

新版 Modbus 库使用说明

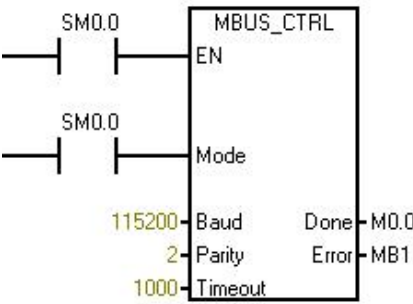
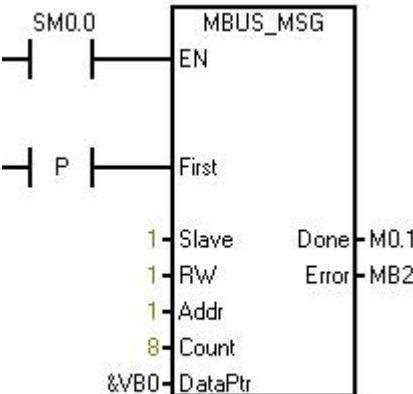
目 录

1. 概述.....	3
2. 主站库使用说明.....	3
2.1 MBUS_CTRL 执行错误代码.....	3
2.2 MBUS_MSG 执行错误代码.....	4
3. 从站库使用说明.....	5
3.1 从站 MBUS_INIT 执行错误代码.....	5
4. 注意事项.....	5

1. 概述

西门子的 MODBUS 库属于上层 PLC 程序实现，程序量大，几乎占用了 2KB 的程序，此外运行效率较低，现把 MODBUS 库集成在 CPU 中，上位机只提供一个库接口。该库接口与原来的西门子 MODBUS 库接口保持一致并且使用方法也一致。支持大部分错误执行码。

2. 主站库使用说明

Modbus RTU Master		<p>Mode (BOOL) : 1=Modbus, 0=PPI (禁用 Modbus)</p> <p>Baud(DWORD): 支持波特率 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200</p> <p>Parity (BYTE) : 0=无校验, 1=奇校验, 2=偶校验</p> <p>Timeout (INT) : 超时时间, 单位为 ms</p> <p>Done (BOOL) : 完成标记 (始终置位)</p> <p>Error (BYTE) : 错误码 (0=无错误)</p>
		<p>First (BOOL) : 新消息 (设置为 1 时仅对新请求扫描一次)</p> <p>Slave (BYTE) : 从站地址: 0~247 (其中 0 为广播地址)</p> <p>RW (BYTE) : 0=读, 1=写</p> <p>Addr (DWORD) : Modbus 地址 (例如 40001)</p> <p>Count (INT) : 元素个数 (1 到 120 个字或 1 到 1920 位)</p> <p>DataPtr (DWORD) : 数据指针 (例 &VB1000)</p> <p>Done (BOOL) : 完成标记 (0=忙, 1=完成)</p> <p>Error (BYTE) : 错误码 (0=无错误)</p>

2.1 MBUS_CTRL 执行错误代码

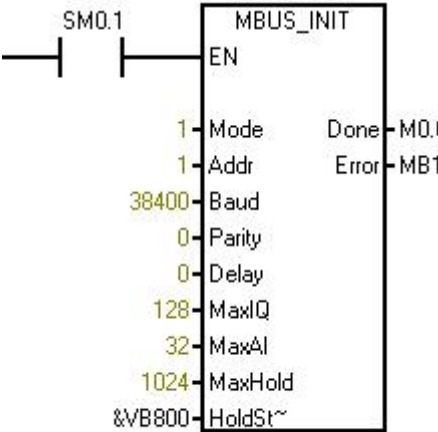
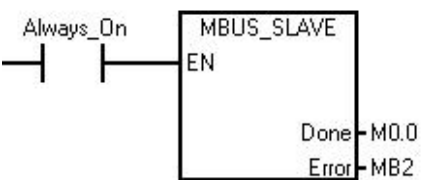
错误码	说明
0	无错误
1	奇偶校验参数不支持, 支持 0=无校验, 1=奇校验, 2=偶校验

2	波特率参数不支持，支持波特率 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
3	超时选择无效（有效范围 1~32767）

2.2 MBUS_MSG 执行错误代码

错误码	说明
0	无错误
3	接收超时：在"超时"时间内，没有来自从站的应答或者是从站地址错误
4	请求参数出错：从站（slave）、读写(RW)、地址(Addr)+计数 Count 被设置为非法值 Slave 允许范围 0~247 RW 允许值 0 和 1 Addr 允许范围：0~9999，10001~19999，30001~39999，40001~49999 注：当 Addr 为 10001~19999 或 30001~39999 时，RW 仅支持 0（读操作）
5	MBUS_CTRL 指令未执行或初始化参数出错
6	Modbus 忙于处理另一个请求：一次只能激活一条 MBUS_MSG 指令
8	从站响应给主站的数据出现 CRC 校验错误
101	主站的请求中含有从站不支持的功能码
102	从站不支持数据地址：主站"地址"+"计数"所请求的地址范围超出了从站所允许的地址范围

3. 从站库使用说明

<p>Modbus RTU Slave</p>		<p>Mode(BYTE): 启动/停止(1=启动 Modbus, 0=停止 Modbus)</p> <p>Addr (BYTE): 从机地址 (1~247)</p> <p>Baud (DWORD): 支持波特率 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200</p> <p>Parity (BYTE): 0=无, 1=奇校验, 2=偶校验</p> <p>Delay (INT): 附加字符间超时, 默认值 0 毫秒 (注: 暂时不支持该功能, 仅作为功能拓展预留口, 填任意参数都可以)</p> <p>MaxIQ (INT): I 和 Q 位最大数目</p> <p>MaxAI (INT): 输入寄存器最大数目 (模拟输入字)</p> <p>MaxHold (INT): 保持寄存器最大数目 (V 区字)</p> <p>HoldStart (DWORD): 保持寄存器在 V 区中的起始地址</p> <p>Done (BOOL): 初始化完成标记</p> <p>Error (BYTE): 初始化错误码 (0=无错误)</p>
		<p>Done (BOOL): 1=处理 Modbus 通讯数据</p> <p>Error (BYTE): 错误码 (0=无错误)</p>

3.1 从站 MBUS_INIT 执行错误代码

错误码	说明
0	无错误
1	内存范围错误: MaxIQ、MaxAI、MaxHold + HoldStart 等参数超出 CPU Q 区, I 区, AI 区, V 区定义的范围大小或 HoldStart 参数非法
2	该波特率或奇偶校验不被支持: 奇偶校验支持 0=无校验, 1=奇校验, 2=偶校验 波特率支持 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
3	从机地址非法: 支持地址 1~247

4	Mode 参数非法： 0=启用 Modbus ， 1=禁止 Modbus
5	保存寄存器地址与指令库存储区分配地址重叠
6	主从站奇偶校验错误
7	从站接收主站的请求数据帧时发生 CRC 校验错误
8	非法功能码/非法请求，从站支持 1,2,3,4,5,6,15,16 功能码
9	请求中含有非法内存地址即主站 MBUS_MSG 的请求参数“Addr+Count”超出从站的范围
10	MBUS_INIT 库指令未执行或初始化不成功

4.注意事项：

1. 烧录集成 Modbus 库固件的 CPU 上同时兼容新版 Modbus 库和西门子的 Modbus 库。
2. 新版 Modbus 库包括端口 0、端口 1 的 Modbus 主站及从站指令。可支持端口 0、端口 1 的 Modbus 主站和从站功能。主站库存储区大小需要 36 字节，从站库存储区大小需要 33 个字节。
3. 新版 Modbus 库使用时，库存储区小，占用程序空间小，可应用于通信频率高、数据传输量大、需要与多个从站建立通信的组态环境，可以有效避免因为通信负荷过大导致主从站通信失败的情况；也可应用于需要端口 1 做 Modbus 从站通信的场合。