XSL 系列仪表 Modbus 通讯协议

1、Modbus 通讯协议简介

1.1. Modbus 通讯协议采用 RTU 传输模式

RTU 模式中每个字节（10 位）的格式为：

1 个起始位	8 个数据位	1 个停止位

注： 帧校验采用循环冗余校验（CRC）

仪表的应答延迟小于 300ms

1.2. 与通讯有关的参数说明

Ad 仪表通讯地址，参数地址 0X000D，取值范围 0~99，出厂设置为 1

bd 通讯速率选择，参数地址 0X000E，取值范围 2400、4800、9600、19200（bps）可选，出厂设置为 9600bps

2、通讯命令简介

本系列仪表支持的 Modbus 命令集

命令名称	Modbus 命令类型	功能码（十六进制）	寻址范围（十进制）
读测量值	读输入寄存器	04	见附表 2
读仪表参数值	读保持寄存器	03	见附表 1
读个通道报警状态	读线圈	01	0～79
设置仪表参数	写保持寄存器	10	见附表 1

指令中涉及到的测量值采用 32 位浮点数（IEEE-754 标准格式）表示，占用 2 个连续的寄存器。仪表参数值采样整型数表示，占用 1 个寄存器

每条指令的具体功能请参见 通讯命令详解

3、通讯命令详解

3.1. 命令说明

所有命令中的数值均采用十六进制表示

1) 读测量值命令

本命令读取巡检仪 1～80 通道的测量值（测量值定义为 2 个连续的输入寄存器）。各通道测量值寄存器地址详见附表 2.每条命令最多可以读取 16 个连续通道的测量值。

命令：AA 04 BBBB DDDD CCCC

AA	04	BBBB	DDDD	CCCC
通讯地址	功能码	寄存器起始地址	寄存器个数	CRC 校验值

响应：AA 04 EE data CCCC

AA	04	EE	data	CCCC
通讯地址	功能码	测量值字节数	测量值	CRC 校验值

“EE”字符表示返回的测量值字节数。数值上等于 DDDD × 2

例：读取设备地址为 01 的巡检仪第 1 通道测量值。该仪表当前第 1 通道测量值为 582.8（16 进制 4411B333）。

命令： 01 04 00 00 00 02 71 CB

响应：01 04 04 **44 11 B3 33** 8A 54

2) 读仪表参数值命令

本命令读取仪表的参数。每次最多可以连续读取 16 个参数。返回参数用整型数表示（占用 1 个寄存器）。参数地址详见附表 1

命令：AA 03 BBBB DDDD CCCC

AA	03	BBBB	DDDD	CCCC
通讯地址	功能码	寄存器起始地址	寄存器个数	CRC 校验值

响应：AA 03 EE data CCCC

AA	03	EE	data	CCCC
通讯地址	功能码	参数值字节数	参数值	CRC 校验值

例：读取设备地址为 01 的仪表的通道 1 的 AH 到 AL 地址连续的 2 个参数。

命令：01 03 00 30 00 02 C4 04

响应：01 03 04 **03 E8 03 E8** 7A FD

通道 1 的参数 AH 数值 0x03E8，即十进制 1000。通道 1 的参数 AL 数值 0x03E8，即十进制 1000。参数的小数点位置的详细信息见说明书。

注：读取 1 个参数时如果此参数不存在，返回错误码。一次读取多于 1 个参数时，如果有的参数不存在或者都不存在，不存在的参数也会被读出，不返回错误码。一次最多可以读取 16 个地址连续的参数。

3) 读各通道报警状态命令

巡检仪最多 80 个通道报警状态

命令：AA 01 BBBB DDDD CCCC

AA	01	BBBB	DDDD	CCCC
通讯地址	功能码	开关量起始地址	开关量个数	CRC 校验值

响应：AA 01 EE data CCCC

AA	01	EE	data	CCCC
通讯地址	功能码	开关量状态字节数	开关量状态	CRC 校验值

BBBB：表示将要读取的报警状态的起始通道。对于巡检仪，1～80 通道报警状态对应的寻址范围 0～79（十六进制 0x0000～0x004F）。

DDDD：字符表示本命令要读取的报警通道的个数。

EE： 表示返回的包含开关量状态的数据字节个数。数值上等于 DDDD / 8，如果余数不等于 0，则等于 DDDD / 8＋1。

Data： 表示返回的报警状态。

例： 读取设备地址为 01 的仪表的第 1～9 通道报警状态。

命令：01 01 00 00 00 09 FC 0C

响应：01 01 02 **B3 01** 0D 0C

通道 8～1 的报警状态表示为十六进制字节 B3，或二进制 10110011。通道 8 报警状态是最高位，通道 1 报警状态是最低位，即通道 1、2、5、6、8 路报警。通道 16～9 的报警状态表示为十六进制字节 01，表示第 9 通道报警

4) 设置仪表参数值命令

本命令修改仪表中的参数的数值。参数地址详见附表 1

命令：AA 10 BBBB DDDD EE data CCCC

AA	10	BBBB	DDDD	EE	data	CCCC
通讯地址	功能码	寄存器起始地址	寄存器个数	参数值字节数	参数值	CRC 校验值

正常响应：AA10BBBBDDDDCCCC

AA	10	BBBB	DDDD	CCCC
通讯地址	功能码	寄存器起始地址	寄存器个数	CRC 校验值

参数值字节数=寄存器个数×2

注：修改除密码外的参数时首先必须把密码写为 1111，然后再修改想要修改的参数。修改 1 个参数时如果此参数不存在，返回错误码。一次修改多于 1 个参数时，如果有的参数不存在或者都不存在，不存在的参数也会被修改，不返回错误码。一次最多可以修改 16 个地址连续的参数。

例：把地址为 01 的仪表，参数地址为 01 到 03 的 3 个参数分别改为 10，32，61。

首先发送命令： 01 10 00 00 00 01 02 **04 57** E5 6E

响应：01 10 00 00 00 01 01 C9

再次发送命令：01 10 00 01 00 03 06 **00 0A 00 20 00 3D** EF 5F

响应：01 10 00 01 00 03 D1 C8

3.2. 异常码返回

当仪表接收到主机发送的指令，在处理过程中出现异常时，返回异常码. 返回的格式为：AABBDDCCCC

AA	BB	DD	CCCC
通讯地址	差错码	异常码	CRC 校验值

BB 的取值为：指令的功能码+0x80

DD 的取值为：01、02、03、04

Modbus 异常码		
代码	名称	含义
01	非法功能	接收到的功能码是不允许的操作。
02	非法数据地址	接收到的数据地址是不允许的地址；例如：仪表具有 100 个参数，带有起始地址 96 和参数个数 5 的读仪表参数命令会产生异常码 02
03	非法数据值	接收到的数据域中包含的是不允许的值。
04	从站设备故障	当仪表正在试图执行请求的操作时，产生不可恢复的错误。（在通讯修改参数值时，发现密码 OA 参数未被置为 1111。）

3.3. 仪表不响应的情况

- ✓ 通讯地址错误
- ✓ 波特率错误
- ✓ CRC 校验错误
- ✓ 命令长度输入错误

注：

- ✓ 在设置状态下，禁止通讯

附表 1

参数类别	参数符号	参数名称	参数的寄存器地址
公共参数	oA	OA	0x0000
	ct	CT	0x0001
	cH	CH	0x0002
	Ld	LD	0x0003
	LC	LI	0x0004
	F1	F1	0x0006
	F2	F2	0x0007
	F3	F3	0x0008
	F4	F4	0x0009
	H1	H1	0x000A
	H2	H2	0x000B
	At	AT	0x000C
	Ad	AD	0x000D
	bd	BD	0x000E
参数类别	参数符号	参数名称	通道参数地址偏移量
通道参数	AH	AH	0
	AL	AL	1
	bH	BH	2
	bL	BL	3
	IA	IA	4
	FI	FI	5
	It	IT	6
	Id	ID	7
	Ur	UR	8
	Fr	FR	9
	Lb	LB	11

注：附表 1 中通道参数的寄存器地址计算公式 = （I－1） × 12 + 48 + R 公式中 I 表示通道号，取值范围 1～ 80 通道。R 表示相应的通道参数地址偏移量取值范围 0～11。例：通道 1 的参数 AL 地址 = （1－1）× 12 + 48 + 1 结果为 49 转换成十六进制地址为 0x0031.

附表 2

通道	对应地址	通道	对应地址
第 1 通道	0000H	第 41 通道	0050H
第 2 通道	0002H	第 42 通道	0052H
第 3 通道	0004H	第 43 通道	0054H
第 4 通道	0006H	第 44 通道	0056H
第 5 通道	0008H	第 45 通道	0058H
第 6 通道	000AH	第 46 通道	005AH
第 7 通道	000CH	第 47 通道	005CH
第 8 通道	000EH	第 48 通道	005EH
第 9 通道	0010H	第 49 通道	0060H
第 10 通道	0012H	第 50 通道	0062H
第 11 通道	0014H	第 51 通道	0064H
第 12 通道	0016H	第 52 通道	0066H
第 13 通道	0018H	第 53 通道	0068H
第 14 通道	001AH	第 54 通道	006AH
第 15 通道	001CH	第 55 通道	006CH
第 16 通道	001EH	第 56 通道	006EH
第 17 通道	0020H	第 57 通道	0070H
第 18 通道	0022H	第 58 通道	0072H
第 19 通道	0024H	第 59 通道	0074H
第 20 通道	0026H	第 60 通道	0076H
第 21 通道	0028H	第 61 通道	0078H
第 22 通道	002AH	第 62 通道	007AH
第 23 通道	002CH	第 63 通道	007CH
第 24 通道	002EH	第 64 通道	007EH
第 25 通道	0030H	第 65 通道	0080H
第 26 通道	0032H	第 66 通道	0082H
第 27 通道	0034H	第 67 通道	0084H
第 28 通道	0036H	第 68 通道	0086H
第 29 通道	0038H	第 69 通道	0088H
第 30 通道	003AH	第 70 通道	008AH
第 31 通道	003CH	第 71 通道	008CH
第 32 通道	003EH	第 72 通道	008EH
第 33 通道	0040H	第 73 通道	0090H
第 34 通道	0042H	第 74 通道	0092H
第 35 通道	0044H	第 75 通道	0094H
第 36 通道	0046H	第 76 通道	0096H
第 37 通道	0048H	第 77 通道	0098H
第 38 通道	004AH	第 78 通道	009AH
第 39 通道	004CH	第 79 通道	009CH
第 40 通道	004EH	第 80 通道	009EH