技术规范

CZSR SMART 系列 Modbus 通讯协议

修订页

序号	版本号	修订内容简述	编制/日期
1	1.0	首次创建	申晓瑞 2022/08/01
2	1.1	添加电源电压、线圈电压、MCU 温度计算公式	周海亭 2023/07/13
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

目录

第1章 概述

1.1 Modbus 协议概述

Modbus 是 OSI 模型第 7 层上的应用报文传输协议，它在连接至不同类型总线或网络的设备之间提供客户机/服务器通信，见图 1 。

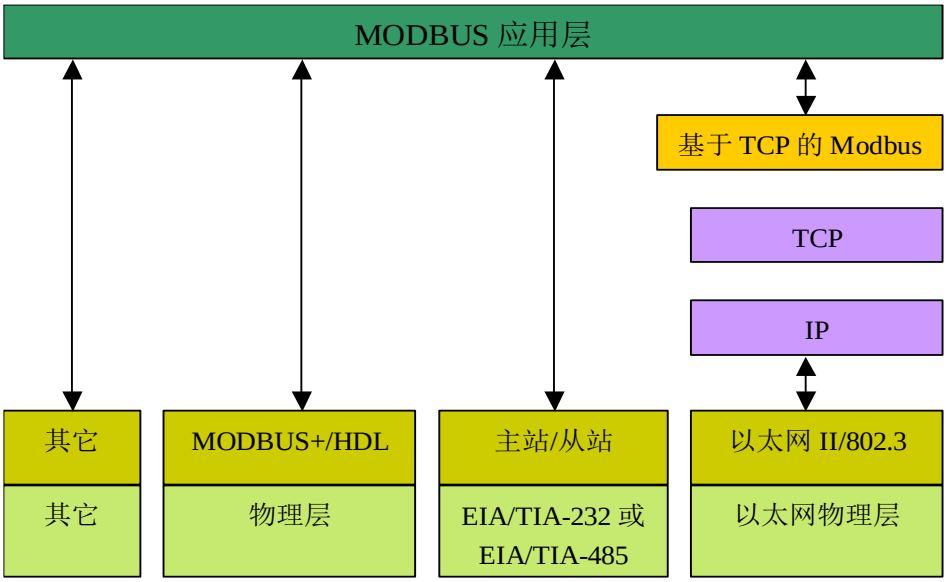

图 1：MODBUS 通信栈

MODBUS 协议允许在各种网络体系结构内进行简单通信。

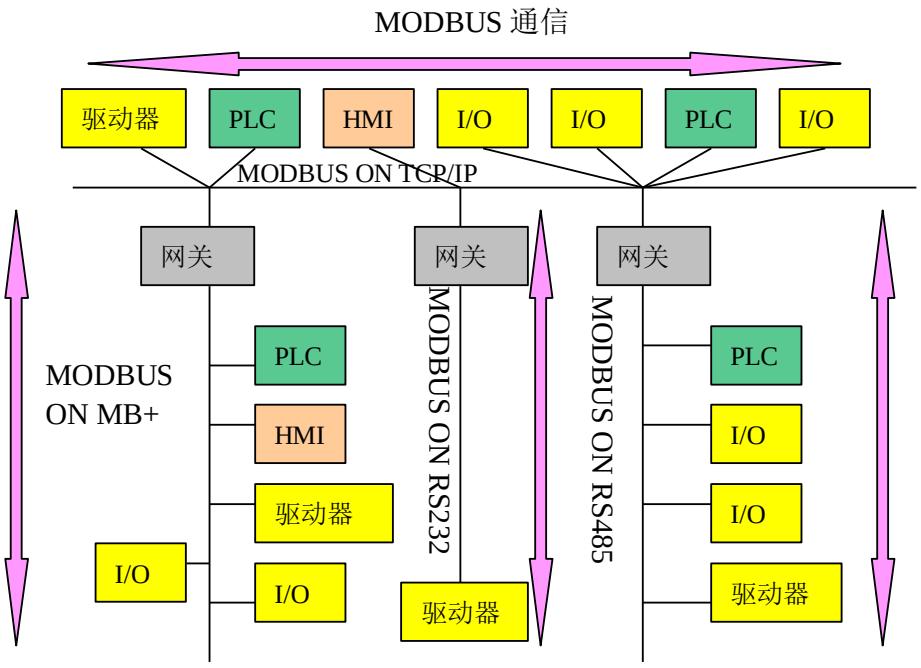

图 2：MODBUS 网络体系结构的实例

Modbus 协议已是全球工业领域最流行的协议之一。它广泛应用于智能设备间建立基于主从方式的通讯连接。Modbus 协议只定义了通讯消息的消息结构，与物理层无关，因此不管是传统的 RS-232、RS-422、RS-485 总线，还是以太网网络，均可支持 Modbus 协议。

当在 Modbus 网络上通信时，Modbus 协议规定每个设备必须要知道它们的设备地址，并识别按地址发来的消息（只接收广播地址消息和本机地址消息），然后根据消息内容执行相应的操作。如果需要回应，则设备须根据 Modbus 协议生成反馈信息并发送到网络。

1.2 传输模式（串行链路）

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向某个“子”节点发出显式命令并处理响应的节点（主站）。从站在没有收到主站的请求时并不主动地传输数据，也不与其他从站通信。图 3 给出了与 7 层 OSI 模型对应的 Modbus 串行通信栈的一般表示。

层	ISO/OSI 模型	
7	应用层	Modbus 协议
6	表示层	空
5	会话层	空
4	传输层	空
3	网络层	空
2	数据链路层	Modbus 串行链路协议
1	物理层	EIA/TIA-485 (或

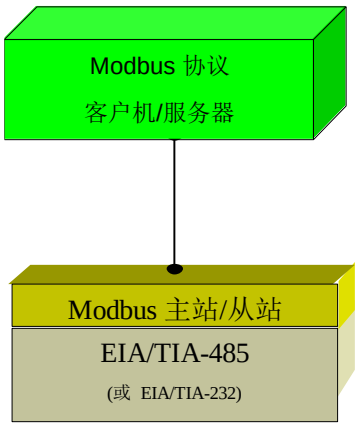

图 3 Modbus 协议和 ISO/OSI 模型

Modbus 标准网络有两种串行传输模式：ASCII 和 RTU。本公司使用 RTU 模式，不支持 ASCII 模式，以下讨论均基于 RTU 模式。

Modbus 帧结构如下表所示：

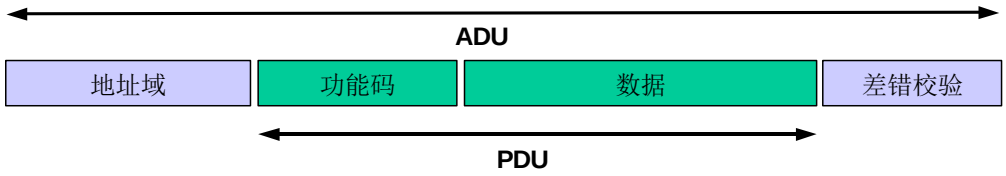

图 4 通用 Modbus 帧

PDU：Protocol Data Unit，协议数据单元。

ADU：Application Data Unit，应用数据单元。

其中，PDU 部分是必须的，ADU 和 PDU 的差异部分根据传输网络的不同而差异，本章节只讨论 PDU 部分。

1.2.1 功能码

用一个字节编码 Modbus 数据单元的功能码域。有效的码字范围是十进制数 1~255（128~255 为异常响应保留）。当消息从主设备发往从设备时，功能代码域将告之从设备需要执行哪些行为，从设备根据功能码的指示执行相应的操作。当从设备回应时，它使用功能代码域来指示是正常回应(无误)还是有某种错误发生（称作异常回应）。

——对正常回应，响应功能码 = 请求功能码。

——对异常回应，响应功能码 = 请求功能代码 + 0x80。

例如：对于功能码为 0x03 的请求，正常回应的功能码也为 0x03，而异常回应的功能码为 0x03 和 0x80 相或的值即 0x83。

异常回应的数据域将包含一异常码（见**错误!未找到引用源。 错误!未找到引用源。**）以指示从设备发生的错误类型。主设备应用程序得到异常回应后，典型的处理过程是重发消息，或者诊断发给从设备的消息并报告给操作员。

下表是 Modbus 支持的功能码：

表 1.Modbus 功能码

功能码	名称	作用
01	读取线圈状态	取得一组逻辑线圈的当前状态（ON/OFF）
02	读取离散量输入状态	取得一组开关输入的当前状态（ON/OFF）
03	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	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	强置单线圈	强置一个逻辑线圈的通断状态
06	预置单寄存器	把具体二进值装入一个保持寄存器
07	读取异常状态	取得 8 个内部线圈的通断状态，这 8 个线圈的地址由控制器决定
08	回送诊断校验	把诊断校验报文送从机，以对通信处理进行评鉴
11	读取事件计数	可使主机发出单询问，并随即判定操作是否成功，尤其是该命令或其他应答产生通信错误时
12	读取通信事件记录	可是主机检索每台从机的 ModBus 事务处理通信事件记录。如果某项事务处理完成，记录会给出有关错误
15	强置多线圈	强置一串连续逻辑线圈的通断
16	预置多寄存器	把具体的二进制值装入一串连续的保持寄存器
17	报告从机标识	可使主机判断编址从机的类型及该从机运行指示灯的状态
20	读文件记录	显示扩展存储器文件中的数据信息
21	写文件记录	把通用参数写入扩展存储文件，或修改之
22	屏蔽写寄存器	设置或清除寄存器中不同的位
23	读/写多个寄存器	在一个单独 Modbus 事务中一个读操作和一个些操作的组合，在读之前写
24	读 FIFO 队列	读远程设备中的先入先出（FIFO）寄存器队列内容
25~64	保留作扩展功能备用	
65~72	保留以备用户功能所用	留作用户功能的扩展编码
73~99	非法功能	
100~110	保留以备用户功能所用	留作用户功能的扩展编码
120~127	保留	留作内部作用

1.2.2 数据域

数据域是由两个十六进制数集合构成的，范围 0x00~0xFF，除非特别指明，凡是大于 1 个字节的数据，均为高字节在前，低字节在后。

Modbus 的数据模型是以一组具有不同特征的表为基础建立的。4 个基本表见表 2。

表 2.Modbus 数据模型

基本表格	对象类型	访问类型	内容
离散量输入	单个比特	只读	I/O 系统提供这种类型数据
线圈	单个比特	读写	通过应用程序改变这种类型数据
输入寄存器	16-比特字	只读	I/O 系统提供这种类型数据
保持寄存器	16-比特字	读写	通过应用程序改变这种类型数据

Modbus 处理的所有数据（位、寄存器）放置在设备应用存储器中。但是，存储器的物理地址不应该与寄存器编号混淆。仅要求将寄存器编号与物理地址链接。

第2章 Modbus 串行

2.1 Modbus 串行链路 RTU 模式

在物理层，Modbus 串行链路系统可以使用不同的物理接口(RS485、RS232)。最常用的是 TIA/EIA-485 (RS485) 两线制接口。作为附加的选项，也可以实现 RS485 四线制接口。当只需要短距离的点到点通信时，TIA/EIA-232-E (RS232) 串行接口也可以使用。

当设备在 Modbus 串行链路上使用 RTU（远程终端单元）模式通信时，报文中每个 8 位字节含有两个 4 位 16 进制字符。这种模式的主要优点是在相同的波特率下其较高的字符密度具有比 ASCII 模式更高的吞吐率。必须以连续的字符流传输每个报文。

RTU 模式每个字节 （ 11 位 ） 的格式为 ：

编码系统： 8 位二进制

报文中每个 8 位字节含有两个 4 位十六进制字符(0 - 9， A - F)

每个字节的位： 1 起始位

8 数据位， 首先发送最低有效位

1 位作为奇偶校验位，无校验则无

1 停止位

偶校验是要求的， 其它模式 （ 奇校验， 无校验 ） 也可以使用。 为了保证与其它产品的最大兼容性，同时支持无校验模式是建议的。默认校验模式必须为偶校验。

注 ： 使用无校验要求 2 个停止位。

详细的字符格式如下所示，每个字符或字节均由此顺序发送(从左到右)：

有校验

起始位	1	2	3	4	5	6	7	8	校验位	停止位

无校验

起始位	1	2	3	4	5	6	7	8	停止位	停止位

2.2 帧格式

对于基于串口的 Modbus，附加地址域采用 1 字节的从站地址，数据校验域采用 2 字节的 CRC 校验，故串口 Modbus 的 ADU 帧格式如下：

子节点地址	功能代码	数据	CRC
1 字节	1 字节	0 到 252 字节	2 字节 CRC 低 | CRC 高

图 5: RTU 报文帧

最大 Modbus RTU 帧是 256 个字节。

2.2.1 从站地址

消息帧的地址域包含 8Bits。可能的从设备地址是 0~247（十进制）。

单个设备的地址范围是 1~247。主设备通过将要联络的从设备的地址放入消息中的地址域来选通从设备。当从设备发送回应消息时，它把自己的地址放入回应消息的地址域中，以便主设备知道是哪一个设备作出回应。地址 0 是用作广播地址，以使所有的从设备都能认识。当 Modbus 协议用于更高水准的网络，广播可能不允许或以其它方式代替。

2.2.2 错误检测域

当选用 RTU 模式作字符帧，错误检测域包含 16Bits 值（用两个 8 位的字符来实现）。错误检测域的内容是通过对消息内容进行循环冗长检测方法得出的。CRC 域附加在消息的最后，添加时先是低字节然后是高字节。故 CRC 的高位字节是发送消息的最后一个字节。

CRC 的实现方法见**错误!未找到引用源。 错误!未找到引用源。**。

第3章 CZSR SMART 系列仪表的 Modbus 协议

3.1 支持的功能码

CZSR SMART 系列仪表支持的 Modbus 功能码：

功能码	名称	读写属性	作用
01	读取线圈状态	只读	取得一组逻辑线圈的当前状态（ON/OFF）
02	读取离散量输入状态	只读	取得一组开关输入的当前状态（ON/OFF）
04	读取输入寄存器	只读	在一个或多个输入寄存器中取得当前的二进制值

3.2 数据类型

CZSR 8500 系列仪表涉及 3 种类型的变量，如下表所示：

类型	说明
Boolean（开关量）	1 Bit Boolean
Integer（寄存器）	16 Bits Integer
Float（寄存器）	32 Bits Float(仅针对 CZSR 8500 系列)

3.3 通讯设置

CZSR 8500 系列仪表支持的 Modbus 通讯相关设置，如下表所示：

序号	描述	属性
1	数据位	8
2	奇偶校验位	无
3	停止位	1
4	传输波特率	38400bps

3.4 支持仪表

下表所列的仪表均支持 Modbus 协议。

序号	仪表型号	所在章节
1	CZSR8901-2A4S	4.1
2	CZSR8501-2A4S	4.2
3	CZSR8502-2A2S2AO	4.3
4		
5		

第4章 各型仪表的寄存器变量说明

4.1 CZSR8902-2A4S

输入寄存器	字节数	说明	功能代码	访问权限
01	00	逻辑块 1 的输出值 True-0x55,False-0xAA	04	只读
	01	逻辑块 2 的输出值 True-0x55,False-0xAA	04	只读
02	02	逻辑块 3 的输出值 True-0x55,False-0xAA	04	只读
	03	逻辑块 4 的输出值 True-0x55,False-0xAA	04	只读
03	04	逻辑块 5 的输出值 True-0x55,False-0xAA	04	只读
	05	逻辑块 6 的输出值 True-0x55,False-0xAA	04	只读
04	06	逻辑块 7 的输出值 True-0x55,False-0xAA	04	只读
	07	逻辑块 8 的输出值 True-0x55,False-0xAA	04	只读
05	08	逻辑块 9 的输出值 True-0x55,False-0xAA	04	只读
	09	逻辑块 10 的输出值 True-0x55,False-0xAA	04	只读
06	10	逻辑块 11 的输出值 True-0x55,False-0Xaa	04	只读
	11	逻辑块 12 的输出值 True-0x55,False-0xAA	04	只读
07	12	逻辑块 13 的输出值 True-0x55,False-0xAA	04	只读
	13	逻辑块 14 的输出值 True-0x55,False-0xAA	04	只读
08	14	逻辑块 15 的输出值 True-0x55,False-0xAA	04	只读
	15	逻辑块 16 的输出值 True-0x55,False-0xAA	04	只读
09	16	逻辑块 17 的输出值 True-0x55,False-0xAA	04	只读
	17	逻辑块 18 的输出值 True-0x55,False-0xAA	04	只读
10	18	输入 CH1 至 CH6 采样值 （低六位有效，其余位保留）	04	只读
	19		04	只读
11	20	输出 OUT1 至 OUT6 采样值 （低六位有效低六位有效，其余位保留）	04	只读
	21		04	只读
12	22	Bit0 至 Bit5：输入 CH1 至 CH6 1/2 脉冲检测故障 Bit6 至 Bit11： 输入 CH1 至 CH6 通道不平衡故障 Bit12 至 Bit15：输出 34 至 64 短路故障	04	只读
	23		04	只读
13	24	当前通讯的 MCU 地址 MCUA-0x01;MCUB-0x02	04	只读
	25	Bit0: MCU 自检故障-断电重启才能消除 Bit1: 双 RAM 比较故障-断电重启才能消除 Bit2：SPI 通讯故障-断电重启才能消除 Bit3：FLASH 故障-可消除 Bit4：RAM 校验故障-可消除 Bit5: 电源电压故障-可消除 Bit6：线圈电压故障-可消除 Bit7：保留	04	只读
14	26	Bit0: 黄灯亮 Bit1: 黄灯闪烁 Bit4: 红灯亮 Bit5: 红灯闪烁 其余位保留	04	只读
	27		04	
15	28	MCU 温度-不能直接用需转化	04	只读
	29		04	
16	30	模块电源电压-不能直接用需转化	04	只读
	31		04	
17	32	线圈电压-不能直接用需转化	04	只读
	33		04	
18	34	基准电压-不能直接用需转化	04	只读

输入寄存器	字节数	说明	功能代码	访问权限
	35		04	
19	36	基准校准-不能直接用需转化	04	只读
	37		04	
20	38	温度校准-不能直接用需转化	04	只读
	39		04	

电源电压、线圈电压、MCU 温度计算公式如下：

基准电压：V_{dd} = 3.3 * register19/ register18;

电源电压：V_{pwr} = (2619 * V_{dd} / 4095) * 43.9 / 3.9 + 1;

线圈电压：$V_{coilpwr}$ = (register17 * V_{dd} / 4095) * 38.8 / 6.8;

基准温度：T_{dd} = 3.3 * register20/ 4095;

MCU 温度：T_{MCU} = (T_{dd} * 1000 - (register15 * V_{dd} / 4095) * 1000) / 4.3 + 30;

注意：Modbus 提取原始数据时注意大小端位置交换。

4.2 CZSR8501-2A4S/CZSR8502-2A2S2AO

输入寄存器	字节数	说明	功能代码	访问权限
01	00	逻辑块 1 的输出值 True-0x55,False-0xAA	04	只读
	01	逻辑块 2 的输出值 True-0x55,False-0xAA	04	只读
02	02	逻辑块 3 的输出值 True-0x55,False-0xAA	04	只读
	03	逻辑块 4 的输出值 True-0x55,False-0xAA	04	只读
03	04	逻辑块 5 的输出值 True-0x55,False-0xAA	04	只读
	05	逻辑块 6 的输出值 True-0x55,False-0xAA	04	只读
04	06	逻辑块 7 的输出值 True-0x55,False-0xAA	04	只读
	07	逻辑块 8 的输出值 True-0x55,False-0xAA	04	只读
05	08	逻辑块 9 的输出值 True-0x55,False-0xAA	04	只读
	09	逻辑块 10 的输出值 True-0x55,False-0xAA	04	只读
06	10	逻辑块 11 的输出值 True-0x55,False-0Xaa	04	只读
	11	逻辑块 12 的输出值 True-0x55,False-0xAA	04	只读
07	12	逻辑块 13 的输出值 True-0x55,False-0xAA	04	只读
	13	逻辑块 14 的输出值 True-0x55,False-0xAA	04	只读
08	14	逻辑块 15 的输出值 True-0x55,False-0xAA	04	只读
	15	逻辑块 16 的输出值 True-0x55,False-0xAA	04	只读
09	16	逻辑块 17 的输出值 True-0x55,False-0xAA	04	只读
	17	逻辑块 18 的输出值 True-0x55,False-0xAA	04	只读
10	18	CZSR8501-2A4S: Bit0 至 Bit3：输入 CH1 至 CH4 采样值 Bit4：编码器正反转采样值 CZSR8502-2A2S2AO: Bit0：输入 CH1 采样值 Bit1：编码器正反转采样值	04	只读
	19	CZSR8501-2A4S: Bit0 至 Bit6：输出 DO1 至 DO6 输出值 CZSR8502-2A2S2AO: Bit0 至 Bit4：输出 DO1 至 DO4 输出值	04	只读
11	20	Pi1 输入频率采样值	04	只读
	21			
12	22			
	23			
13	24	Sin 输入频率采样值	04	只读
	25			
14	26			

输入寄存器	字节数	说明	功能代码	访问权限
	27			
15	28	CZSR8501-2A4S：保留 CZSR8502-2A2S2AO：AO1 输出值	04	只读
	29			
16	30			
	31			
17	32	CZSR8501-2A4S：保留 CZSR8502-2A2S2AO：AO2 输出值	04	只读
	33			
18	34			
	35			
19	36	CZSR8501-2A4S：保留 CZSR8502-2A2S2AO：AO1 输出类型 0xCB-电流输出；0xCC-电压输出	04	只读
	37	CZSR8501-2A4S：保留 CZSR8502-2A2S2AO：AO2 输出类型 0xCB-电流输出；0xCC-电压输出		
20	38	CZSR8501-2A4S： Bit0 至 Bit3：输入 CH1 至 CH4 1/2 脉冲检测故障 Bit4 至 Bit7：输入 CH1 至 CH4 输入不平衡故障 Bit8:接近开关频率采样不平衡故障 Bit9:编码器频率采样不平衡故障 Bit10 至 Bit13:输出 SO1 至 SO4 输出短路故障 其余位保留 CZSR8502-2A2S2AO： Bit8:接近开关频率采样不平衡故障 Bit9:编码器频率采样不平衡故障 Bit10 至 Bit13:输出 SO1 至 SO4 输出短路故障 其余位保留	04	只读
	39			
21	40	Bit0: MCU 自检故障-断电重启才能消除 Bit1:双 ram 比较故障-断电重启才能消除 Bit2：SPI 通讯故障-断电重启才能消除 Bit3：FLASH 故障-可消除 Bit4：RAM 校验故障-可消除 Bit5: 电源电压故障-可消除 Bit6：线圈电压故障-可消除 其余位保留	04	只读
	41	当前通讯的 MCU 地址 MCUA-0x01;MCUB-0x02		
22	42	Pi1 指示灯信息 0x00-灭/0x01-亮/0x02-闪	04	只读
	43	Pi2 指示灯信息 0x00-灭/0x01-亮/0x02-闪		
23	44	sin 指示灯信息 0x00-灭/0x01-亮/0x02-闪		
	45	cos 指示灯信息 0x00-灭/0x01-亮/0x02-闪		
24	46	RO1 指示灯信息 0x00-灭/0x01-亮/0x02-闪		
	47	ERR1 指示灯信息 0x00-灭/0x01-亮/0x02-闪		
25	48	MCU 温度-不能直接用需转化	04	只读
	49			
26	50	模块电源电压-不能直接用需转化	04	只读
	51			
27	52	线圈电压-不能直接用需转化	04	只读
	53			
28	54	基准电压-不能直接用需转化	04	只读
	55			

输入寄存器	字节数	说明	功能代码	访问权限
29	56	基准校准-不能直接用需转化	04	只读
	57			
30	58	温度校准-不能直接用需转化	04	只读
	59			
31	60	MCU 计算的 CRC 值	04	只读
	61			
32	62	保留值	04	只读
	63			
33	64	Pi1 输入频率采样值	04	只读
	65			
34	66			
	67			
35	68	sin 输入频率采样值	04	只读
	69			
36	70			
	71			
37	72	Pi2 输入频率采样值	04	只读
	73			
38	74			
	75			
39	76	cos 输入频率采样值	04	只读
	77			
40	78			
	79			

电源电压、线圈电压、MCU 温度计算公式如下：

基准电压：V_{dd} = 3.3 * register29/ register28;

电源电压：V_{pwr} = (2619 * V_{dd} / 4095) * 43.9 / 3.9 + 1;

线圈电压：$V_{coilpwr}$ = (register27 * V_{dd} / 4095) * 38.8 / 6.8;

基准温度：T_{dd} = 3.3 * register30/ 4095;

MCU 温度：T_{MCU} = (T_{dd} * 1000 - (register25 * V_{dd} / 4095) * 1000) / 4.3 + 30;

注意：Modbus 提取原始数据时注意大小端位置交换。

第5章 命令实例及解释

以下实例均基于串口模式，设备地址默认为地址 1。

5.1 功能码 02（0x02）：读取离散量输入状态

问询帧：

名称	设备地址	功能码(0x02)	起始地址高	起始地址低	数据数量高	数据数量低	CRC
长度(字节)	1	1	1	1	1	1	2

应答帧（正常应答）：

名称	设备地址	功能码(0x02)	返回字节数 N	返回数据	CRC
长度(字节)	1	1	1	N×1	2

特别说明：

问询帧：数据数量表示从起始地址开始读多少个离散输入量状态。

应答帧：每一个字节表示 8 个输入的值，CZSR SMART 系列最低支持连续读 10 个以上的离散输入量，每一位表示对应离散输入量的状态。

范例：

- 读取的 CZSR SMART 系列的离散输入量。

问询：0x01 0x02 0x00 0x00 0x00 0x10 0x79 0xC6

应答：0x01 0x02 0x02 0x02 0x00 0xA1 0x18

表示成功读取 CZSR SMART 系列的 16 个离散输入量，其中低六位有效，其余位无效。

5.2 功能码 04（0x04）：读一个或多个寄存器

问询帧：

名称	设备地址	功能码(0x04)	起始地址高	起始地址低	数据数量高	数据数量低	CRC
长度(字节)	1	1	1	1	1	1	2

应答帧（正常应答）：

名称	设备地址	功能码(0x03)	返回字节数 N	返回数据	CRC
长度(字节)	1	1	1	N×1	2

特别说明：

问询帧:数据数量表示读取寄存器的个数,数据范围 CZSR8902-2A4S 为 20 个,CZSR8501-2A4S 和 CZSR8502-2A2S2AO 为 40 个。

应答帧：每一个寄存器的高字节在前，低字节在后。(浮点数数据按浮点格式排列)

范例：

- 读取的 CZSR SMART 系列的寄存器值。

询问：0x01 0x04 0x00 0x00 0x00 0x28 0xF0 0x14

应答：0x01 0x04 0x50 0x55 …… 0x06 0xC6 0xEA

表示成功读取 CZSR8501-2A4S 和 CZSR8502-2A2S2AO 的 40 个寄存器的值。