

A man in a light blue shirt is seen from the side, holding a tablet. He is in a factory environment with various industrial equipment and a clock in the background. Overlaid on the image are several digital graphics: a '24/7' icon with a circular arrow, a 'NEWS' icon with a person silhouette, a 'Home' icon with a house, and a 'Industry Online Support' icon with a network diagram. The background is a blurred factory floor with overhead lights and a clock on the wall.

SIEMENS

Ingenuity for life

SMART Modbus 轮询

STEP 7-Micro/WIN SMART V3

<https://w2.siemens.com.cn/smart/Download>

法律信息

应用示例的使用

应用示例说明了通过文本、图形和/或软件模块形式的几个组件的交互来解决自动化任务。应用示例是西门子（中国）有限公司或其子公司（“西门子”）提供的免费服务。所有应用示例均“按现状”予以提供，且不提供保修、赔偿、支持或其他承诺。应用程序示例仅对典型任务提供帮助；它们不构成客户特定的解决方案。您有责任按照适用的法律法规正确和安全操作产品，还必须检查相应应用示例的功能并根据您的系统进行定制。您亦应当遵循警告、安全说明以及任何其他依法使用的信息（如适用），例如通用条件、文档或操作说明。

西门子授予您非排他性的、不可再许可的和不可转让的权利，由经过技术培训的人员、为您的内部业务目的使用应用示例。未经西门子书面许可，您不得将应用示例用于任何外部或商业用途，亦不得(i)转售、转移、分许可、发布、出借或出租任何应用示例或为任何第三方的利益使用；(ii) 修改、更改、篡改、修复；(iii) 逆向工程（reverse engineer）、反汇编（disassemble）、反编译（decompile）或以其他方式试图发现任何应用示例的源代码；(iii) 将任何应用示例用于开发或增强与该产品有竞争关系的任何竞争产品；或 (vi) 删除任何产品中包含或随附的任何专有声明或图例。您对应用示例的使用还应遵守附件的“可接受的使用政策”。

对应用程序示例的任何更改都由您负责。该应用实例无须接受收费产品的习惯测试和质量检验；它们可能具有功能和性能缺陷以及错误，其所包含的功能未必能满足您的要求。您有责任据此设计您的使用机制并以恰当的方式使用它们，从而确保可能发生的故障均不会导致环境、财产损失或人身伤害。

免责声明

西门子不基于任何法律原因而对应用示例的使用承担任何责任，包括但不限于应用示例的可用性、完整性和无缺陷性以及相关信息、配置和性能数据及其造成的任何损害。这不适用于适用法律有强制性规定的情况，或故意、重大过失造成的人身伤害。上述规定并不意味着对您不利的举证责任的任何改变。对于第三方因您使用应用示例而提出的任何索赔，您应向西门子作出赔偿，除非西门子负有法定赔偿责任。

通过使用应用示例，您承认西门子对上述责任条款之外的任何损害不承担责任。

知识产权

应用示例及其所有权利，但不限于其中的专有权利(包括但不限于应用示例中包含的源代码、目标代码、图片、照片、动画、视频、音频、音乐、文本和小程序)、随附材料和每份副本，以及其中的所有知识产权(包括任何版权、专利、商标、商业秘密和公开权)均归西门子、其许可方或关联公司所有。除非本文档明确规定，西门子未就上述知识产权向您明示或默示授予任何权利。您同意，对于任何因您使用应用示例而引发的知识产权侵权索赔或诉讼或与之相关的任何其他损害，应由您(而非西门子)全权负责。

其他信息

西门子保留随时更改应用示例的权利，无需另行通知。如果应用实例中的建议与其他西门子文档(如目录)之间存在差异，则应优先考虑其他文件的内容。

如您发现应用示例的任何问题或缺陷，请及时与西门子取得联系。西门子会在技术可行和商业合理的范围内，自行决定调查和修复任何问题或缺陷，为您提供支持。

安全信息

西门子提供具有工业安全功能的产品和解决方案，支持工厂、系统、机器和网络的安全运行。

为了保护工厂、系统、机器和网络免受网络威胁，有必要实施——并持续维护——一个整体的、最先进的工业安全概念。西门子的产品和解决方案构成了这一概念的一个元素。

客户有责任防止对其工厂、系统、机器和网络的未经授权的访问。

这些系统、机器和组件只应在必要的情况下连接到企业网络或 Internet，并且只有在适当的安全措施(例如防火墙和/或网络分割)到位的情况下才应连接到这种连接。有关可能实施的工业保安措施的其他资料，请浏览 <https://www.siemens.com/industrialsecurity>。

西门子的产品和解决方案经过不断的发展，使其更加安全。西门子强烈建议，一旦产品更新可用，就立即应用产品更新，并使用最新的产品版本。使用不再受支持的产品版本以及未能应用最新更新可能会增加客户遭受网络威胁的风险。

了解产品更新，请订阅西门子工业安全 RSS <https://www.siemens.com/industrialsecurity>。

西门子已建立接收西门子产品和解决方案安全漏洞信息的平台。您可以通过向 productcert@siemens.com 或 src.cyscn.cn@siemens.com 发送邮件的方式报送您发现或遇到的西门子产品和解决方案的安全漏洞。西门子将在 <https://www.siemens.com/industrialsecurity> 上不时公布西门子产品和解决方案的安全漏洞和修补措施（如有）。用户应定期访问上述网站并及时采取相关修补措施。西门子强烈建议用户在上述网站登记并订阅 Security Advisory，从而以获取关于最新的安全漏洞和修补措施的及时推送。

可接受使用政策

本可接受使用政策（简称“AUP”）规定了您和您的代表在使用我们的产品和服务时必须遵守的条款。

1. 凭证

您应：

- 不得使用虚假身份获取产品和服务的访问权限；
- 妥善保管和保护访问凭证和安全令牌，不得用于未经授权的访问、披露或使用；
- 不得通过任何其他方式（即在用户账户或其他我方允许方式以外）获取产品和服务的访问权限；
- 不得规避或披露贵方用户账户的验证和安全机制、底层技术或与之相关的任何主机、网络或账户信息等；
- 确保任何访问凭证仅由被授权人员使用且不得与其他人共享。我们有权根据合理性和必要性判断，自行决定更改相关访问凭证。

2. 无非法、有害或攻击性使用或内容

您不得自己或鼓励、鼓动、协助或指示他人将产品和服务用于任何非法、有害或攻击性用途，或传输、存储、展示、分发或以任何其他方式提供非法、有害、欺诈、侵权或攻击性的内容。您对产品和服务的使用和存储在产品和服务中的内容均不得：

- 违反任何国家、地区的法律、法规；
- 侵犯他人权利；
- 以任何方式（包括提供或传播假冒商品、服务、方案或促销活动、快速赚钱计划骗局、庞氏骗局或传销、网络钓鱼、网域嫁接骗局或其他欺骗手段）危害他人或我们的声誉；
- 在贵方自己的内容中针对任何非法或您无相应授权的外部网站或数据源（包括嵌入式小工具）进行输入、存储或发送超链接，或提供访问权限或任何其他访问方式；
- 具有诽谤、淫秽、侮辱或侵犯隐私权的行为或性质。

3. 无违反使用限制

您不得：

- 针对产品和服务进行转售、转让、再许可、出借、出租或发布、或将产品和服务用于运营业务流程外包或其他外包或分时服务（经我们明确允许的情形除外）；
- 针对产品和服务或其底层技术进行逆向工程、反汇编、反编译或以其他方式修改、合并、篡改、修复、或试图发现其源代码（与您所在地区适用法律存在冲突时除外）；
- 攻击、干扰、扰乱或不利影响任何服务、硬件、软件、系统、网站或网络，包括但不限于使用大量自动化手段（包括机器人、爬虫、脚本或类似的数据收集或提取方法）访问或攻击任何服务、硬件、软件、系统、网站或网络；
- 传输任何数据、发送或上传任何包含病毒、蠕虫、特洛伊木马、网络定时炸弹、键盘记录器、间谍软件、广告软件或任何其他有害程序或类似的旨在对任何计算机硬件或软件的操作或安全产生不利影响的计算机代码；
- 从任何被适用的制裁和/或（再）出口管制法律和法规（包括中国、欧盟、美国和/或任何其他适用国家的此类法律和法规）禁止或制裁或有许可要求的地点访问产品和服务，并且您应仅上传非受控的内容（例如，在欧盟的分类为“N”，而在美国 ECCN 为“N”或“EAR99”），适用的（再）出口管制法律和法规或相应政府许可或批准另行允许的情形除外。

4. 无滥用

您不得：

- 出于避开或绕过任何使用限制（例如访问和存储限制）、监控或避免产生费用等目的使用产品和服务；
- 出于性能测试、构建竞争产品或服务或复制其功能或用户界面等目的访问或使用产品和服务；
- 干扰我们系统的任何正常功能或安全；
- 分发、发布、发送或协助发送任何未经许可的群发邮件或其他消息、促销活动、广告或招徕信息（包括商业广告和信息通知）。未经发送人明确许可，您不得修改或隐藏邮件标题或假冒发送人身份发送邮件。

5. 无安全违规

您不得以可能对产品和服务或其底层技术造成或促成安全威胁的方式使用产品和服务。特别是，您应：

- 采取合理措施，预防和抵御针对您用于连接和/或访问产品和服务的自有系统、本地硬件、软件或服务相关的任何安全攻击、病毒和恶意代码；
- 未经我方事先书面明确同意，不得针对产品和服务或其底层技术进行任何渗透测试；
- 不得使用不符合行业标准安全政策（例如密码保护、病毒防护、更新和补丁级别）的设备访问或使用产品和服务。

6. 我方监控和报告

您确认我们及我们的分包商有权通过产品和服务监控您的 AUP 遵守情况。我们保留对任何违反本 AUP 的行为进行调查的权利。如果您了解任何违反本 AUP 的行为，应立即通知我们，并应我们请求提供相应协助，用

以阻止或缓解相应违反行为或进行相关补救。我们有权删除、禁止访问或修改任何违反本 AUP 或其他贵方与我方之间有关产品和服务使用的协议的内容或资源。我们有权向相关执法机关、监管机构或其他相关第三方举报任何我们怀疑的违法或违规行为。如有第三方声称您对产品或服务的使用或您的内容侵犯了其权利或违反任何法律或法规，我们有权与其共享相关客户信息。

7. 版权

西门子将按照其版权政策，对有关内容的版权侵权通知作出回应。您可通过相关西门子关联公司网站或访问产品和服务的网站获取该政策的网络链接。

目录

- 1 应用概述..... 6
 - 1.1 通用描述 6
 - 1.2 硬件及软件需求 6
- 2 程序功能..... 7
 - 2.1 程序架构 7
 - 2.2 轮询控制 8
 - 2.3 单站读写 9
 - 2.4 多站读写 12
- 3 扩展及优化..... 14
 - 3.1 程序扩展 14
- 4 更新日志..... 15

© Siemens AG 2025 All rights reserved

1 应用概述

1.1 通用描述

Modbus-RTU 协议是一种开放的串行通信协议，在不同的行业中都有非常广泛的应用，因为其是串行通信，所以其报文的传送需要按照串行队列来发送，而具体到 S7-200 SMART 的 Modbus-RTU 主站通信的编程中就需要考虑针对不同地址和不同站的轮询的问题，为了提高轮询的效率和轮询程序的通用性，本文推出了 Modbus 轮询的应用库，可以简化用户轮询编程，也可以实现根据需要写入功能，更可以实现仅当设定值改变时的参数值写入功能。

该功能库更新功能类型，增加传输数据量，提供从站通讯开关，细化不同的通讯架构和方法。

该轮询样例适用于单站或少数从站，每个站有多个通讯地址，和多站连续地址，或者多站少数不连续地址的情况。该功能分别支持 31 个地址片区的读取和写入。

1.2 硬件及软件需求

本应用软硬件的需求

为了使得本应用案例成功运行，必须满足以下硬件和软件需求。

硬件

- S7-200 SMART PLC V3.0.1
- SIMATIC SMART LINE V5

软件

- Micro/WIN SMART V3.0.1
- WINCC Flexible SMART V5

2 程序功能

2.1 程序架构

简要说明

程序中包括单站多地址和多站单地址的数据轮询。

该程序通过监控单个变量的数值变动或变量数组的数据变动，触发写入操作，在没有写入需求时执行实时读取操作。

同时通过 ModbusQueue 控制数据读写轮询。

程序内容

样例程序架构如下：

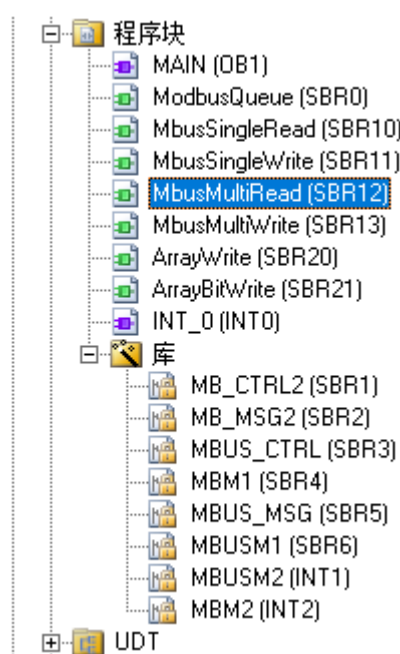


图 2.1.1 程序架构

2.2 轮询控制

简要说明

ModbusQueue 子程序控制读写轮询。
当没有写入需求时，会实时读取数据，当有写入需求时，优先写入。

调用方式

对每一个物理端口分别调用 ModbusQueue 子程序，分别控制每一个连接的轮询。

引脚内容

引脚的含义和注意事项如下：

	变量名	地址	变量类型	数据类型	注释
1	EN		IN	BOOL	
2	readStart	L0.0	IN	BOOL	读取触发
3	writeType	L0.1	IN	BOOL	0-Single, 1-Mult
4			IN		
5	write	L0.2	IN_OUT	BOOL	触发时写入数据
6	readDone	L0.3	IN_OUT	BOOL	读取MSG完成
7	writeDone	L0.4	IN_OUT	BOOL	写入MSG完成
8	readCtrl	LD1	IN_OUT	DWORD	V区或M区读取顺序变量，最多31个站或地址
9	writeCtrl	LD5	IN_OUT	DWORD	V区或M区写入顺序变量，最多31个站或地址
10	lastQueue	LD9	IN_OUT	DWORD	外部中间变量，用于保存上一读写状态
11			IN_OUT		
12			OUT		
13			TEMP		

图 2.2.1 ModbusQueue 引脚

控制逻辑

当 readStart 引脚被激活时，程序开始读取轮询，可以通过开机扫描或上升沿触发，该引脚仅可触发一次。
当 write 引脚被触发时，该轮询控制程序会优先触发写入操作，在完成当前读取指令后，会优先进入写入序列，并保留读取序列。
readDone 和 writeDone 引脚应从读写的程序块中获取。

2.3 单站读写

简要说明

该部分介绍单站不连续多地址的读写轮询和少数从站多地址的轮询。

程序调用

调用逻辑如下

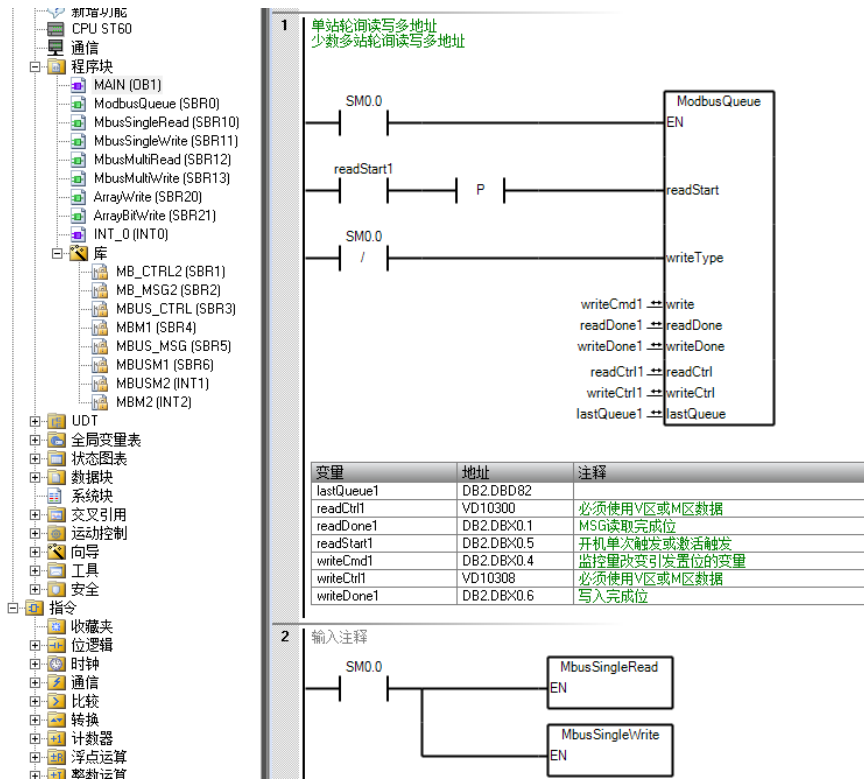


图 2.3.1 单站轮询程序调用

通讯激活

在读取轮询中，调用 MBUS_CTRL 指令库，激活 Modbus 通讯。

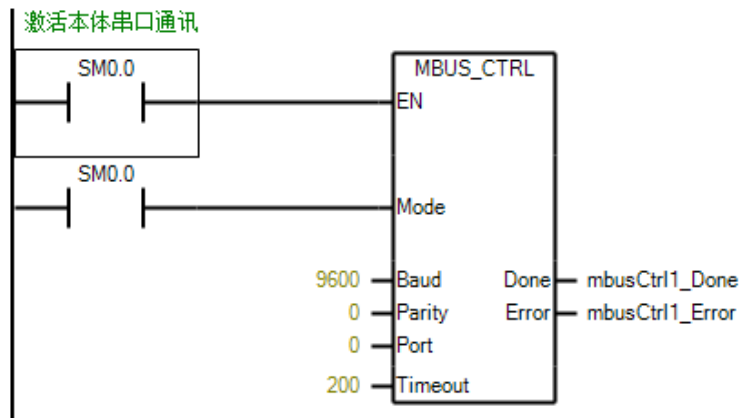


图 2.3.2 通讯激活

通讯配置

将重试次数设置为 0，避免 Modbus 从站通讯掉站后出现通讯阻塞的情况。

重试次数的变量地址可在全局变量表中的 Modbus RTU Master 库变量中查询，变量名称为 mModbusRetries，为库地址偏移 257 字节地址。

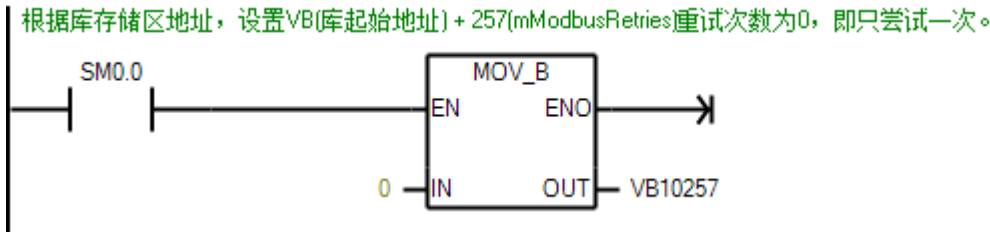


图 2.3.3 通讯配置

读取编写

基于从站数量和不连续地址区数量编写读取程序，

读取的控制字顺序应考虑到字节的高低位变化。

如下图所示，左侧红色框中的变量为读取顺序控制字，通过 M 区或 V 区变量控制该字符循环移位，以此控制顺序读取。

该顺序读取变量在 ModbusQueue 轮询块中作为输入输出引脚使用。

在 MBUS_MSG 块中输入不同的从站站号和 Modbus 地址，并配置合适的读取数量及保存在 PLC 中的地址。

读取程序块数量限制为 31 个。

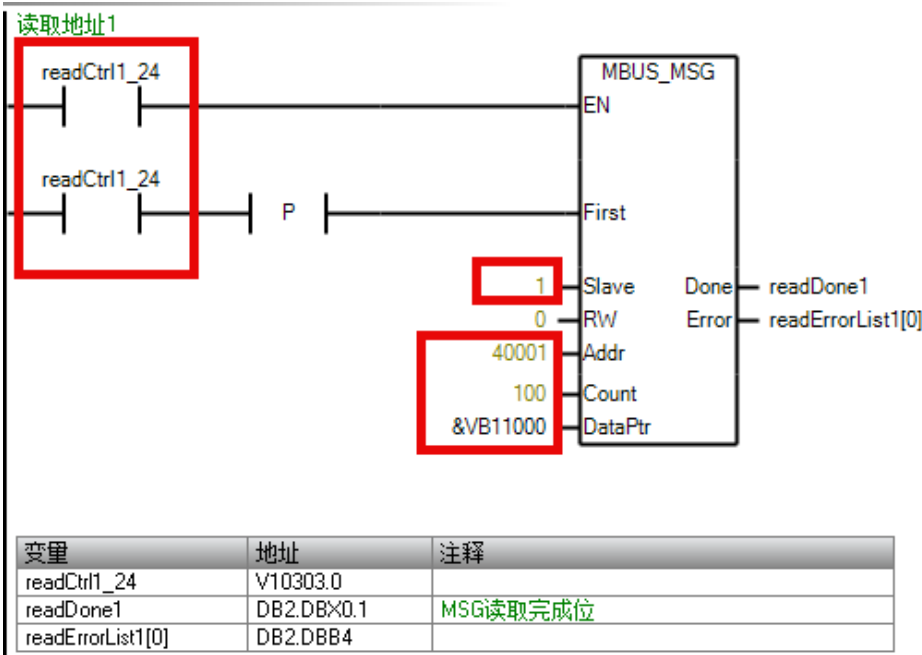


图 2.3.4 读取程序

写入程序

基于从站数量和不连续地址区数量调用 ArrayWrite 和 ArrayBitWrite 程序块，

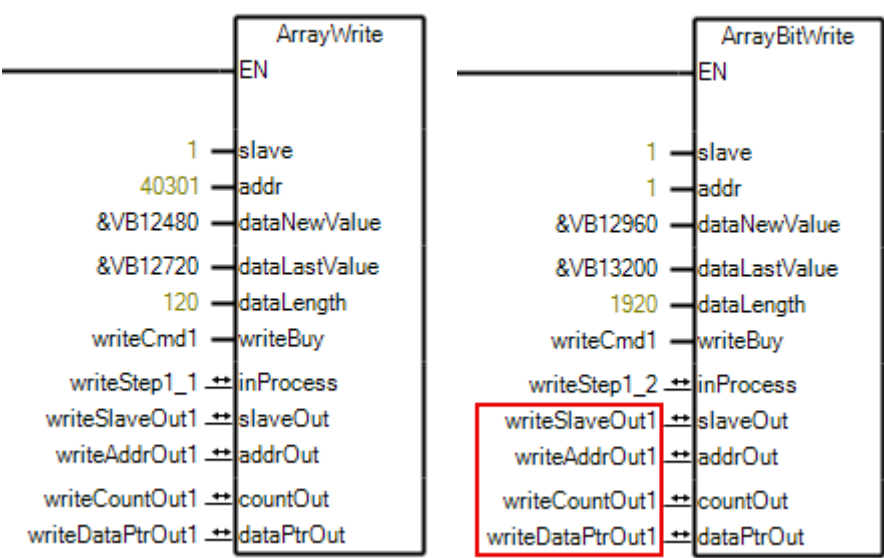


图 2.3.5 写入程序对比块

slave	LB0	IN	BYTE	从站站号
addr	LD1	IN	DWORD	写入从站地址
dataNewValue	LD5	IN	DWORD	监控变量连续地址
dataLastValue	LD9	IN	DWORD	内部保存变量连续地址
dataLength	LD13	IN	DWORD	不得大于120
writeBuy	L17.0	IN	BOOL	任一写入监控块写入指令激活时触发
		IN		
inProcess	L17.1	IN_OUT	BOOL	该监控块写入指令激活
slaveOut	LB18	IN_OUT	BYTE	中间变量，统一用于写入MSG块
addrOut	LD19	IN_OUT	DWORD	中间变量，统一用于写入MSG块
countOut	LW23	IN_OUT	INT	中间变量，统一用于写入MSG块
dataPtrOut	LD25	IN_OUT	DWORD	中间变量，统一用于写入MSG块

图 2.3.6 写入程序块引脚

上述引脚中，应根据不同的地址区和不同的从站配置这两个程序块，即每一个需要写入的从站及地址区都需要一个相对应的程序块。例如，存在 3 个从站，需要同时写入 40301 这个地址段，则需要调用 3 次 ArrayWrite 程序块，若存在 2 个从站，一个从站存在 40301 和 40501 两个地址段，另一个从站存在 40301 地址段，则同样需要调用 3 次 ArrayWrite 程序块。

上图中红色框中的引脚用于 Mbus_MSG 写入程序块。

连续地址的数据对比会消耗 PLC 的资源，提高总体的扫描时间。400 个变量的数据对比的耗时大约在 2s 左右，具体的时间和资源消耗应考虑实际项目。

2.4 多站读写

简要说明

多站读写的程序逻辑与单站读写的程序逻辑类似。区别在于应用场景不同，写入时往往是对不同从站的同一地址进行写入操作，适用于一带多且是同一型号的从站。
多站轮询可以通过画面控制激活。

程序调用

程序的调用与单站读写相同。

通讯激活

通讯激活与单站读写相同。

通讯配置

通讯配置与单站读写相同。

读取程序

读取程序可以通过 slaveEnable 变量控制从站激活功能。

写入程序

通过某个控制条件触发后，会循环移位写入变量，并通过该变量的不同位控制写入通讯。
对于每一个从站或每一个从站地址，都需要单独配置一个写入程序块，并在每一个写入程序块中配置相应的地址。
每一个写入块都可以通过 slaveEnable 变量控制是否激活该从站。
若地址和数据长度一致，可使用同一变量设置地址。

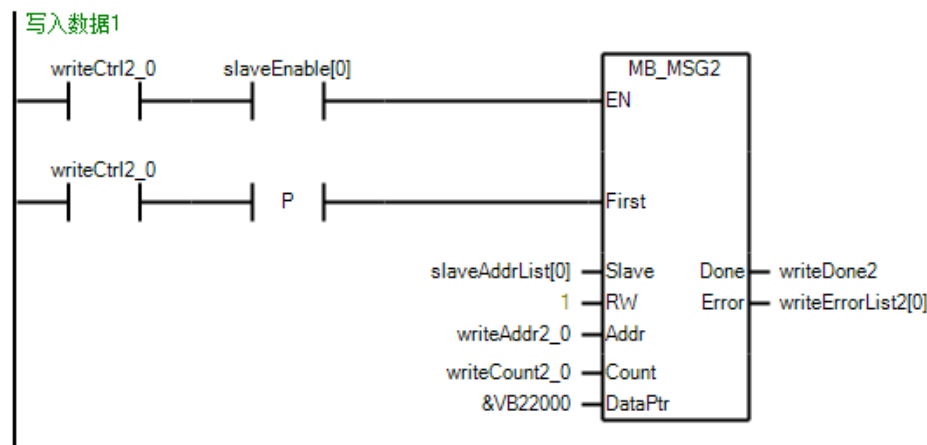


图 2.4.1 写入程序块引脚

控制画面

通过控制画面设置从站的站号，并可通过启用按钮激活该从站的数据通讯。

从站 1

站号

激活

从站2

站号

激活

从站3

站号

激活

从站4

站号

激活

从站5

站号

激活

从站6

站号

激活

从站7

站号

激活

从站8

站号

激活

主界面

图 2.4.2 从站控制画面

3 扩展及优化

3.1 程序扩展

从站数量

通讯目标地址数量限定为 31 个，当不连续地址或从站数量超出限制时，建议整理数据地址或者使用多个轮询块拼接。

参数对比

当触摸屏上修改参数，并写入从站时，建议增加参数修改按钮，通过该修改按钮状态的修改，触发数据写入操作。

数据对比数量多时，会影响程序扫描周期，测试 400 个变量增加的通讯周期大约在 2s 左右。

从站属性

在一对多的 Modbus RTU 通讯中，可以通过触摸屏设置从站的通讯属性，包括从站的站号、地址、数据长度等。

适用于主站连接的从站类型相同，数据结构一致的情况。

触摸屏功能拓展

可以通过 SMARTLINE 的数据传输功能收发数据，通过组态的方式快速传输数据。

4 更新日志

版本& 日期	更新描述
V1.0.0 07/2025	