

ECtox 气体侦测器

Modbus-RTU 通信协议



目 录

1. 编写目的.....	1
2. 基本定义.....	1
2.1 上位机.....	1
2.2 下位机.....	1
2.3 通信方式.....	1
3. 接口可选方案.....	1
3.1 对下位机.....	1
3.2 对上位机.....	1
4. Modbus通信协议基础知识.....	2
4.1 Modbus通信协议的简要说明.....	2
4.1.1 Modbus通信协议报文的基本格式.....	2
4.1.2 Modbus通信协议的数据模型.....	2
4.1.3 Modbus通信协议常用的功能码解析.....	2
4.1.4 Modbus地址.....	2
4.1.5 Modbus Master 协议库支持的功能.....	3
4.2 Modbus通信协议常用功能码的报文格式及举例.....	3
4.2.1 01 读取线圈状态 MODBUS地址 00001~.....	3
4.2.2 02 读取输入状态 MODBUS地址 10001~.....	4
4.2.3 03 读保持寄存器 MODBUS地址 40001~.....	5
4.2.4 04 读输入寄存器 MODBUS地址 30001~.....	5
4.2.5 05 设置单个继电器状	6
4.2.6 06 设置单个保持寄存.....	7
4.2.7 15 设置多个继电器状态.....	8
4.2.8 16 设置多个保持寄存器.....	9
5. 通信协议.....	10
5.1 特殊指令用于修改用户Modbus协议地址.....	10
5.2 Modbus功能码已实现功能.....	10
5.3 寄存器-数据对应表.....	11
5.4 读取数据返回错误码.....	11
5.5 软件版本号读取.....	12

编写目的

为了实现MCU电路模块与PC机、PLC等设备进行数据传输，制定本通讯协议。

基本定义

上位机

即通信过程中的主机，例如PC机、PLC、DCS等。用于实现从MCU电路板获取参数和检测数据，可以将标定的相关参数和被测气体信息下发至MCU电路板，并进行参数调整和存储记录；还可以调试传感器所需参数和MCU电路板的性能参数。

下位机

即通信过程中的从机，如MCU电路板、终端设备等。用于实现基本的测量、参数设置功能，接受上位机下发的读写命令，向上位机传送数据。

通信方式

采用串口异步半双工应答式通信，即下位机不主动上发数据，当接收到上位机发送的命令之后才给上位机发送数据。

接口可选方案

对下位机

凡是可采用串口异步半双工通信方式的物理层接口电路均可采用此协议；建议采用标准485通信接口。（最终要求通信双方直接对接的接口必须一致）

对上位机

建议采用标准485通信接口；（最终要求通信双方直接对接的接口必须一致）

采用232通信接口转485通信接口方式；

采用USB通信接口转485通信接口方式；

采用USB通信接口转232通信接口再转485通信接口方式。

注：

串口设置：波特率9600bps,8位数据位，1位起始位，1位停止位,无奇偶校验位。

上位机与下位机以数据包的形式，采用问答方式通讯。首先由上位机向下位机发送命令数据包，然后下位机向上位机返回应答数据包或返回错误代码。

Modbus 通信协议基础知识

Modbus 通信协议的简要说明

• Modbus 通信协议报文的基本格式

标准 Modbus 通信协议的报文包括地址域、功能码、数据区、循环冗余校验。报文的基本格式如下：

起始位	地址域	功能码	数据区	CRC循环冗余校验	结束符
T1 T2 T3 T4	8bits	8bits	N*8bits	16bits	T1 T2 T3 T4

• Modbus 通信协议的数据模型

Modbus 协议是以一系列具有不同特征表格上的数据模型为基础，四个基本表格如下：

基本表格	对象类型	访问类型	内 容
线圈	单个比特，位数据	只 读	I/O系统提供这种类型数据
输入状态	单个比特，位数据	读 写	通过应用程序改变这种数据
输入寄存器	16个比特，字	只 读	I/O系统提供这种类型数据
保持寄存器	16个比特，字	读 写	通过应用程序改变这种数据

• Modbus 通信协议常用的功能码解析

功能码	名 称	作 用
01 (0x01)	读取线圈状态	取得一组逻辑线圈的当前状态 (ON/OFF)
02 (0x02)	读取输入状态	取得一组开关输入的当前状态 (ON/OFF)
03 (0x03)	读取保持寄存器	在一个或多个保持寄存器中取得当前的二进制值
04 (0x04)	读取输入寄存器	在一个或多个输入寄存器中取得当前的二进制值
05 (0x05)	强置单线圈	强置一个逻辑线圈的通断状态
06 (0x06)	预置单保持寄存器	把具体二进制值装入一个保持寄存器
15 (0x0f)	强置多线圈	强置一串连续逻辑线圈的通断
16 (0x10)	预置多保持寄存器	把具体的二进制值装入一串连续的保持寄存器

• Modbus 地址

通常 Modbus 地址由 5 位数字组成，包括起始的数据类型代号，以及后面的偏移地址。

Modbus Master 协议库把标准的 Modbus 地址映射为所谓 Modbus 功能号，读写从站的数据。

Modbus Master 协议库支持如下地址：

00001 – 09999: 线圈	可读写位数据的数字量输入、输出
10001 – 19999: 输入状态	只读位数据的数字量输入
30001 – 39999: 输入寄存器	只读字数据的模拟量输入
40001 – 49999: 保持寄存器	可读写字数据的模拟量输入、输出

• Modbus Master 协议库支持的功能

为了支持 Modbus 地址的读写, Modbus Master 协议库需要从机支持下列功能:

Modbus 地址	访问方式 (读或写)	Modbus 从站须支持的功能 (常用功能码)
00001 – 09999: 线圈	读	0x01: 读取线圈状态
	写	0x05: 强置单线圈 0x0f: 强置多线圈
10001 – 19999: 输入状态	读	0x02: 读取输入状态
	读	0x04: 读取输入寄存器
40001 – 49999: 保持寄存器	读	0x03: 读取保持寄存器
	写	0x06: 预置单保持寄存器 0x10: 预置多保持寄存器

Modbus 通信协议常用功能码的报文格式及举例

• 01 读取线圈状态 MODBUS地址 00001~

MODBUS 请求

功能码	起始地址	读取数量
1 BYTE	2 BYTE	2 BYTE
0X01	0X0000 TO 0xFFFF	1 TO 2000(0X7D0)

MODBUS 响应

功能码	字节计数	线圈状态
1 BYTE	1 BYTE	n BYTE
0X01	N	n =N or N+1

N =读取数量/8 如果余数不为0 则N=N+1

错误 响应

功能码	错误代码
1 BYTE	1 BYTE
0X01+ 0X80	0x01~0x07

举 例

请 求		响 应	
域名称	数据 (hex)	域名称	数据 (hex)
功能码	01	功能码	01
起始地址高(字节)	00	字节计数	03
起始地址低(字节)	13	27 (h) ~20状态	CD
读取数量高(字节)	00	35 (h) ~28状态	6B
读取数量低(字节)	13	38 (h) ~36状态	05

• 02 读取输入状态 MODBUS地址 10001~

MODBUS 请求

功能码	起始地址	读取数量
1 BYTE	2 BYTE	2 BYTE
0X02	0X0000 TO 0xFFFF	1 TO 2000(0X7D0)

MODBUS 响应

功能码	字节计数	输入状态
1 BYTE	1 BYTE	n BYTE
0X02	N	n =N or N+1

N =读取数量/8 如果余数不为0 则N=N+1

错 误 响 应

功能码	错误代码
1 BYTE	1 BYTE
0X02+ 0X80	0x01~0x07

举 例

请 求		响 应	
域名称	数据 (hex)	域名称	数据 (hex)
功能码	02	功能码	02
起始地址高(字节)	00	字节计数	03
起始地址低(字节)	C4	204(h)~197状态	AC
读取数量高(字节)	00	212(h)~205状态	DB
读取数量低(字节)	16	218(h)~213状态	35

• 03 读保持寄存器 MODBUS地址 40001~

MODBUS 请求

功能码	起始地址	读取数量
1 BYTE	2 BYTE	2 BYTE
0X03	0X0000 TO 0xFFFF	1 TO 125 (0X7D)

MODBUS 响应

功能码	字节计数	数 �据
1 BYTE	1 BYTE	N*2 BYTE
0X03	N*2	/

错误 响应

功能码	错误代码
1 BYTE	1 BYTE
0X03+ 0X80	0x01~0x07

举 例

请 求	响 应
域名称	数据 (hex)
功能码	03
起始地址高(字节)	00
起始地址低(字节)	6B
读取数量高(字节)	00
读取数量低(字节)	03
	域名称
	数据 (hex)
	功能码
	03
	字节计数
	06
	寄存器高 (108)
	02
	寄存器低 (108)
	2B
	寄存器高 (109)
	00
	寄存器低 (109)
	00
	寄存器高 (110)
	00
	寄存器低 (110)
	64

• 04 读输入寄存器 MODBUS地址 30001~

MODBUS 请求

功能码	起始地址	读取数量
1 BYTE	2 BYTE	2 BYTE
0X04	0X0000 TO 0xFFFF	1 TO 125 (0X7D)

ECtox 气体侦测器 Modbus-RTU 通信协议

Easy Gas Detection Device Innovations

MODBUS 响应

功能码	字节计数	输入状态
1 BYTE	1 BYTE	N*2 BYTE
0X04	N*2	/

错误 响应

功能码	错误代码
1 BYTE	1 BYTE
0X04+ 0X80	0x01~0x07

举例

请求	响应
域名称	数据 (hex)
功能码	04
起始地址高(字节)	00
起始地址低(字节)	08
读取数量高(字节)	00
读取数量低(字节)	01
域名称	数据 (hex)
功能码	04
字节计数	02
输入寄存器高 (9)	00
输入寄存器低 (9)	0A

• 05 设置单个继电器状态

MODBUS 请求

功能码	设置地址	设置内容
1 BYTE	2 BYTE	2 BYTE
0X05	0X0000 TO 0XFFFF	0x0000 OR 0xFF00 0x0000 释放继电器 0xff00 吸合继电器

MODBUS 响应

功能码	设置地址	设置内容
1 BYTE	2 BYTE	2 BYTE
0X05	0X0000 TO 0xFFFF	0x0000 OR 0xFF00

错误 响应

功能码	错误代码
1 BYTE	1 BYTE
0X05+ 0X80	0x01~0x07

举 例 (吸合6号继电器)

请 求	响 应
域名称	数据 (hex)
功能码	05
设置地址高(字节)	00
设置地址低(字节)	05
设置内容高(字节)	FF
设置内容低(字节)	00

• 06 设置单个保持寄存器

MODBUS 请求

功能码	设置地址	设置内容
1 BYTE	2 BYTE	2 BYTE
0X06	0X0000 TO 0xFFFF	0x0000 TO 0xFF00

MODBUS 响应

功能码	设置地址	设置内容
1 BYTE	2 BYTE	2 BYTE
0X06	0X0000 TO 0xFFFF	0x0000 TO 0xFF00

错误 响应

功能码	错误代码
1 BYTE	1 BYTE
0X06+ 0X80	0x01~0x07

ECtox 气体侦测器 Modbus-RTU 通信协议

Easy Gas Detection Device Innovations

举 例 (设置9号保持寄存器内容为25)

请 求		响 应	
域名称	数据 (hex)	域名称	数据 (hex)
功能码	06	功能码	06
设置地址高(字节)	00	设置地址高(字节)	00
设置地址低(字节)	08	设置地址低(字节)	08
设置内容高(字节)	00	设置内容高(字节)	00
设置内容低(字节)	19	设置内容低(字节)	19

• 15 设置多个继电器状态

MODBUS 请求

功能码	设置起始地址	设置长度	字节计数	设置内容
1 BYTE	2 BYTE	2 BYTE	1 BYTE	N BYTE
0X0F	0X0000 TO 0XFFFF	0X0000 TO 0X7B0	N	

MODBUS 响应

功能码	设置起始地址	设置长度
1 BYTE	2 BYTE	2 BYTE
0X0F	0X0000 TO 0XFFFF	0X0000 TO 0X7B0

错误 响应

功能码	错误代码
1 BYTE	1 BYTE
0X0F+ 0X80	0x01~0x07

举 例 (设置1~4号继电器吸合)

请 求		响 应	
域名称	数据 (hex)	域名称	数据 (hex)
功能码	0F	功能码	0F
设置地址高(字节)	00	设置地址高(字节)	00
设置地址低(字节)	00	设置地址低(字节)	00
设置数量高(字节)	00	设置数量高(字节)	00
设置数量低(字节)	04	设置数量低(字节)	04
字节计数	01		
设置内容高(字节)	00		
设置内容低(字节)	0F		

• 16 设置多个保持寄存器

MODBUS 请求

功能码	设置起始地址	设置长度	字节计数	设置内容
1 BYTE	2 BYTE	2 BYTE	1 BYTE	N*2 BYTE
0X10	0X0000 TO 0XFFFF	0X0000 TO 0X7B0	N*2	

MODBUS 响应

功能码	设置起始地址	设置长度
1 BYTE	2 BYTE	2 BYTE
0X10	0X0000 TO 0XFFFF	0X0000 TO 0X7B0

错误 响应

功能码	错误代码
1 BYTE	1 BYTE
0X10+ 0X80	0x01~0x07

举 例 (设置多个保持寄存器)

请 求	响 应
域名称	数据 (hex)
功能码	域名称
设置地址高(字节)	功能码
设置地址低(字节)	设置地址高(字节)
设置数量高(字节)	设置地址低(字节)
设置数量低(字节)	设置内容高(字节)
字节计数	设置内容低(字节)
设置内容高(字节)	数据 (hex)
设置内容低(字节)	10
设置内容高(字节)	功能码
设置内容低(字节)	00
设置内容高(字节)	设置地址高(字节)
设置内容低(字节)	01
设置内容高(字节)	设置地址低(字节)
设置内容低(字节)	00
设置内容高(字节)	设置内容高(字节)
设置内容低(字节)	02
字节计数	设置内容低(字节)
设置内容高(字节)	04
设置内容低(字节)	00
设置内容高(字节)	0A
设置内容低(字节)	01
设置内容高(字节)	02

通信协议

本产品采用RS485通信

波特率:9600

传输模式:RTU

本文档只涉及与本产品有关的协议。

Modbus默认地址为0x01,用户如有需要, 可以自行设置地址。

特殊指令用于修改用户Modbus协议地址:

指令头										地址
0x80	0x72	0x65	0x70	0x6F	0x6C	0x65	0x76	0x65	0x44	X

返回:

指令头										地址
0xFF	0x72	0x65	0x70	0x6F	0x6C	0x65	0x76	0x65	0x44	X

注意: 在修改Modbus地址的时候, 需要单个刷新 (总线上只有需要修改的设备)。

Modbus 功能码已实现功能

功能码	名称	作用	是否实现
01 (0x01)	读取线圈状态	取得一组逻辑线圈的当前状态 (ON/OFF)	否
02 (0x02)	读取输入状态	取得一组开关输入的当前状态 (ON/OFF)	否
03 (0x03)	读取保持寄存器	在一个或多个保持寄存器中取得当前的二进制值	是
04 (0x04)	读取输入寄存器	在一个或多个输入寄存器中取得当前的二进制值	否
05 (0x05)	强置单线圈	强置一个逻辑线圈的通断状态	否
06 (0x06)	预置单保持寄存器	把具体二进值装入一个保持寄存器	否
15 (0x0F)	强置多线圈	强置一串连续逻辑线圈的通断	否
16 (0x10)	预置多保持寄存器	把具体的二进制值装入一串连续的保持寄存器	否

寄存器-数据对应表

地 址	数 据	是否可读写	说 明
0x2000	byte[0]	只 读	浓度值为Float类型
	byte[1]	只 读	(byte[0]<<24) (byte[1]<<16) (byte[2]<<8) byte[3]
0x2002	byte[2]	只 读	然后按照32位float数据类型转换
	byte[3]	只 读	
0x2004	byte[4]	只 读	温度, 16位带符号整形
	byte[5]	只 读	byte[4]<<8 byte[5],包含2位小数
0x2006	byte[6]	只 读	湿度, 16位无符号整型
	byte[7]	只 读	byte[6]<<8 byte[7], 包含2位小数
0x2008	byte[8]	只 读	最大量程, 16位无符号整型
	byte[9]	只 读	byte[8]<<8 byte[9]
0x200A	byte[10]	只 读	固定为0
	byte[11]	只 读	传感器类型
0x200C	byte[12]	只 读	固定为0
	byte[13]	只 读	气泵状态: 0-正常, 1-吸气错误, 2-排气错误, 3-损坏
0x200E	byte[14]	只 读	固定为0
	byte[15]	只 读	量程状态: 0-量程范围内, 1-超量程
0x2010	byte[16]	只 读	固定为0
	byte[17]	只 读	缺省
0x2012	byte[18]	只 读	固定为0
	byte[19]	只 读	零点状态: 0-零点正常, 1-零点溢出
0x2014	byte[20]	只 读	固定为0
	byte[21]	只 读	浓度值是否无效: 0-有效, 1-无效
0x2016	byte[22]	只 读	固定为0
	byte[23]	只 读	传感器状态: 0-正常, 1-需要更换传感器 2-保留, 3-建议更换传感器

读取数据返回错误码:

0x01	功能码错误
0x02	获取长度超出, 或者寄存器地址错误

软件版本号读取

Byte index	地 址	是否可读写	说 明	样 例(ascii)
0	0x3000	只 读	byte[0]	1
1		只 读	byte[1]	.
2	0x3001	只 读	byte[2]	1
3		只 读	byte[3]	.
4	0x3002	只 读	byte[4]	1
5		只 读	byte[5]	.
6	0x3003	只 读	byte[6]	0
7		只 读	byte[7]	.
8	0x3004	只 读	byte[8]	2
9		只 读	byte[9]	0
10	0x3005	只 读	byte[10]	2
11		只 读	byte[11]	0
12	0x3006	只 读	byte[12]	0
13		只 读	byte[13]	8
14	0x3007	只 读	byte[14]	2
15		只 读	byte[15]	4



德国研发生产中心

EC Sense GmbH

Wangener Weg 3 | 82069 Hohenschäftlarn, Germany
Tel: +49(0)8178 99992-10
Fax: +49(0)8178 99992-11
Email: office@ecsense.com
www.ecsense.com www.ecnose.de

亚太区·中国应用设计研发中心

宁波爱氪森科技有限公司

浙江·宁波市鄞州区金谷北路 228 号中物科技园 17 幢 4
邮编: 315100
座机: 0574-88097236, 88096372
邮箱: info@aqsystems.cn
网址: www.ecsense.cn, www.ecnose.com