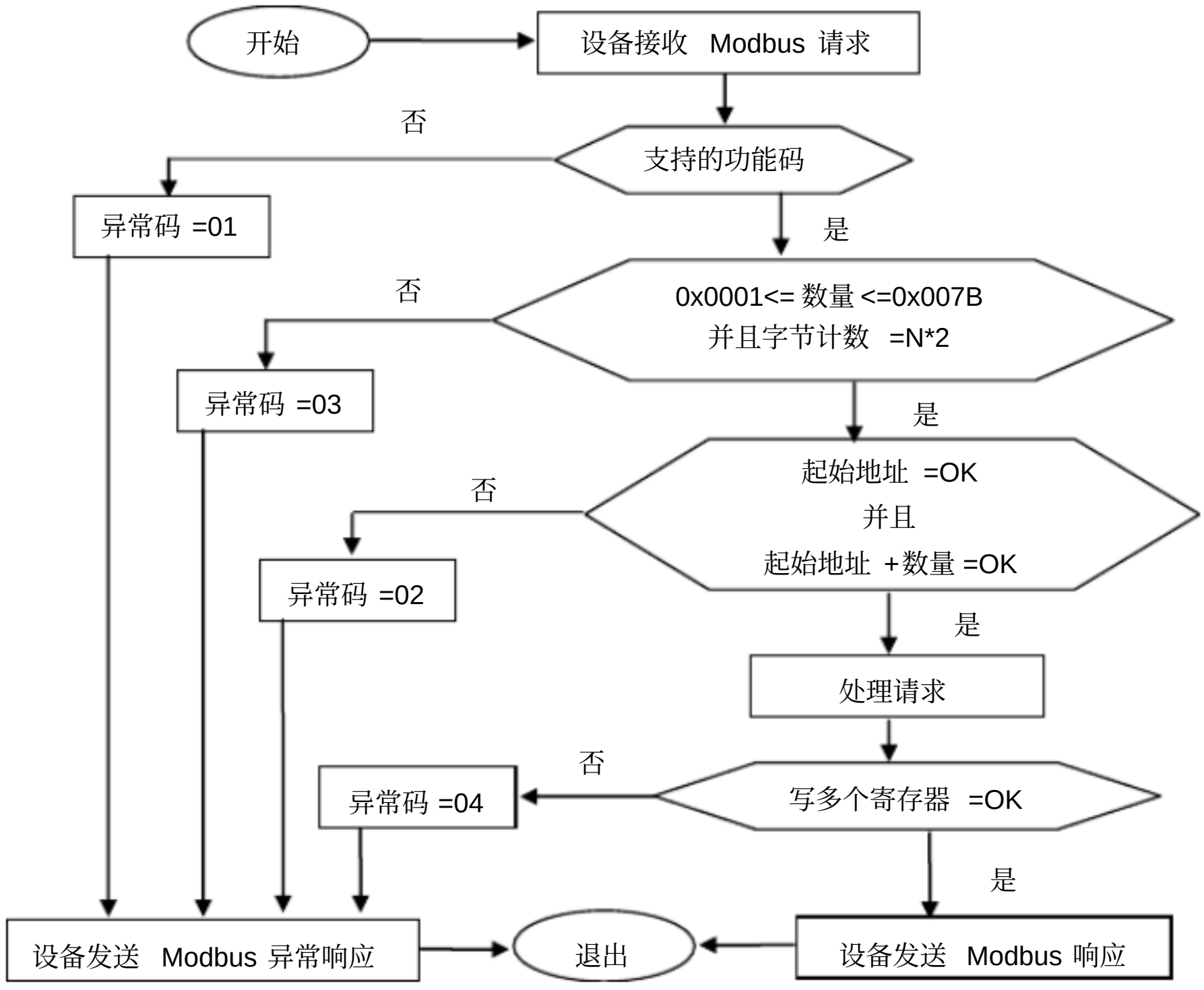


图 4.8 写多个寄存器状态图

该功能码可写设备中连续保持寄存器块　(1~123 个寄存器)的内容。

在请求数据字段中指定了请求写入的值并将数据按每个寄存器两字节打包。

正常的响应返回功能码、起始地址以及被写入寄存器的数量。

表 4.32 是一个请求将十六进制　00 0A 和 01 02 写入以第 2 个寄存器开始的两个寄存器的示例。

表 4.32 写入连续两个寄存器

请求		响应	
字段名	十六进制	字段名	十六进制
功能	10	功能	10
起始地址 Hi	00	起始地址 Hi	00
起始地址 Lo	01	起始地址 Lo	01
寄存器数量 Hi	00	输出数量 Hi	00
寄存器数量 Lo	02	输出数量 Lo	02
字节计数	04		
寄存器值 Hi	00		
寄存器值 Lo	0A		
寄存器值 Hi	01		
寄存器值 Lo	02		

4.9 43/14(0x2B/0x0E)读设备标识 **(**只支持单个设备标识的读取　**)**

功能码　43/14(0x2B/0x0E)用于读取与设备物理和功能描述相关的标识和附加信息，如图 4.9 和表 4.33~4.36所示：

读设备标识接口由包含一组可寻址数据元素组成的地址空间构成。　　数据元素被称作对象，有对象 ID 识别它们。

接口由 2 类对象组成：

——基本设备标识。该类别的所有对象都是强制的：厂商名称、产品代码和修订版本号。

——常规设备标识。除基本数据对象以外，设备提供了附加的和可选的标识以及数据对象描述。本部分定义了该类别的不分对象，但它们是可选的。

表 4.33 读设备标识

对象 ID	对象名称 /描述	类型	强制的 /可选的	类别
0x00	厂商名称	ASII 字符串	强制的	基本的
0x01	产品代码	ASII 字符串	强制的	
0x02	版本号	ASII 字符串	强制的	
0x03	厂商网址	ASII 字符串	可选的	常规的
0x04	产品名称	ASII 字符串	可选的	
0x05	型号名称	ASII 字符串	可选的	

表 4.34 读设备标识请求

功能码	1 字节	0x2B
MEI 类型	1 字节	0x0E
读设备 ID 码	1 字节	04
对象 ID	1 字节	0x00~0x06

表 4.35 读设备标识响应

功能码	1 字节	0x2B
MEI 类型	1 字节	0x0E
读设备 ID 码	1 字节	04
一致性等级	1 字节	0x81 或 0x82
连续标识	1 字节	00
下一个对象 ID	1 字节	00
对象数量	1 字节	1
列表		
对象 ID	1 字节	0x00/0x01/0x02 或 0x03/0x04/0x05
对象长度	1 字节	对象的字节长度
对象值	对象长度	对象值

表 4.36 读设备标识的错误响应

异常功能码	1 字节	功能码 +0x80
异常码	1 字节	01 或 02 或 03

请求参数描述：

Modbus 封装接口指配的的编号 14(0x0E)表示读标识请求。

参数“ 读设备 ID 码 ”定义的访问类型：

04：请求获得特定标识对象 (单个访问)。

若读设备 ID 码是无效的, 则在响应中返回异常码 03。

若对象 ID 不匹配任何已知对象 (0x00/0x01/0x02/0x03/0x04/0x05), 那么设备返回一个异常码=02(非法数据地址)的异常响应。

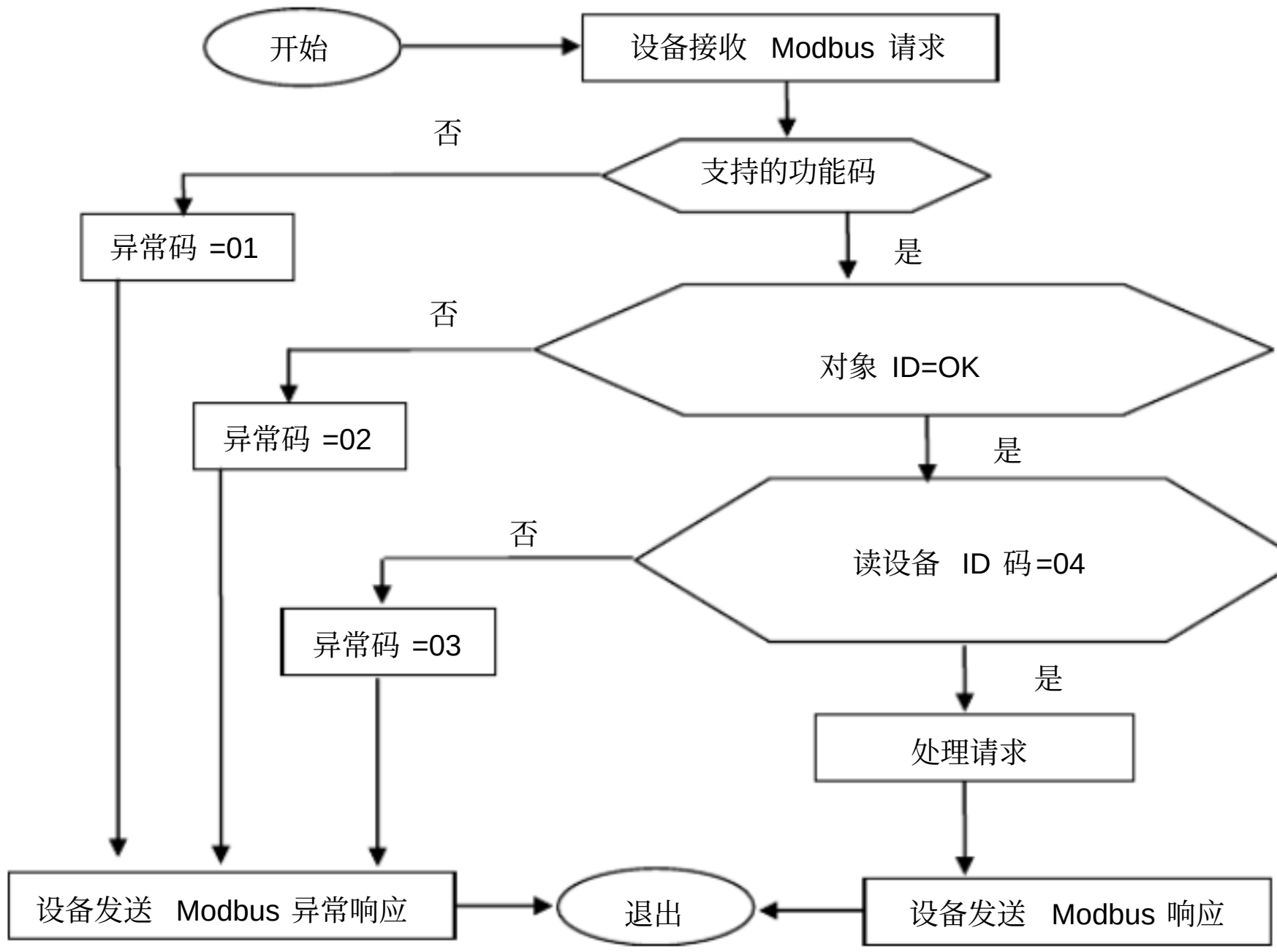


图 4.8 写多个寄存器状态图

响应参数描述：

功能码： 功能码 43(0x2B)

MEI 类型： 为设备标识接口指配的编号 MEI 类型 14(0x0E)

读设备 ID 码： 与请求读设备 ID 码相同： 04

一致性等级： 设备的标识一致性等级和支持的访问类型

0x81：基本标识 (流访问和单个访问)

0x82：常规标识 (流访问和单个访问)

接续标识： 00：没有后续的对象
下一个对象 ID ： 00
对象数目： 单个访问，对象数目 =1
对象 ID ： 请求的对象的标识
对象长度： 对象的字节长度
对象值： 对象的值 (对象长度字节)
表 4.37 是读取设备中厂商名称的示例。

表 4.37 读取厂商名称

请求		响应	
字段名	值	字段名	值
功能	2B	功能	2B
MEI 类型	0E	MEI 类型	0E
读设备 ID 码	04	读设备 ID 码	04
对象 ID	00	一致性等级	81
		接续标识	00
		下一个对象 ID	00
		对象数量	01
		对象 ID	00
		对象长度	09
		对象值	“ ColliHigh ”

注：产品信息

1.厂商名称： ColliHigh
2.产品代码：共 16 个字符
3.版本号：如“ V1.0 ”
4.厂商网址： www.klha.cn
5.产品名称：英文名称，首字母大写，单词之间用空格隔开
6.型号名称：产品型号

4.10 65(0x41)读标定参数及相关系统参数

该功能码用于读取设备的标定参数及相关系统参数，其使用方法和读保持寄存器的功能码 03(0x03)一样，请参照 03(0x03)功能码的使用介绍。

4.11 66(0x42)写多个标定参数及相关系统参数

该功能码用于写设备的标定参数及相关系统参数，其使用方法和写多个保持寄存器的功能码 16(0x10)一样，请参照 16(0x10)功能码的使用介绍。

五. Modbus 异常响应

当上位机向设备发送请求后可能导致下列 4 种事件之一：

——若设备接收到无通讯错误的请求，并可以正常的处理询问，则设备将返回一个正常响应。

——若由于通讯错误设备没有收到请求，则不能返回响应。上位机程序可按超时处理。

——若设备接收到请求，但是检测到一个通信错误 (奇偶校验、 LRC、CRC...)，则不能返回响应。上位机程序将按超时处理。

——若设备接收到无通信错误的请求，但不能处理这个请求 (例如，如果请求读一个不存在的输出或寄存器)，则设备将返回一个异常响应，通知上位机出错原因。

异常响应报文有两个与正常响应不同的字段：

1)功能码字段：正常的响应中，设备在响应的功能码字段复制原始请求的功能码。所有功能码的 MSB 都为 0(它们的值都低于 0x80)。在一场响应中，设备设置功能码的 MSB 为 1。这使得异常响应中的功能码值比正常响应中的功能码值高 0x80。
通过设置功能码的 MSB，上位机的应用程序能够识别异常响应，并且能够检测异常码的数据字段。

2)数据字段：在正常的响应中设备可以在数据字段中返回数据或统计值 (请求中要求的任何信息)。在异常响应中设备在数据字段中返回异常码，表明了设备产生异常的原因。

表 5.1 列出了异常码

表 5.1 异常码

Modbus 异常码		
代码	名称	含义
01	非法功能	对于设备来说，询问中接收到的功能码是不准许的
02	非法数据地址	对于设备来说， 询问中接收到的数据地址是不准许的地址。 特别是寄存器编号和传输长度的组合是无效的。
03	非法数据值	对于设备来说， 询问数据字段中包含的数不准许的值。 它表示组合请求中剩余部分结构方面的错误， 例如隐含长度不正确。 它绝不表示寄存器中被提交存储的数据项有一个应用程序之外的值， 因为 Modbus 协议并不知道任何特殊的寄存器的任何特殊值的具体含义。
04	从站设备故障	当设备正在试图执行所请求的操作时，产生不可恢复的差错。

六. Modbus 协议在串行链路上的实现规范

本部分描述串行链路上的 Modbus 协议。Modbus 串行链路协议是一个主 -从协议。该协议位于 OSI 模型的第 2 层。主——从类型的系统有一个主节点 (主站)，它向某个从节点 (从站)发出命令并处理响应。从站在没有收到主站的请求时并不主动的传输数据，也不与其他从站通信。在物理层，串行链路上的 Modbus 系统可以使用不同的物理接口 (RS485、RS232)。

6.1 Modbus 主/从协议原理

Modbus 串行链路协议是一个主 -从协议。在同一时间，总线上只能有一个主站和一个或多个(最多 247 个)从站。 Modbus 通信总是有主站发起，当从站没有收到来自主站的请求时，不会发送数据。从站之间不能相互通信。主站同一时间只能启动一个 Modbus 事物处理。

主站用单播模式 (暂不支持广播模式)向从站发出 Modbus 请求：

——主站寻址单个从站，从站接收并处理完请求后向主站返回一个报文 (应答)。

在这种模式下，一个 Modbus 事务处理包含 2 个报文：一个主站请求；一个从站应答。每个从站必须有唯一的地址 (1~247)，这样才能区别于其他站独立被寻址。

6.2 Modbus 寻址规则

如表 6.1 所示，Modbus 寻址空间由 256 个不同的地址组成， 地址 0 为广播地址 (暂不支持)，主站没有特定地址，只有从站有唯一的一个地址。

表 6.1 Modbus 寻址范围

0	1~247	248~255
广播地址	从站地址	保留

6.3 Modbus 帧描述

Modbus 应用协议定义了一个与下层通信无关的简单协议数据单元 (PDU)，如图 6.1 所示：

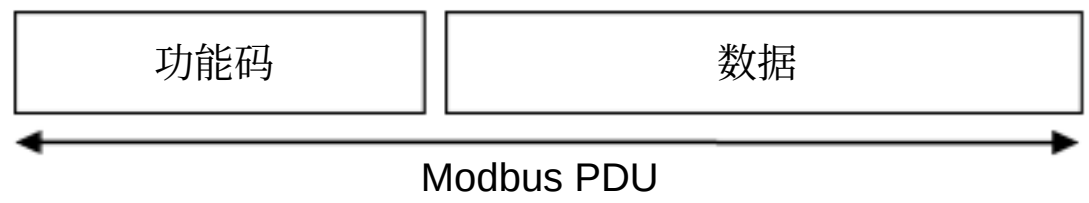


图 6.1 Modbus 协议数据单元

通过在协议数据单元 (PDU)上增加一些附加字段完成 Modbus 协议到具体总线或网络的映射，启动 Modbus 事务处理的上位机构造成 Modbus PDU，然后添加附加字段， 一般构成相应的通信 PDU，如图 6.2 所示：

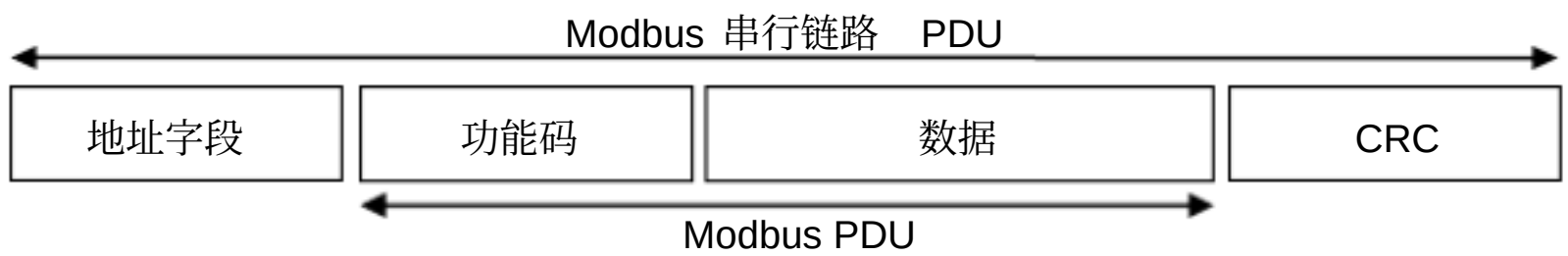


图 6.2 串行链路上的 Modbus 帧

——在 Modbus 串行链路上地址字段只含有从站地址。

主站将从站地址放置在报文的地址字段中来寻址从站。当从站返回响应时，它将自己的地址放到响应地址字段中，以便使主站知道那个从站正在响应。

——功能码指示设备要执行何种操作。 功能码的后面是含有请求或响应参数的数据字段。

——差错检验字段是根据报文内容执行“ 冗余校验 ”计算的结果。

6.4 主站 /从站状态图

Modbus 数据链路层由两个独立子层组成：

——主 /从协议；

——传输模式 (只支持 RTU 模式)。

6.4.1 主站状态图

图 6.3 说明了主站的行为：

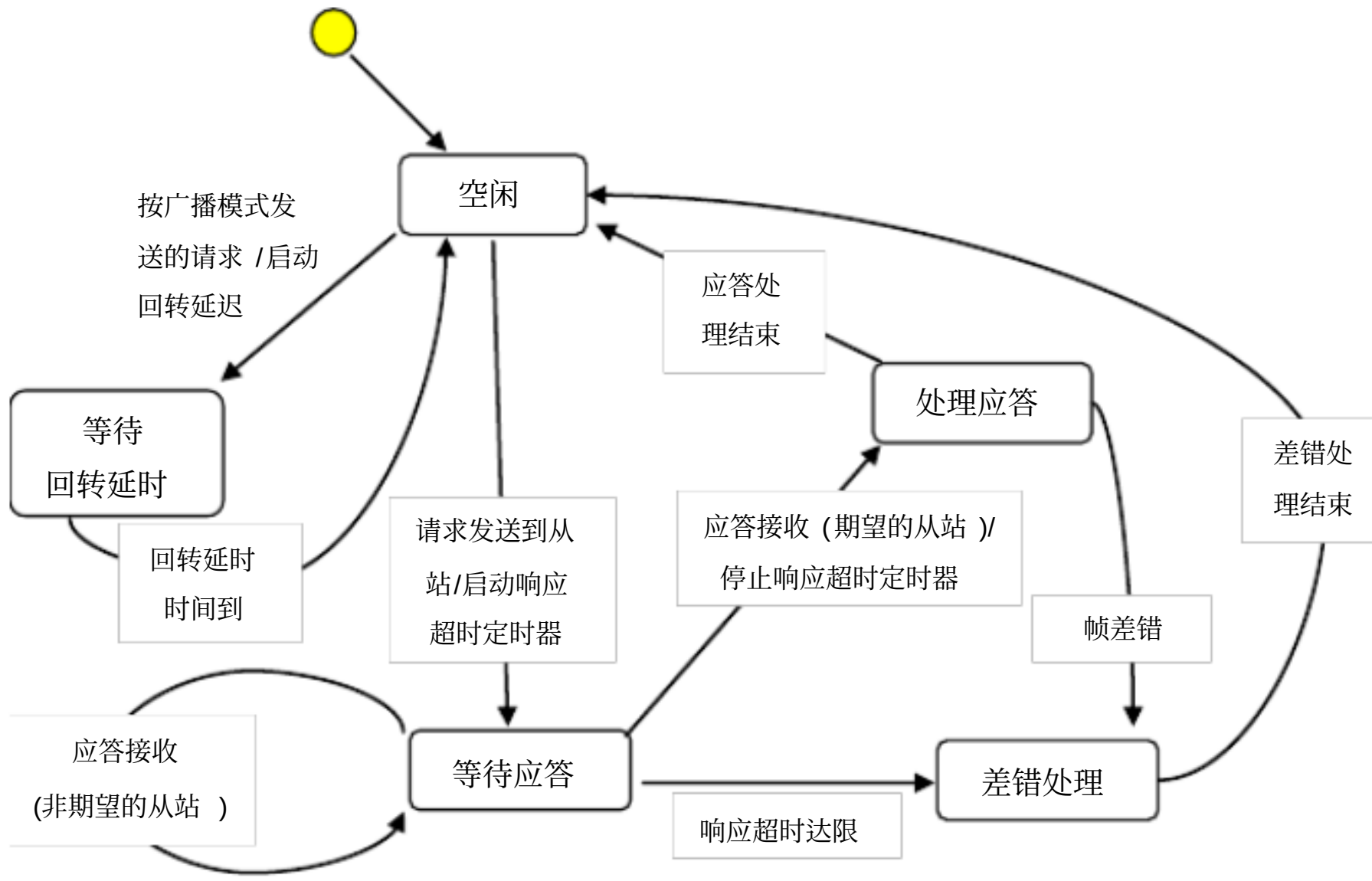


图 6.3 主站状态图

——状态“ 空闲 ” =无挂起请求。这是电源加电后的初始状态。只有在“ 空闲 ”状态下才能发送请求。发送一个请求后，主站离开“ 空闲 ”状态，并且不能同时发送第二个请求。

——当向从站发送单播请求时，主站将进入“ 等待应答 ”状态，并且启动一个“ 响应超时 ”定时器。它防止主站无限期地停留在“ 等待应答 ”状态下。响应超时的时间与具体应用有关。

——当收到一个应答时，主站在处理数据之前检验应答。在某些情况下，检验的结果发现错误，例如：收到来自非期望从站的应答或在接收到的帧中有错误。当收到来自非期望从站的应答时，响应超时继续计时。如果在帧上检测到差错，可以进行重试。

——如果没有接收到应答，响应超时时间到，产生一个错误。然后，主站进入“ 空闲 ”

状态，并发出一个重试请求。重试的最大次数与主站设置有关。

——当在串行总线上发送广播请求时，从站不返回响应 (暂不支持广播模式)。然而，主站需要考虑延迟，以便再发送信的请求之前准许从站处理当前请求。这个延迟被称作“ 回转延迟 ”。因此，在返回“ 空闲 ”状态并且能够发送另一个请求之前， 主站进入“ 等待回转延迟 ”状态。

——在单播模式下，必须设置足够长的响应超时时间，以便从站处理请求并返回响应；在广播模式下，必须有足够长的回转延迟，以便从站处理请求并能够接收到新请求。因此，回转延迟应该比响应超时短。 通信速率在 9600bit/s 时，典型的响应超时值为 1s 到几秒，而回转延迟为 100ms~200ms。

——帧错误校验包括：每个字符的奇偶校验；整个帧的冗余校验。

6.4.2 从站状态图

图 6.4 说明了从站的行为：

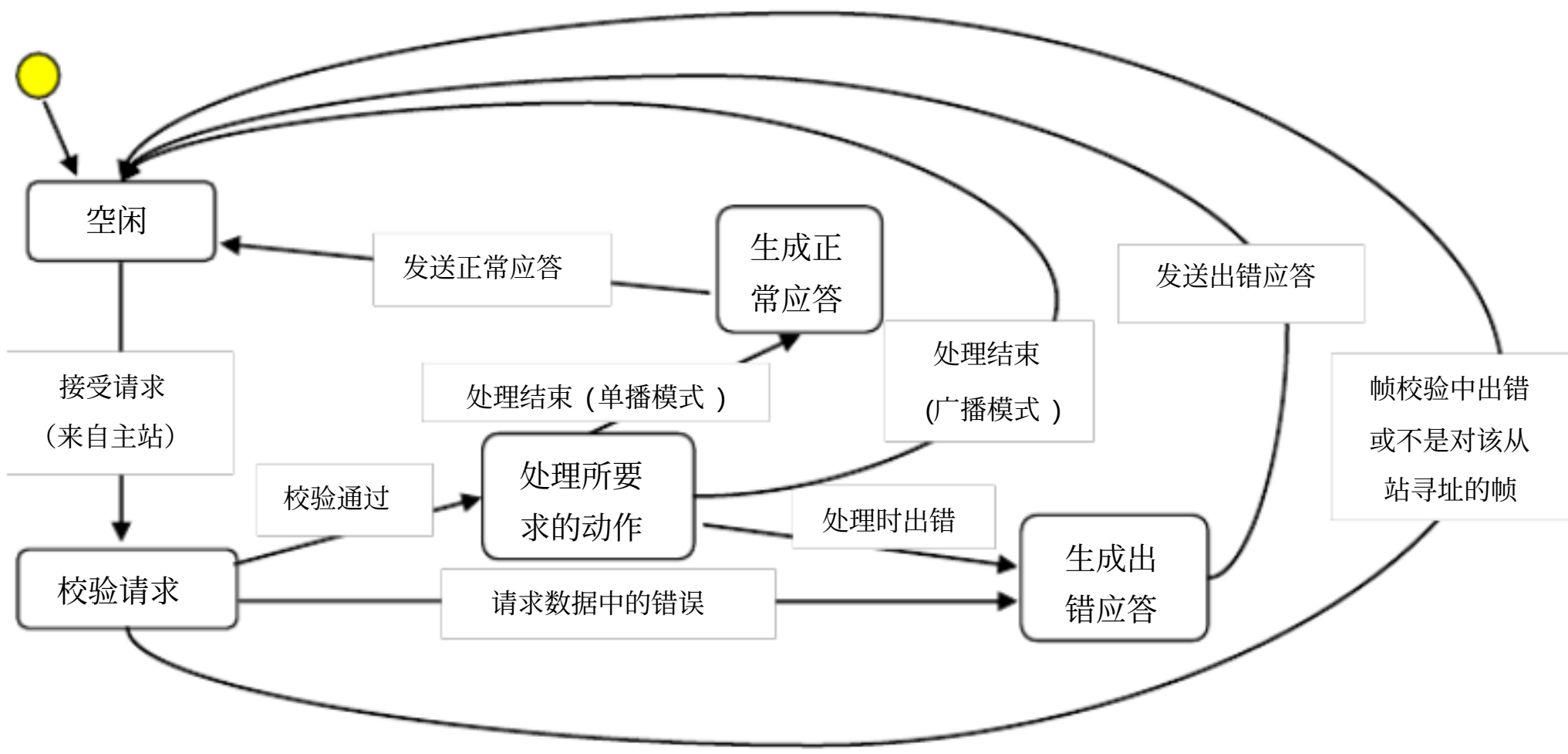


图 6.4 从站状态图

——状态“ 空闲 ” =无提起请求。这是设备上电后的初始状态。

——当收到一个请求时，在处理报文包中所请求的动作之前，从站校验报文包，可能出现不同的错误：如请求的格式错误、无效动作等。当检测到错误时，必须向主站发送应答。

——一旦完成请求的动作，单播报文要求必须生成应答并将其发送给主站。

——如果从站检测到接收帧中的错误，那么不向主站返回相应。

6.5 串行传输模式

本标准暂时只支持一种串行传输模式： RTU 模式。

RTU 模式中的每个字符 (11 位)的格式为：

编码系统： 8 位二进制

每个字节的位： 1 个起始位

8 个数据位，首先发送最低有效位

1 个奇偶校验位

1 个停止位

要求使用偶校验，也可使用其他模式 (奇校验、无校验)。为了保证与其他产品的最大兼容性，建议还支持无校验模式。默认校验模式是偶校验。

注：使用无校验时要求 2 个停止位。

穿行的传送字符的方法为：发送每个字符或字节的顺序是从左到右，见表 6.2。

最低有效位 (LSB).....最高有效位 (MSB)

表 6.2 RTU 模式中的位序列

带奇偶校验										
起始	1	2	3	4	5	6	7	8	校验	停止

通过配置，设备可以接受奇校验、偶校验或无校验。如果无校验，那么传送一个附加的停止位来填充字符帧使其成为完整的 11 位异步字符，见表 6.3

表 6.3 RTU 模式中的位序列 (无校验)

带奇偶校验										
起始	1	2	3	4	5	6	7	8	停止	停止

帧校验字段：循环冗余校验 (CRC)

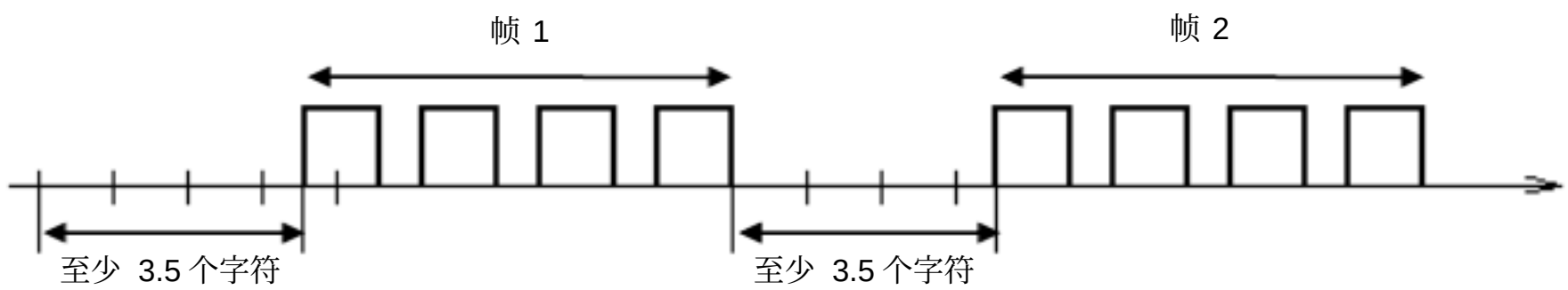
帧描述：

从站地址	功能码	数据	CRC	
1 字节	1 字节	0~252 字节	2 字节	
			低字节	高字节

Modbus RTU 帧最大长度是 256 个字节。

6.5.1 Modbus 报文 RTU 帧

在 RTU 模式中，时长至少为 3.5 个字符时间的空闲间隔将报文帧区分开，这个时间间隔成为 $t_{3.5}$，见图 6.5。



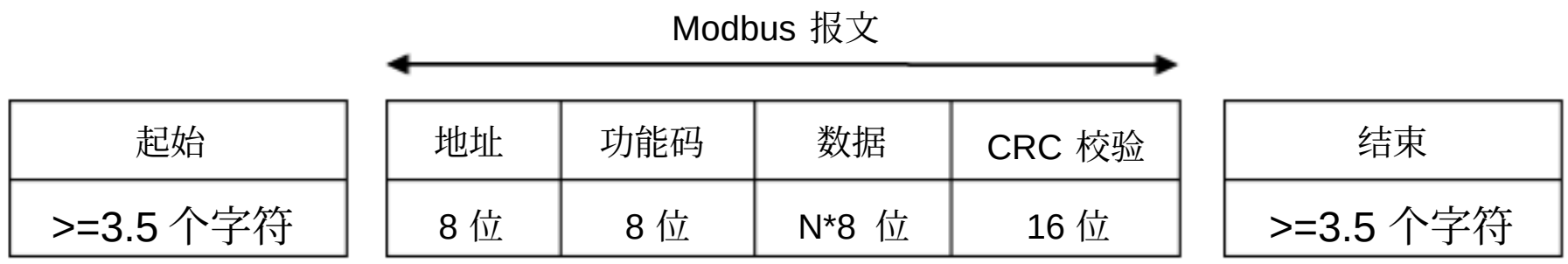


图 6.5 RTU 报文帧

必须已连续的字符流发送整个报文帧。

如果两个字符之间的空闲间隔大于 1.5 个字符时间 ($t_{1.5}$)，那么认为报文帧不完整，并且接收站应该丢弃这个报文帧，见图 6.6。

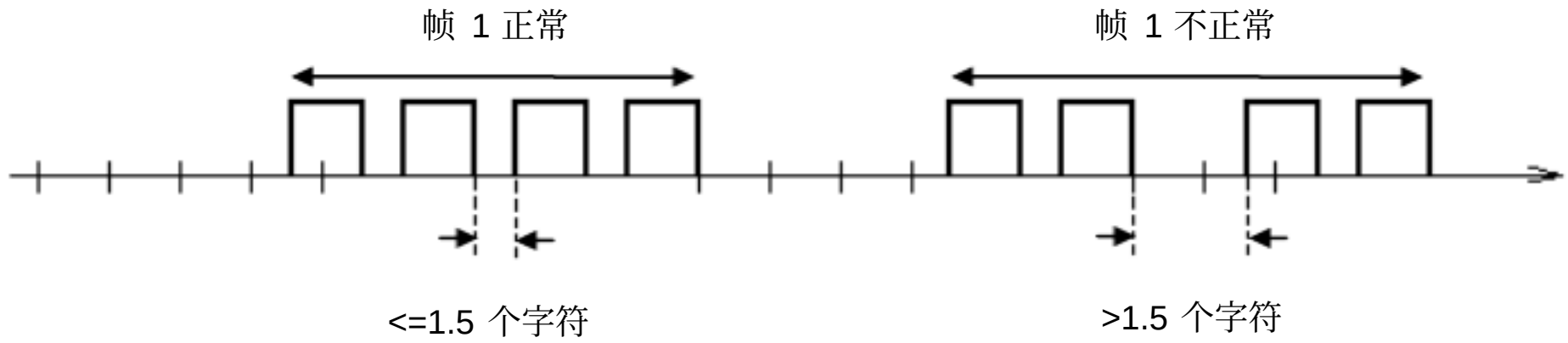


图 6.6 Modbus 帧内间隔

注：实现了 RTU 接收的驱动程序会隐含着对由 $t_{1.5}$ 和 $t_{3.5}$ 定时器引起的大量中断的管理。在较高的通信波特率下这将导致 CPU 负担加重，因此当波特率等于或低于 19200bit/s 时，必须严格遵守这两个定时；波特率大于 19200bit/s 的情况下，两个定时器宜使用固定值，建议字符间超时时间 ($t_{1.5}$)为 750us，帧间的延迟时间 ($t_{3.5}$)为 1.75ms。

6.5.2 CRC 校验

RTU 模式包含一个差错校验字段，该字段是基于循环冗余校验 (CRC)方法对全部报文内容执行的。

CRC 字段校验整个报文的内容。无论单个字符报文使用何种奇偶校验方式，均应用这种校验。 CRC 校验字段为两个字节，包括一个二进制 16 位值。发送设备计算 CRC 值，并将其附加到报文中。在接收过程中，接收设备重新计算 CRC 值，并将计算值于收到的 CRC 字段中实际值相比较，如果两个值不相等，则说明报文有错误。

通过对一个 16 位寄存器预装载全“ 1 ”来启动 CRC 计算，然后开始将报文中的后续 8 为字节与当前寄存器中的内容进行计算，只有每个字符中的 8 个数据位参与生成 CRC 的计算，起始位、停止位和校验位不参与 CRC 计算。

在生成 CRC 过程中，每个 8 位字符与寄存器中的值异或，然后，向最低有效位 (LSB)方向移动这个结果，而用零填充最高有效位 (MSB)，提取并检查 LSB，如果 LSB 为 1，则寄存器中的值与一个固定的预置值异或；如果 LSB 为 0，则不进行异或操作。

这个过程将重复直到执行完 8 次移位，完成最后一次 (第 8 次)移位之后，下一个 8 位字节与寄存器的当前值异或，然后像上述描述的那样重复 8 次这个过程。在已经计算报文中所有字节之后，寄存器的最终值就是 CRC。

生成一个 CRC 的过程是：

a) 将十六机制 FFFF(全 1)装入一个 16 位寄存器。将这个寄存器称作 CRC 寄存器。

b) 将报文的第一个 8 位字节与 16 位 CRC 寄存器的低字节异或， 将结果放置在 CRC 寄存器中。

c) 将 CRC 寄存器右移 1 位(向 LSB 方向)， MSB 填充零。提取并检测 LSB。

d) 若 LSB 为 0 则重复步骤 c)；若 LSB 为 1 则将 CRC 寄存器与多项式值 0xA001 异或。

e) 重复步骤 c)和 d)，直到完成 8 次移位。在完成这个操作之后，即完成了对一个完整的 8 位字节的处理。

f) 对报文的下一个 8 位字节重复步骤 b)~e)。继续进行这种操作，直到处理报文中的所有字节为止。

g) CRC 寄存器中的最终内容为 CRC 值。

h) 当将 CRC 值放置到报文中时，必须把低字节放在前面，高字节放在后面，如图 6.7 所示。

例如：如果 CRC 值为十六进制 1241，见图 6.7。

地址	功能码	数据计数	数据	数据	数据	数据	CRC 低位	CRC 高位
							0x41	0x12

图 6.7 CRC 字节序列