

PLC-Recorder

用户手册

手册版本：V1.8.2 2/2021

软件版本：V1.8.2

一个用于 PLC 信息录波和分析的软件

目录

1. 软件概述.....	5
1.1. 功能特点.....	5
1.2. 支持设备或协议.....	6
1.3. 主要参数.....	7
1.4. 新版功能变化.....	7
1.5. 安全与提醒.....	8
1.6. 支持.....	9
2. 名词和基本概念.....	10
2.1. 名词.....	10
2.2. 基本概念.....	10
2.2.1. 数据类型及长度对照（部分）	10
2.2.2. 变量的状态及切换.....	11
2.2.3. 网络 7 层模型.....	11
2.2.4. TCP/IP 协议.....	12
2.2.5. TCP 协议.....	12
2.2.6. 工业以太网.....	12
3. 安装和运行.....	15
3.1. 需要环境.....	15
3.2. 安装过程.....	15
3.3. 目录文件说明.....	16
3.4. 软件升级方法.....	16
3.5. 授权.....	16
3.5.1. 硬件授权.....	17
3.5.2. 授权码.....	17
3.6. 如何建立数据文件的关联？	18
4. 配置.....	19
4.1. 通道配置.....	19
4.1.1. 通道参数.....	19
4.1.2. 变量导出.....	21
4.1.3. 变量导入.....	21
4.1.4. 数据文件.....	24
4.1.5. 记录模式.....	25

4.2. 变量配置.....	28
4.2.1. 简介.....	28
4.2.2. 非显示变量列表.....	28
4.2.3. 显示变量列表.....	28
4.2.4. 变量操作.....	29
4.2.5. 变量的可配置信息.....	29
4.2.6. 批量添加变量.....	30
4.3. 字符串变量.....	30
4.4. 配置的保存和打开.....	31
5. 采集.....	32
5.1. 采集过程.....	32
5.2. 软件界面的操作.....	33
5.2.1. 最小化和退出.....	33
5.2.2. 录波窗口置顶.....	33
5.3. 字符串采集.....	33
5.4. 数据保存.....	33
5.5. 通讯状态监控.....	34
5.6. 仿真.....	34
6. 数据转发.....	35
6.1. 功能说明.....	35
6.2. 启用和停止方法.....	35
6.3. 客户端开发.....	36
7. 显示和分析.....	37
7.1. 数据显示.....	37
7.2. 显示区域和功能选项.....	37
7.3. 曲线高度的拖拽.....	39
7.4. 显示格式.....	40
7.5. Y 轴局部自适应功能.....	40
8. 文件管理.....	41
9. 快捷键.....	42
10. 常见问题 (FAQ)	43
10.1. 连接问题.....	43
10.1.1. 如何确认 PLC 是否可以访问?	43
10.1.2. 如何判断连接是否成功?	43
10.1.3. 连接失败怎么办?	44

10.2. 系统.....	44
10.2.1. 录波时，软件的 CPU 负荷占用过大，甚至卡顿.....	44
10.2.2. 如何使软件永久获得管理员权限？	44
10.2.3. Windows XP SP2 下的安装方法.....	45
10.3. 图形操作.....	45
10.3.1. 如何修改变量在波形上的高度？	45
10.3.2. 如何测量信号的长度？	45
10.3.3. 如何将数据导入 excel？	45
10.3.4. 如何合并多个波形文件？	45
10.4. 窗口显示大红叉，怎么办？	46
11. 软件版本更新说明.....	47
附录 1 各品牌设备的地址规范.....	51
1. AMSAMOTION 艾莫迅.....	51
2. Beckhoff 倍福.....	52
2.1. 符号地址：	52
2.2. 绝对地址：	52
2.3. 默认通道参数.....	52
2.4. 倍福通讯设置示意.....	53
2.5. 倍福通讯 ADS 通讯的一些经验.....	56
2.6. 故障代码.....	57
3. DELTA 台达.....	60
3.1. 地址对照表.....	60
3.2. 默认通道参数.....	60
4. Keyence 基恩士设备.....	61
4.1. 地址对照表.....	61
4.2. 默认通道参数.....	61
5. INOVANCE 汇川.....	62
5.1. 地址对照表（H3U、H5U、XP 系列）	62
5.2. 地址对照表（AM400_800）	62
5.3. 默认通道参数.....	62
6. MITSUBISHI 三菱设备.....	64
6.1. MC(Binary)、MC(ASCII)协议.....	64
6.2. A1E 协议.....	64
6.3. FxSerialTcp 协议.....	65
6.4. 默认通道参数.....	65

6.5. 三菱 PLC 设置示意.....	66
7. 标准 Modbus-TCP 设备.....	73
7.1. 通用说明.....	73
7.2. 默认通道参数.....	73
8. Omron 欧姆龙设备.....	74
8.1. Fins-TCP 协议.....	74
8.2. CIP 协议.....	74
8.3. 默认通道参数.....	74
9. Rockwell 罗克韦尔 (AB) 设备.....	75
9.1. 地址规范.....	75
9.2. 默认通道参数.....	76
10. RunPower 蓝普峰.....	77
11. Panasonic 松下设备.....	78
11.1. Mewtocol 协议.....	78
11.2. MC(Binary).....	79
11.3. 默认通道参数.....	79
12. Schneider 施耐德.....	80
12.1. Quantum (昆腾)	80
12.2. Premium (奔腾系列)	81
12.3. M580.....	82
13. SIEMENS 西门子设备.....	83
13.1. 地址规范.....	83
13.2. 默认通道参数.....	83
13.3. 其他相关信息.....	84
附录 2 变量导出文件格式.....	92
附录 3 转发信息交互的过程.....	93
附录 4 转发电文格式.....	94

1. 软件概述

1.1. 功能特点

欢迎使用 **PLC-Recorder** 软件，该软件用于连续采集 PLC (及其他符合相关协议的设备，比如 Modbus-TCP 协议的仪表设备、采集模块等。为描述方便，后面统称为 PLC) 的信息，并可以进行后续的分析。本软件自带驱动，不需要安装任何 PLC 厂家软件 (倍福除外)。可以同时对于多个 PLC 进行采集。本软件仅读取 PLC 内的信息，没有任何写入操作，因此，本软件不会对 PLC 内的数据和信息进行任何修改。

应用场景 (不限于)：

- ✓ 协助 PLC 调试
- ✓ 协助进行 PLC 系统故障分析、偶发故障追踪
- ✓ 工艺数据的记录、生产优化
- ✓ 全员生产维护 (TPM)、效能评估 (OEE)、质量保证 (QA)
- ✓ 重要数据长期存档
- ✓ 设备维护、改进、培训

1.2. 支持设备或协议

大类	设备系列/型号/协议	本软件对应 系列/型号/协议
AMSAMOTION 艾莫迅	ETH-AMX-FX3U 等带有以太网的系列	三菱 FxSerialTcp
Beckhoff 倍福	TwinCAT2、TwinCAT2 (需要 TwinCAT 环境)	对应系列
DELTA 台达	DVP 系列	Modbus-Tcp 标准
Keyence 基恩士	MC(Binary)和 MC(ASCII)协议	对应协议
INOVANCE 汇川	H3U、H5U、AM 系列	Modbus-Tcp 标准
MITSUBISHI 三菱	MELSEC 系列：MC (Binary)协议、MC(ASCII) 协议、A-1E 协议、FxSerialTcp	对应协议
Modbus-Tcp 设备	各种数据采集器、仪表等	标准
Omron 欧姆龙	Fins-TCP 协议、CIP 协议	对应协议
Rockwell 罗克韦尔(AB)	ControlLogix5000、Micro800	对应系列
RunPower 蓝普峰	RPC2000 系列	Modbus-Tcp 标准
Panasonic 松下	Mewtocol 协议、MC (Binary)协议	对应协议
Schneider 施耐德	施耐德 PLC：昆腾系列、奔腾系列、M 系列 PLC	施耐德 Modbus-Tcp 标准
SIEMENS 西门子	S7-200、S7-200SMART、S7-1200、S7-1500、S7-300、S7-400	对应系列
	840D 及 840Dsl	S7-300
	S7-PLCSIM *1)	所仿真的 PLC 系列
	S7-PLCSIM Advanced	S7-1500

说明

本软件仅支持以太网通讯。

如果没有找到想要通讯的设备类型，可以查看该设备支持的通讯协议，并选择符合该协议的设备类型进行通讯尝试。比如：基恩士的设备如果支持 EtherNet/IP™，则可以用 AB 的设备类型进行尝试。另外，大部分的 PLC 都支持 Modbus-TCP 协议，因此，也可以作为一种替代访问方式。

*1)：S7-PLCSIM 需要利用 NetToPLCsim 进行协议转换，[实施步骤请参考文献](#)。

1.3. 主要参数

- ✓ 时间单位：精确到毫秒(ms)
 - ✓ 同时采集的变量数量：20-无限^{*1)}
 - ✓ 同时采集的通道数量：2-16^{*1)}
 - ✓ 连续记录时长 (小时)：6-无限^{*1)}
 - ✓ 转发功能：同时服务的客户端数量：0-4 个^{*1)}
-

说明

^{*1)}: 与授权类型有关

1.4. 新版功能变化

- ✓ 增加西门子 STEP7、博图项目数据块内变量导入功能。
- ✓ 开关量可实心显示 (bar 图)。
- ✓ 转发优化：增加了仅转发，不本地存储的功能。
- ✓ 基恩士变量访问格式优化，大部分变量可以按照 PLC 内的格式进行访问。
- ✓ 松下驱动优化。
- ✓ 欧姆龙 CIP 访问优化。
- ✓ 变量配置窗口优化：数据类型上动态提示 PLC 内的对应类型。
- ✓ 修正其他已经发现的错误。

1.5. 安全与提醒

- ！ 在开始记录时，本软件与 PLC 建立通讯连接，因此，用户需要确认该操作不会导致 PLC 的通讯资源用到极限而给正常的控制通讯带来危害。
- ！ 在通讯速率有限，或者节点较多，或者极其繁忙的网络里，如果本软件的采集速度过快，会抢占资源而导致其他站点的通讯受到影响，如果发现这种现象，请降低采样的速度。
- ！ 本手册的内容可能与实际界面和功能有出入，望谅解。
- ！ 除非指定的 PLC，本软件不会发生任何其他通讯。如果发现广告、其他链接等异常行为，可能威胁控制网络的安全，请从正式渠道获取本软件。
- ！ 本公司不对软件使用过程中发生的损失负责。
- ！ 如果遇本软件功能范围内的问题：请查看本手册，如果无法解决，请到官网查看软件是否已经升级，并尝试最新版软件。如果依然无法解决问题，请加入 QQ 群反映，或发邮件给下面的支持邮箱（service@HiddenMap.cn 附带：问题描述故障信息文件、出问题时的波形文件），核实后，您将获得奖励（具体措施以官网为准）。

1.6. 支持

官 网： www.HiddenMap.cn 提供下载、升级、购买、技术支持等完整服务。

技术交流： QQ 群（群号见官网），正式客户可以申请进入，申请时，请提供您购买软件时的联系邮箱。

感谢群友的大力协助：

*Jun (932507362), JingshengMao (422302625), 昆山-似水流年 (767368092), 星空 (414552306),
Paul (1246384221)、信念 (1838701584)、NULL (136044669)、37 嘉い凍結媛 (543491567)、
浪迹天涯 (516736044)、GangLiu (多伦多)、陈中、海马 (3357161997)、大成 (852491929) 等等。*

版权所有 (All rights reserved)：

上海隐图智能科技有限公司
Shanghai Hidden Map Intelligent Technology Co., Ltd.
2019-2021

电话： +86-(0)21-6877 6656

Email: service@HiddenMap.cn
Web: www.HiddenMap.cn



2. 名词和基本概念

2.1. 名词

名词	含义
通道	每个待采集的设备称为一个通道
变量	<p>每个需要采集的数据称为一个变量，变量包括名称、起始地址、数据类型、所属通道、显示格式等一系列内容。</p> <p>变量是本软件的核心元素，并用于后续的很多分析功能，为避免混淆，变量的名称在项目里是唯一的。</p> <p>依据状态，变量会被保存在不同的位置：导出文档、项目文档、数据文件、非装载列表、已装载列表等，通过导入，导出，装载、卸载等操作可以实现其转换。</p>
项目文件	独立的软件配置、通道配置、变量配置的保存容器，纯文本格式。
数据文件	带有项目文件内容及历史数据的二进制文件，扩展名为“.ihm”。
采集周期	变量的轮询周期。
装载	将变量从不采集状态切换成采集状态。
卸载	将变量从采集状态切换成不采集状态。

2.2. 基本概念

2.2.1. 数据类型及长度对照（部分）

本软件支持类型	长度	控制器数据类型 (西门子) *	控制器数据类型 (AB)
bool	1位	Bool	BOOL
byte	1字节	Byte, USint, Sint	SINT
char		Char	
short (int16)	2字节， 单字	Int	INT
ushort (uint16)		Uint	
int (int32)	4字节， 双字	Dint、Time	DINT、TIMER、 COUNTER、CONTROL
uint (uint32)		UDint	
float (real)		Real	REAL
long (int64)	8字节	Lint	
ulong (uint64)		ULint	
double		LReal	
string	变长	String, WString	

说明

*西门子各系列支持的数据类型不同，具体请参考相关手册。

*各PLC变量类型的英文名称基本一致，中文名称可能不同。

2.2.2. 变量的状态及切换

本软件内部管理的变量可以导出到.csv文件，用于保存和批量处理。也可以在导入到软件里。这个文件遵循PLC-Recorder的内部格式（见[附录2](#)），以免导入出错。

本软件可以导入部分PLC厂家编程软件符号表的导出结果。

在软件内部，变量可能是未使用的，保存在未装载列表内。也可能是处于使用状态，分为显示部分和不显示部分，都将进行采集。变量状态及转换方法见下图。

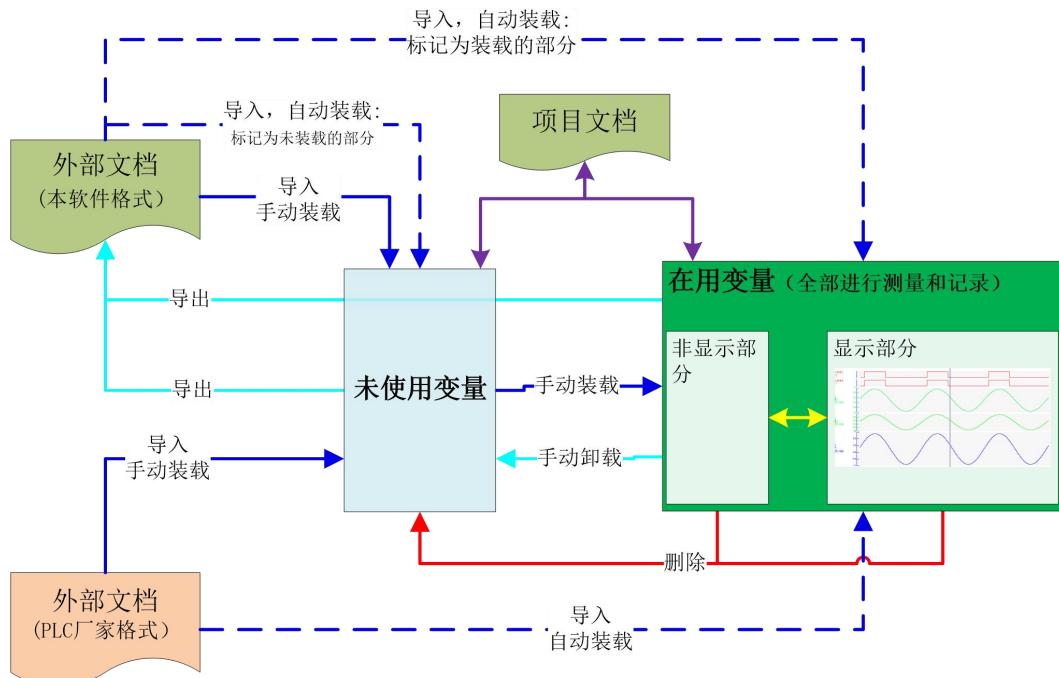


图 2.1 变量保存位置及状态切换图

2.2.3. 网络7层模型

七层模型，亦称OSI（Open System Interconnection）。参考模型是国际标准化组织（ISO）制定的一个用于计算机或通信系统间互联的标准体系，一般称为OSI参考模型或七层模型。

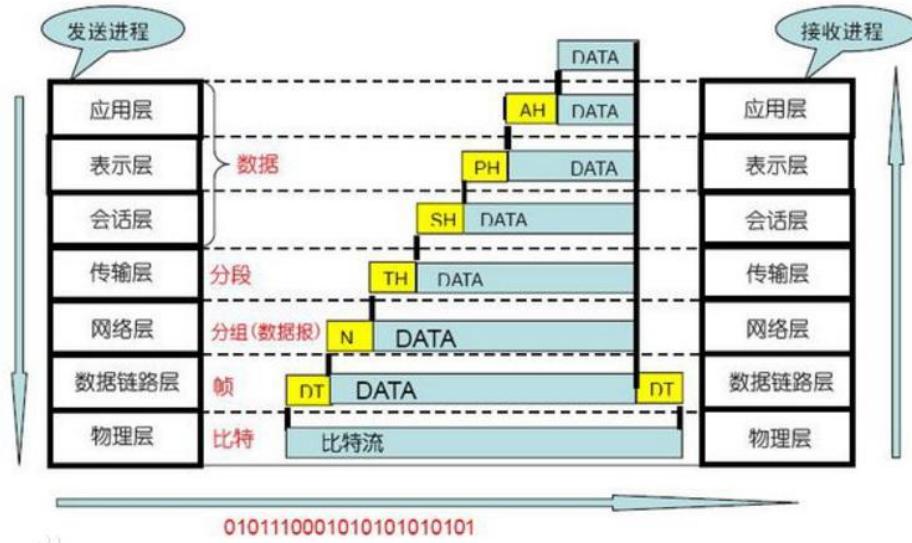


图 2.2 7 层模型

2.2.4. TCP/IP 协议

TCP/IP 协议（传输控制协议/互联网协议）不是简单的一个协议，而是一组特别的协议，包括：TCP，IP，UDP，ARP 等，这些被称为子协议。在这些协议中，最重要、最著名的就是 TCP（传输层的传输控制协议）和 IP。因此，大部分网络管理员称整个协议族为“TCP/IP”。

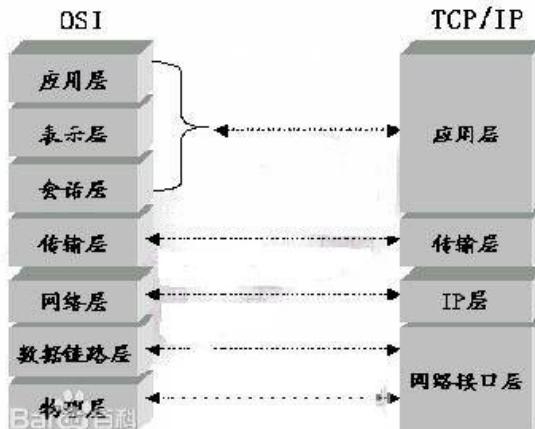


图 2.3 OSI 与 TCP/IP 的关系

2.2.5. TCP 协议

传输控制协议（TCP，Transmission Control Protocol）是一种面向连接的、可靠的、基于字节流的传输层通信协议，由 IETF 的 RFC 793 定义。

2.2.6. 工业以太网

各种工业以太网的区别其实就是协议的区别，其中最主要的还是应用层协议的区别。都是以太网通讯，只是每个公司的叫法不一样，西门子用 Profinet、AB 用

Ethernet/IP、施耐德的 Modbus-TCP。

2.2.6.1. Profinet 协议

Profinet 由 PROFIBUS 国际组织 (PROFIBUS International, PI) 推出, 是新一代基于工业以太网技术的自动化总线标准。

定义了以下三种的通讯协议:

- ✓ TCP/IP 是针对 Profinet CBA 及工厂调试用, 其反应时间为 100ms。
- ✓ RT (实时) 通讯协定是针对 Profinet CBA 及 Profinet IO 的应用, 其反应时间小于 10ms。
- ✓ IRT (等时实时) 通讯协定是针对驱动系统的 Profinet IO 通讯, 其反应时间小于 1ms。

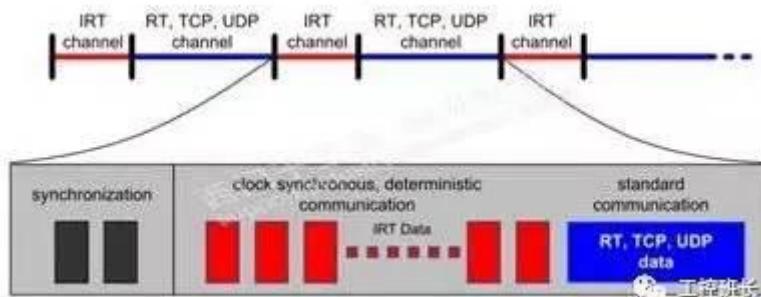


图 2.4 PN 控制器和 PN 设备的分片处理机制

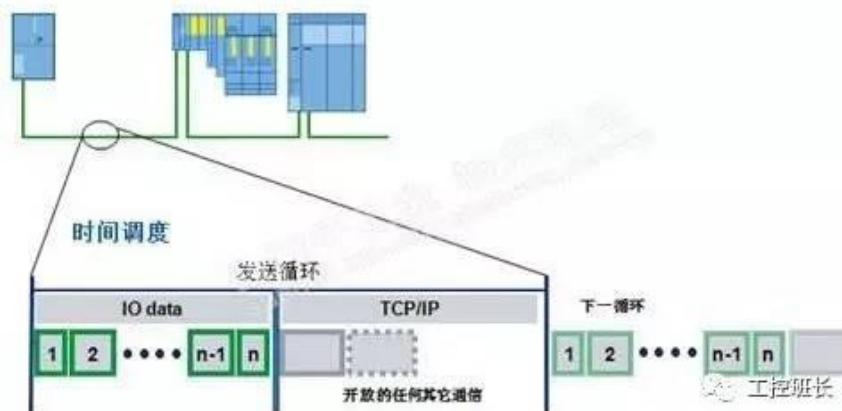


图 2.5 RT 的时间调度机制

2.2.6.2. Modbus-TCP

Modbus-TCP 是简单的、中立厂商的用于管理和控制自动化设备的 Modbus 系列通讯协议的派生产品, 显而易见, 它覆盖了使用 TCP/IP 协议的 “Intranet” 和 “Internet” 环境中 Modbus 报文的用途。协议的最通用用途是为诸如 PLC's, I/O 模块, 以及连接其它简单域总线或 I/O 模块的网关服务的 Modbus-TCP 使 Modbus-RTU 协议运行于以太网, Modbus-TCP 使用 TCP/IP 和以太网在站点间

传送 Modbus 报文, Modbus-TCP 结合了以太网物理网络和网络标准 TCP/IP 以及以 Modbus 作为应用协议标准的数据表示方法。Modbus-TCP 通信报文被封装于以太网 TCP/IP 数据包中。与传统的串口方式, Modbus-TCP 插入一个标准的 Modbus 报文到 TCP 报文中, 不再带有数据校验和地址。

2.2.6.3. CIP 协议

控制及信息协议(CIP)是一种为工业应用开发的应用层协议, 被 DeviceNet、ControlNet、EtherNet / IP 等 3 种网络所采用, 因此这 3 种网络相应地统称为 CIP 网络。

2.2.6.4. Ethernet/IP

EtherNet / IP 采用和 DevieNet 以及 ControlNet 相同的应用层协 CIP(Control and Information Protocol), 因此, 它们使用相同的对象库和一致的行业规范, 具有较好的一致性。EtherNet / IP 采用标准的 EtherNet 和 TCP / IP 技术来传送 CIP 通信包, 这样, 通用且开放的应用层协议 CIP 加上已经被广泛使用的 EtherNet 和 TCP / IP 协议, 就构成 EtherNet / IP 协议的体系结构。

EtherNet / IP 在网络层和传输层采用标准的 TCP / IP 技术。对于面向控制的实时 I / O 数据, 采用 UDP / IP 协议来传送, 而对于显式信息(如组态、参数设置和诊断等)则采用 TCP / IP 来传送过程监控层流通的数据基本是显式信息, 采用 TCP / IP 来传送, 其优先级较低。而将来采用工业以太网 EtherNet / IP 协议的现场设备层, 流通的数据基本是实时 I / O 数据, 采用 UDP / IP 质议来传送, 其优先级较高。

2.2.6.5. EtherCat

EtherCAT (以太网控制自动化技术) 是一个开放架构, 以以太网为基础的现场总线系统, 其名称的 CAT 为控制自动化技术 (Control Automation Technology) 字首的缩写。EtherCAT 是确定性的工业以太网, 最早是由德国的 Beckhoff 公司研发。

自动化对通讯一般会要求较短的更新时间 (或称为周期时间)、同步时的通讯抖动量低, 而且硬件的成本要低, EtherCAT 开发的目的就是让以太网可以运用在自动化应用中。

3. 安装和运行

3.1. 需要环境

本软件基于.net 4.0 框架。

支持操作系统: Windows XPSP3 及以上系统, 32 和 64 位都可以运行。[\(Windows XP SP2 下的安装方法见 FAQ\)](#)

必要软件:

- ✓ XP 系统: 需要安装.net 4.0(有时候需要事先安装 WIC 软件, 才能安装.net4.0, 这些软件都在支撑软件目录中)。
- ✓ 其他系统, 请安装或启用.net 功能。

3.2. 安装过程

本软件为免安装软件, 放置在任何目录都可以直接使用。

主界面如下:

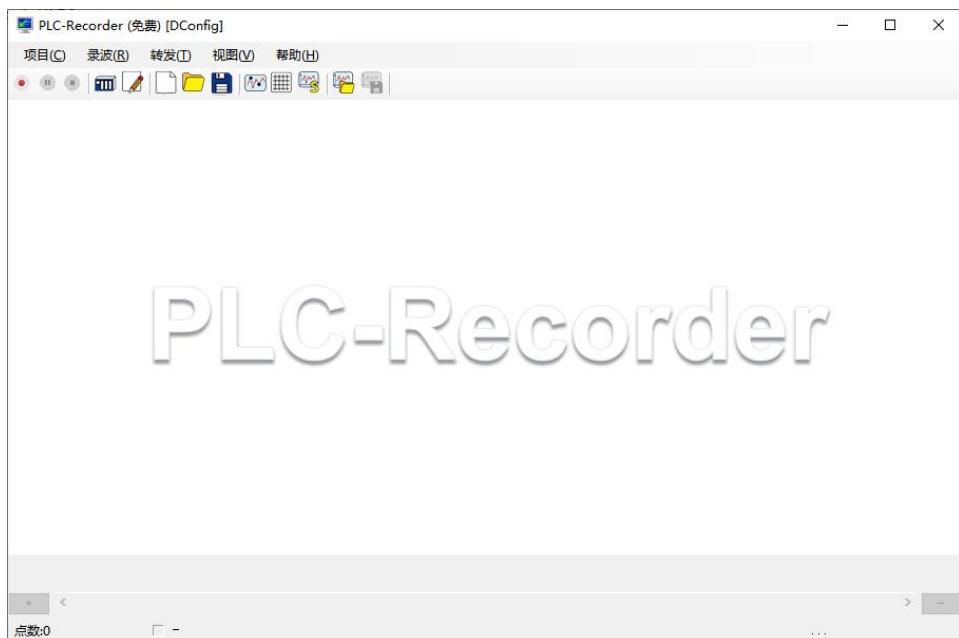


图 3.1 主界面

说明

本软件未申请过高的权限, 因此, 请将本软件放置在 WINDOWS 专用目录之外, 以确保能正常访问该目录。推荐: C:\PLC-Recorder\, 或者 D:\PLC-Recorder\

3.3. 目录文件说明

类别	文件名	作用
必须文件	Ana.exe	Ana 主程序
必须文件	Ana.exe.config	Ana 主程序
必须文件	Dongle_d.dll	USBKEY 必须文件 (丢失将导致程序无法启动)
必须文件	helpA.pdf	Ana 的帮助文件
必须文件	helpR.pdf	PLCRecorder 的帮助文件
必须文件	HslCommunication.dll	通讯组件
必须文件	HslCommunication.xml	通讯组件
必须文件	ihm.ico	图标
必须文件	libPLCRecorder.dll	公司专用库
必须文件	Newtonsoft.Json.dll	通讯组件
必须文件	Newtonsoft.Json.xml	通讯组件
必须文件	PLCRecorder.exe	PLCRecorder 主程序
必须文件	PLCRecorder.exe.config	PLCRecorder 主程序
必须文件	TwinCAT.Ads.dll	倍福通讯组件
必须文件	TwinCAT.Ads.xml	倍福通讯组件
必须文件	*.pem、*.Rsapub	USBKEY 必须文件
必须文件	*.ico、*.png	各种图标
必须文件	Rockey1S.dll	USBKEY 必须文件 (丢失将导致程序无法启动)
衍生文件	Authorize.txt	授权码文件 (授权方式之一)
衍生文件	Aconfig.apj	Ana 软件退出时的项目文件
衍生文件	configAna.ini	Ana 软件的操作习惯记录
衍生文件	configRec.ini	PLCRecorder 软件的操作习惯记录
衍生文件	DConfig.ipj	PLCRecorder 软件退出时的项目文件
衍生文件	exceptionLog.txt	致命缺陷记录
衍生文件	logs (目录)	日志文件目录
临时文件	*.dat	录波过程中的临时文件 (停止录波时, 这些文件会自动删除)

3.4. 软件升级方法

如果需要保留原来的配置和操作习惯, 可以将下载的压缩文件内容全部拷贝进原运行目录, 并进行替换。

如果需要全新开始, 将下载的压缩文件解压到一个新目录即可, 运行一次 PLCRecorder.exe 即可 (如果是 WIN10 系统, 请用管理员权限运行, 详见[如何建立数据文件的关联?](#))。

3.5. 授权

如果已经授权, 在 “关于” 页面里会显示出来并区分授权类别:

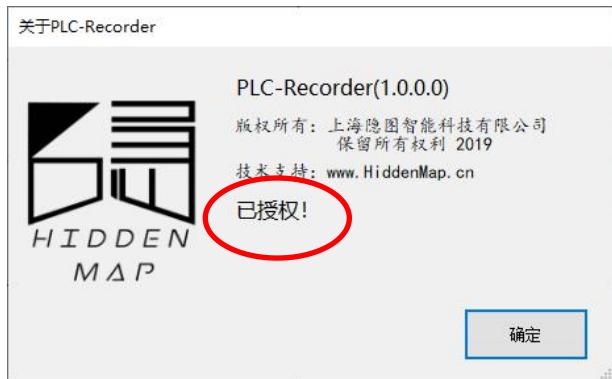


图 3.2 已授权示意图

如果没有授权，会显示申请码：



图 3.3 未授权示意图

本软件支持硬件和授权码两种授权方式。

3.5.1. 硬件授权

在工作时，电脑上插入授权 USBKEY（软件运行时不可拔下）即可。

USBKEY 在刚插入电脑时，指示灯将亮起。

不管先前状态如何，在软件运行过程中，指示灯将一直亮着，最后一个软件（如果同时打开了多个）关闭后，指示灯将熄灭。

硬件授权包括个人授权和商业授权两种，运行时，会在软件名称上区别显示。请勿将个人授权用于商业目的。

3.5.2. 授权码

正式用户请到官网 www.HiddenMap.cn 注册，登录，到订单管理栏目里，自主下载授权（提交申请码），文件名为 Authorize.txt 的文本文件（授权文件，需放入软件的运行目录），内容为授权码。

授权文件不可删除，每次启动时，以及启动后的关键时刻，都会检查。

申请码与电脑关键硬件的序列号相关，更改部分硬件后，可以重新申请授权。

授权码仅进行个人授权，运行时，会在软件名称上区别显示。请勿将个人授权用于商业目的。

原则上，虚拟机与主机是不同的系统，不保证能共享授权码。

禁止通过虚拟机拷贝等方法在多个系统上使用同一授权。

3.6. 如何建立数据文件的关联？

程序运行时，会自动修改注册表，将扩展名为“.ihm”的数据文件与离线分析软件Ana进行关联，从而可以双击打开。将扩展名为“.ipj”的项目文件与PLCRecorder.exe进行关联，可以双击打开。

如果拥有足够的权限，程序能够自动完成文件关联的注册。

对于部分无法完成自动注册的系统，手动处理步骤如下：

步骤1：打开本软件所在目录，找到本软件的可执行文件“PLCRecorder.exe”。

步骤2：在文件上点击鼠标右键，选择“以管理员身份运行”。

步骤3：正常启动一次后，就完成了注册。

说明

对于需要手动处理的系统，如果软件目录发生了变化，还需要再次进行手动关联，如果目录不发生变化，则不需要再次注册。

4. 配置

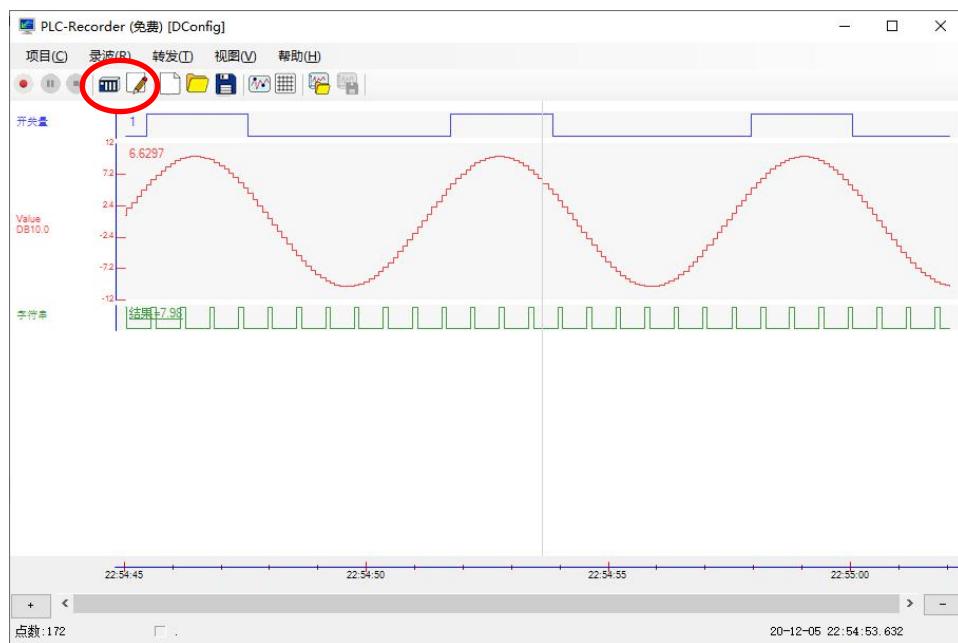


图 4.1 配置按钮的位置

4.1. 通道配置



图 4.2 通道配置示意图

4.1.1. 通道参数

按“添加”按钮可以添加通道。

选择某个通道条目，按“删除”将删除通道，及所有相关变量。

选择某个通道条目，按“配置”，进入配置画面，可以修改通道的信息。



图 4.3 通道参数修改示意图

- ✓ 通道类型：选择产品系列。
- ✓ 通道名称：为通道选择一个不重复的名称。

通道参数随设备不同而不同，上图给出了两个例子，无法确认的参数请保持默认值（能满足绝大多数需要，各设备的默认值可参考附录 1）。

西门子 S7 系列 PLC 采用的协议是一致的，但是框架、槽号、端口等因设备而不同，同一设备里，随着 CPU 的位置不同，也可能出现默认参数无法访问的事情，这时，请对照 PLC 的硬件配置进行设置。

其他设备大都区分协议，在使用时，请通过手册等资料确认目标设备所用（或激活）的协议和参数。

- ✓ IP 地址：目标设备的地址，请确保与本电脑在同一网段。
- ✓ 采集周期：

每次采集，都将对于所有的变量进行一次查询。每次采集耗时因通讯协议、设备运行速度、网络速度、网络繁忙程度、变量的多少而不同。

如果采集周期大于采集耗时，软件在采集完成后，将进行等待，以便实现等周期的采集。

如果采集周期设置过小，短于采集耗时，在采集完成后，将立即进行下一次采集。采集周期最小可以设置为 30ms。采集周期最大无限制，但是建议在 1 分钟以内（主要考虑人的感受）。

说明

由于被采集设备的内部扫描周期一般短于本软件的实际采集周期，因此，本软件可能无法捕获快速的信号变化。

- ✓ 激活：是否投入采集的选项。如果不激活，该通道的所有变量都将不投入下次采集。

4.1.2. 变量导出

选择一个或多个通道，点击“变量导出”按钮，就可以将这些通道的所有变量分别导出成.csv 格式的文件，并可以通过 EXCEL 等软件进行编辑，再次导入。

如果仅选择了一个通道，导出文件名就是对话框选择的文件名。如果选择了多个通道，在文件名后会增加通道名称，以示区别。

导出文件格式见[附录 2](#)。

4.1.3. 变量导入

选择通道，点击“变量导入”按钮，将进入变量导入的对话窗口，为该通道导入变量。



图 4.4 变量导入窗口

窗口左上角显示本通道的信息。

本软件格式导入用于导入符合[本软件格式](#)的变量列表，以.csv 为扩展名。

厂家格式用于从编程软件导出的符号表等信息。目前支持：

- 西门子 STEP7 软件 (S7-300、S7-400) 的符号表导出文件 (扩展名为.asc)、数据块导出文件 (扩展名为.AWL)，[参考步骤](#)。
- 西门子博图软件 (S7-300、S7-400、S7-1200、S7-1500) 的符号表导出文件 (请导出为.xls 格式文件，然后用 excel 等软件另存为.csv 格式)、数据块导出文件 (扩展名为.db)，[参考步骤](#)。

对于不支持导入的 PLC 型号，导入按钮将无效。

导入时，将进行各种检查，并配合多种导入选项，确保变量可用：

导入方式：

“全新” 将用导入变量替换掉本通道的所有现存变量。

“增量” 导入时如果发现与现有变量重名，将进行比较，如果发现有差异，则进行替代或者询问。

重名处理：

在增量导入时，如果发现有差异的重名变量，若选择“替代”，则直接替换。若选择“询问”，则会弹出窗口，列出两个变量的异同（不同的项次用红色标识），由用户自行选择。



图 4.5 变量比较窗口

错误处理：在导入的过程中，将进行多种检查，如果发现异常，则可以提醒或者直接忽略。

装载方式（本软件格式文件）：

“手动”：

如果是全新导入，则将所有的变量放入非装载列表，然后弹出装载窗口，由用户自行选择，装载。

如果是增量导入，对于未重名的部分，也将放入非装载列表，然后弹出装载窗口，由用户自行选择，装载。

“自动”：

如果是全新导入，则根据变量的装载状态，分别放入不同的列表。

如果是增量导入，重名部分由用户决定。非重名且标记为装载的变量放入已装载列表，变量立即投入使用。其他变量放入非装载列表。如果变量非常多，请谨慎使用“自动”功能，以免投入采集的变量过多而影响性能。

装载方式（厂家格式文件）：

“手动”：

如果是全新导入，则将所有的变量放入非装载列表，然后弹出装载窗口，由用户自行选择，装载。

如果是增量导入，对于未重名的部分，也将放入非装载列表，然后弹出装载窗口，由用户自行选择，装载。

“自动”：

如果是全新导入，变量全部放入已加载列表。

如果是增量导入，重名部分由用户决定。非重名变量放入已装载列表，变量立即投入使用。如果变量非常多，请谨慎使用“自动”功能，以免投入采集的变量过多而影响性能。

导入完成后，信息框内会显示导入结果。

变量装载窗口可以进行变量装载和卸载，并可以删除多余变量（不可恢复），可以通过输入变量名称中的部分字符来快速筛选变量。

变量装载: PLC1		
-	未装载变量列表	>
名称	起始地址	类型
int样例0[19]	M20	Int16
int样例0[18]	M18	Int16
int样例0[17]	M16	Int16
int样例0[16]	M14	Int16
int样例0[15]	M12	Int16
int样例0[14]	M10	Int16
int样例0[13]	M8	Int16
int样例0[12]	M6	Int16
<	已装载变量列表	-
名称	起始地址	类型
bool样例0	M0..0	Bool
int样例0	M2	Int16
int样例0[0]	M2	Int16
int样例0[1]	M4	Int16
int样例0[2]	M6	Int16
int样例0[3]	M8	Int16
int样例0[4]	M10	Int16
int样例0[5]	M12	Int16
int样例0[6]	M14	Int16
int样例0[7]	M16	Int16
int样例0[8]	M18	Int16
int样例0[9]	M20	Int16
int样例0[10]	M2	Int16
int样例0[11]	M4	Int16

筛选: 8/8 筛选: 14/14

图 4.6 变量装载和卸载窗口

4.1.4. 数据文件

- ✓ 文件保存路径: 历史数据文件的保存位置。
- ✓ 文件名含项目名称: 如果选择, 则历史数据的文件名将以项目名称开头。
- ✓ 日目录: 如果选择, 将按日组织数据文件。
- ✓ 文件保存间隔:

开始采集后, 多长时间保存一次数据文件 (每次都在不同的文件内)。为了减少数据丢失的风险, 该时间不要设置太长 (建议 30 分钟到 2 小时)。

每个通道、一次采集 (一次保存) 的总数据量 (总点数与 (变量个数+1) 的乘积) 是有限制的, 为 268435455 个。假设某通道有 100 个变量, 50ms 采集一次, 则单个文件采集的时间上限=268435455/101/20/3600/24=1.53 天 (36.9 小时), 降低采集频率或者减少变量数量都可以增加采集时间。如果不想降低采样频率及变量数量, 则可以通过减少文件保存间隔来解决, 比如, 改成 30 小时。

保存间隔的最小值不得小于采集周期的 2 倍。

4.1.5. 记录模式

点击记录模式的设置按钮，进入设置画面，提供多种启动和停止模式，这些模式可以组合使用：



图 4.7 记录模式设置

启动条件：

- ✓ 包括“手动”和“条件”两种模式。
- ✓ “手动”模式与以前的按钮启动功能一样，按钮后开始记录。
- ✓ “条件”模式，则根据设定条件进行判断。在这种模式下，会按照预采集时间进行提前采集。即：开始记录后，如果启动条件不满足，将循环记录触发前的数据（预采集）。在预采集的过程中，如果启动条件满足，则立即转入正式采集模式。满足条件的时刻也叫触发时刻，用蓝色虚线表示。

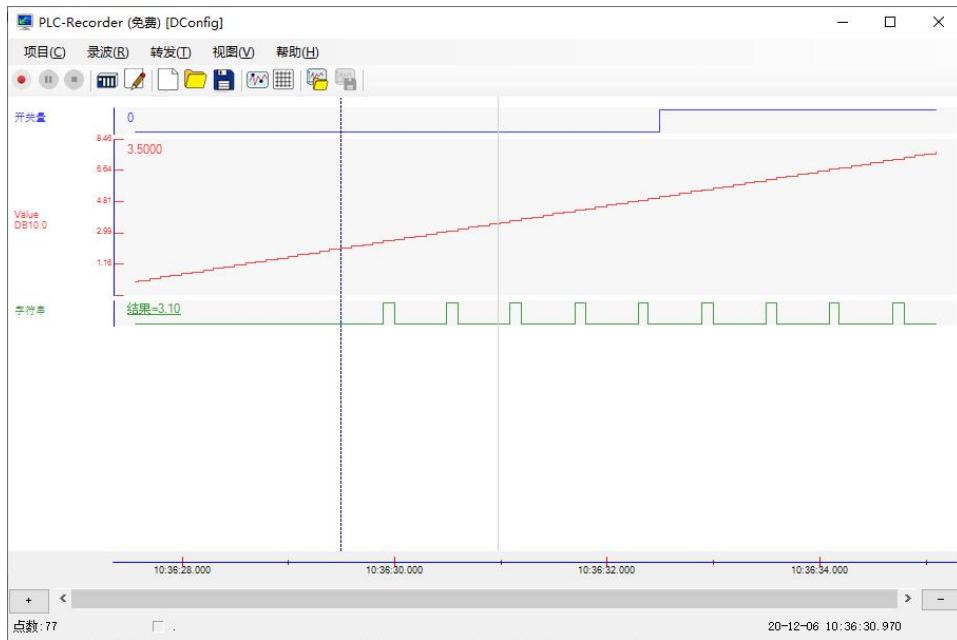


图 4.8 条件记录的波形示意

停止条件:

- ✓ 包括“手动”、“条件”、“延时”三种模式。
- ✓ “手动”模式与以前的按钮停止功能一样，按钮后停止记录。
- ✓ “条件”模式，开始正式采集后，根据设定条件进行判断，一旦条件满足，则终止采集。



图 4.9 停止条件设置

- ✓ “延时”模式，开始正式采集后，开始延时，延时到后，终止采集。

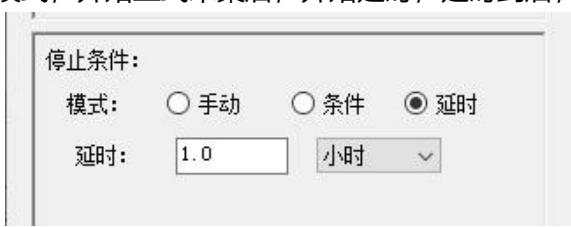


图 4.10 延时停止的设置

高级功能（需要授权）:

- ✓ “开机自启动”：将本软件加入开机自启动项，随系统启动。

- ✓ “自动开启录波”：本软件启动后，延时设定时间，然后启动录波。由于启动速度和网络准备的时间因系统和计算机性能而不同，因此，请测试并寻址适合自己计算机的参数，以免录波失败。
- ✓ “停止后自动关机”：当停止条件非手动时，一旦满足停止条件，则会发出延时关机指令（60s），并正常退出本软件。

以上 3 个选项结合，可以实现本软件随系统启动，并自动录波。并可以实现受控的关机功能，比如，UPS 供电的控制系统在发现主电源出现故障后，就可以给录波软件发出停机信号，由录波软件进行正常关机，避免计算机的损坏。

说明

测试发现 XP 系统对于以上功能，存在一定的不确定性，因此，请测试后再进行使用。

关机指令会强制关机，因此，在开启关机功能后，请退出不必要的软件，以免数据的意外丢失。

设置开机自启动，需要管理员权限，因此，需要修改设置时，请以管理员权限运行本软件。步骤如下：

- 1) 打开本软件所在目录，找到本软件的可执行文件“PLCRecorder.exe”。
- 2) 在文件上点击鼠标右键，选择“以管理员身份运行”。

- ✓ “循环录波”：如果启动模式设置为“条件”，停止模式非手动，则该功能可以实现循环录波的功能。

4.2. 变量配置

4.2.1. 简介

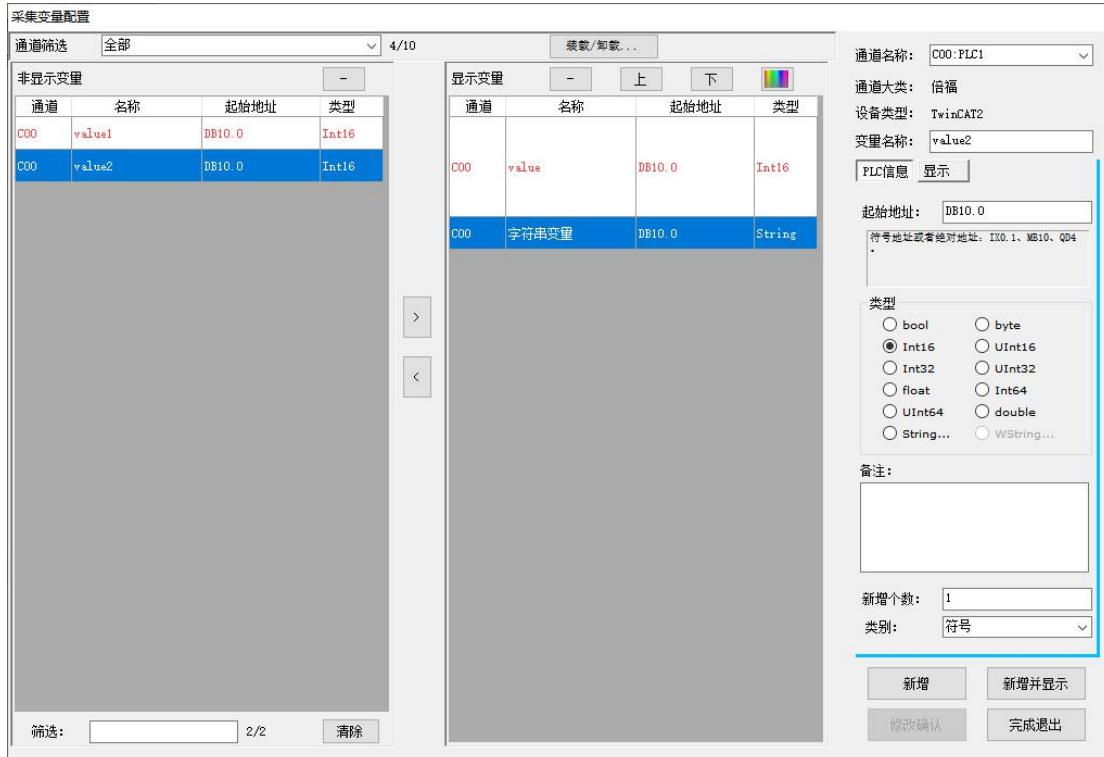


图 4.11 变量配置界面

顶部的通道筛选可以筛选某个通道，或者全部通道的变量，右侧为所选通道的已加载变量总数及非装载变量总数。指定某个通道，可以调出装载窗口。

变量分成显示和不显示两种，都进行采集和记录，因此，可以在后期进行是否显示的选择。

4.2.2. 非显示变量列表

- ✓ 显示和操作那些不进行显示的变量。
- ✓ 可以通过“Shift”、“Ctrl”配合鼠标进行多选。
- ✓ 可以将增删变量。
- ✓ 可以将变量转入显示列表。
- ✓ 可以进行排序操作。
- ✓ 可以通过输入变量名中的部分内容来快速筛选变量。

4.2.3. 显示变量列表

- ✓ 显示和操作那些需要进行显示的变量。

- ✓ 可以通过“Shift”、“Ctrl”配合鼠标进行多选。
- ✓ 可以将增删变量。
- ✓ 可以将变量转入非显示列表。
- ✓ 可以进行单个变量显示顺序的修改（通过上移和下移按钮）（多通道时，需要选择全部通道）。
- ✓ 可以修改显示的高度（通过拉变量行的下框线实现）。
- ✓ 不可以进行排序（因为这就是显示的顺序）。

说明

在数据量巨大时，如果需要显示的变量过多，则会影响响应速度，也可能导致内存不足，如遇这种情况，请减少显示变量的个数。

4.2.4. 变量操作

- ✓ 在左侧列表里响应右箭头、删除键；
- ✓ 在右侧列表里响应左箭头、删除键；
- ✓ 在变量名称区域内按回车，会进行重名检查，并跳转。
- ✓ 在起始地址区域内按回车，会进行语法检查。

通过“+”按钮进行变量的添加，添加步骤：

步骤 1：选择一个参考变量，然后在右侧的变量修改区域内进行变量名称、起始地址、变量个数等信息的修改。

步骤 2：按“+”按钮，实现变量的新增。

通过“-”按钮将变量转成非加载状态。

说明

新增变量时，高度将设定为该变量类型的默认高度，不再与样板变量一致。

4.2.5. 变量的可配置信息

- ✓ 通道：

选择变量隶属的通道编号。

- ✓ 起始地址：

起始地址是变量在 PLC 内部的地址，不同的 PLC 的表达方式可能完全不同。比如，西门子的 PLC，其起始地址为 M0.0、DB10.0 等绝对地址，而 AB PLC 则是变量在 PLC 内的符号名字。

地址的提示栏会显示本设备允许的部分地址格式，完整部分见（附录1 各品牌设备的地址规范）。回车、离开起始地址栏（或者切换变量的通道时），将马上进行语法检查，需要确定的部分将变成**红色字体**。

- ✓ 变量名称：该变量在本软件内的名称。在一个通道内部，名称不可重复。
- ✓ 类型：确定采集数据的长度和数据格式。
- ✓ 备注：
- ✓ 变换：变量的线性变换参数，公式为： $y=kx+b$ ，其中：k 为放大倍数，b 为偏移量。
- ✓ 显示：Y 轴的显示范围。如果最小值大于或相等最大值，将自动设置坐标轴，来显示完整的 Y 轴范围。小数位将控制曲线相关各数值的显示精度（即使是整数，经过变换后，也可能变成了带有小数点的数字，因此，除开关量以外的所有变量，小数位的设定都是有效的）。点击自动按钮将会把 Y 轴的最大值和最小值都设置成 0，如果是浮点或者双精度，则小数位设置成 2，其他设置成 0。
- ✓ 颜色：曲线的颜色，点击“显示”表单里的色块，可以调出设置对话框。点击  按钮，将自动设置所有显示变量的颜色。

在打开配置文件或者历史文件时，将读取变量配置，并进行简单的变量类型检查，如果发现不一致，将会提醒。这时候请进入变量配置画面，检查修改变量类型。修改方法：

- 步骤 1：选择变量；
- 步骤 2：点击变量起始地址；
- 步骤 3：点击变量的其他可编辑部分，比如变量名称，将会进行一次变量自动匹配；
- 步骤 4：保存。

4.2.6. 批量添加变量

如果在“新增个数”内填写大于 1 的值，将根据当前PLC类型、变量类型，自动确定后续的合理起始地址，添加指定个数的变量。变量名称也将自动添加序号，如果遇到重复的，将自动跳过。

4.3. 字符串变量

每种 PLC 的字符串变量结构和编码不尽相同。比如，西门子的各型 PLC 都提供了字符串的类型（String），其中 S7-1200 和 S7-1500 还提供了扩展字符串变量（WString），变量头部都有长度信息。而日系 PLC 字符串无长度信息，但是有结尾标志。

本软件提供了字符串变量的配置界面：



依据设备类型和变量类型，长度的单位为字节或者字，请注意区分。

结构 1 用于指明截取字符串变量内部，不包括头尾信息，但是，对于日系 PLC，还是会在结果解析时查看结尾标志，并截取结尾前的部分，如果没有发现结尾标志，则截取全部长度的内容。

结构 2 用于西门子的字符串类型，结果解析时，会查看字符串自身反馈的长度信息和设定的长度信息，取其中较小者。对于该结构，建议长度设定稍微大于字符串的长度，由软件自动解析长度，确保获得完整字符串。

结构 3 用于日系 PLC 的字符串类型，会根据结尾标志确定实际的长度，并截取结尾前的部分，如果没有发现结尾标志，则截取全部长度的内容。对于该结构，建议长度设定稍微大于字符串的长度，由软件自动解析长度，确保获得完整字符串。

说明

相对于数值型变量，字符串变量的信息较长，对于采集速度影响较大，因此，请谨慎使用，并尽可能缩短变量长度，减少无用的内容读取。

允许的字符串结构将依据设备类型自动选择。

4.4. 配置的保存和打开

可以通过“项目文件”菜单来保存和打开配置文件 (.ipj 文件)。

也可以通过导入功能从现有的数据文件里导入配置信息。

软件启动后，将打开退出时的配置内容。

5. 采集

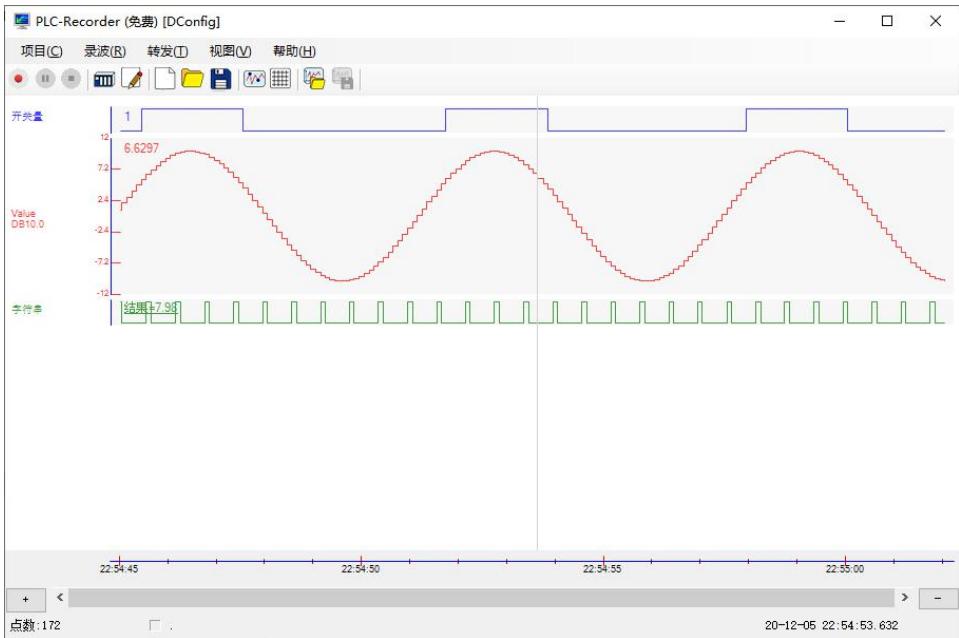


图 5.1 采集主界面

5.1. 采集过程

点击 (启动) 后，开始数据的采集。

首先进行通讯的连接：如果激活的通道无法建立连接，将提醒是否要禁用该通道。

在所有启用的通道成功建立连接后，将进行变量的可访问性测试，如果发现异常，将进行提醒。如果没有异常，则开始连续采集。

如果在设定的周期内没有完成采集，将继续使用下一个周期时间（该周期内不再启动下一次采集）。因此，如果发现这种现象，最好延长采集周期，以便得到等周期的数据。如果将时间设置的足够短，则会实现连续采集的目的。

按钮上的数字表示已经完成的采集次数（多通道采集时，该数字为各通道采集次数的最大值）。

采集时，将滚动显示最新的采集数据。

点击 (暂停) 按钮，曲线填充窗口后，将不再滚动（不影响记录）。

按 (停止) 按钮后，将停止采集。

在采集过程中，点击底部的“+”、“-”按钮，可以扩大或者缩小显示的时间范围（改变窗口滚动的速度）。

“+”按钮上方的文字随采集状态而变化，在正常采集时，会显示累计采集的时间。

为减少采集时的资源占用，在采集过程中，仅显示窗口范围内的数据，数据一旦滚动出窗口，将不再被实时显示（不影响数据的保存和历史显示）。

5.2. 软件界面的操作

5.2.1. 最小化和退出

点击右上角的关闭按钮，软件将缩小为右下角的图标。可以通过图标双击或者菜单操作来恢复界面或者退出。

通过菜单“项目->退出”，也可以实现彻底退出。

5.2.2. 录波窗口置顶

通过菜单“视图->录波时置顶”，可以让录波窗口停留在大部分软件的前面，确保波形观察。

5.3. 字符串采集

字符串变量在波形上以 BOOL 的格式进行展示，当字符串内容发生变化时，BOOL 值变成高电平，并保持一个采集周期。

波形的标签处显示当前的字符串内容。

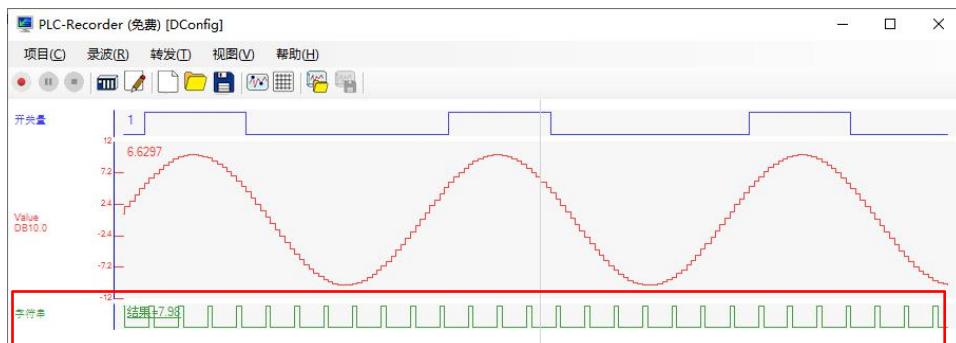


图 5.2 字符串的波形示例

5.4. 数据保存

达到设定条件后，数据将被保存在指定目录的历史文件中，文件名称为本文件开始采集的时刻，比如：20190410215828.ihm。

再次点击采集按钮，将停止采集，最后采集的数据也将存入历史文件中，并进行显示。

数据文件名称可以包含项目名称，请在通道配置里进行功能勾选。

在采集的过程中，点击“保存当前数据”按钮 ，则会将还未来的数据进行一次保存，并继续采集。

5.5. 通讯状态监控

在采集的过程中，左下角将显示连接状态，未连接时为灰色，正常连接为绿色，任何一个通道连接不佳时为黄色，任何一个通道长时间无反应时为红色。在采集时，通讯会自动检测和恢复。

5.6. 仿真

本软件提供录波仿真功能，可以模拟 SIN 曲线或者斜线。开启 SIN 模拟时，数据将来自于内部的正弦波信号发生器。

该功能通过菜单进行开关：录波->仿真-正弦或者仿真-斜线来进行操作。对外部设备录波时，请不要选择任何一个。

6. 数据转发

6.1. 功能说明

软件的转发功能，可在录波的同时，将当前数据转发给第三方的软件。

本软件可以开启一个 WebSocket 服务器，可以为 WebSocket 客户端（C 端或者 B 端）提供数据服务。

客户端连接服务器后，需要进行身份验证（通过输入正确的服务器识别号），变量订阅。身份验证和变量订阅成功后，将发送全部变量的当前值（仅发送一次）。随后，服务器将按照设定的周期检查数据的变化，将变化的变量数据发生给客户端。交互过程请参考[附录 3](#)。

主要参数：

- ✓ 同时服务的客户端数量：最大 4 个。
- ✓ 每个客户端订阅的变量数量：建议不超过 1000 个。
- ✓ 最小更新周期：100ms。
- ✓ 信息格式：JSON 字符串（详见[附录 4](#)）。
- ✓ 协议版本：V1.0.1

6.2. 启用和停止方法

通过菜单“转发”->“配置...”，打开配置窗口设置端口号和服务器识别码，点击“应用退出”。

如果勾选“原始值”，则转发采集到的值。如果不勾选，则转发经过 $y=kx+b$ 变换后的值。

如果勾选“本地不保存”，则在转发时，数据不进行本地存储。



图 6.1 转发配置窗口及默认参数

然后通过“启动服务器”和“停止服务器”来切换服务器的状态。启动后，软件标

题中将出现 “[转发中]” 的字符。

6.3. 客户端开发

请参考客户端 DEMO 源码，下载地址：www.HiddenMap.cn

7. 显示和分析

7.1. 数据显示

可以通过“打开数据文件”按钮来调用离线分析软件 Ana 来打开最近一个历史数据文件进行曲线显示和后续的分析。

也可以双击数据文件利用离线分析软件 Ana 来进行分析。

7.2. 显示区域和功能选项

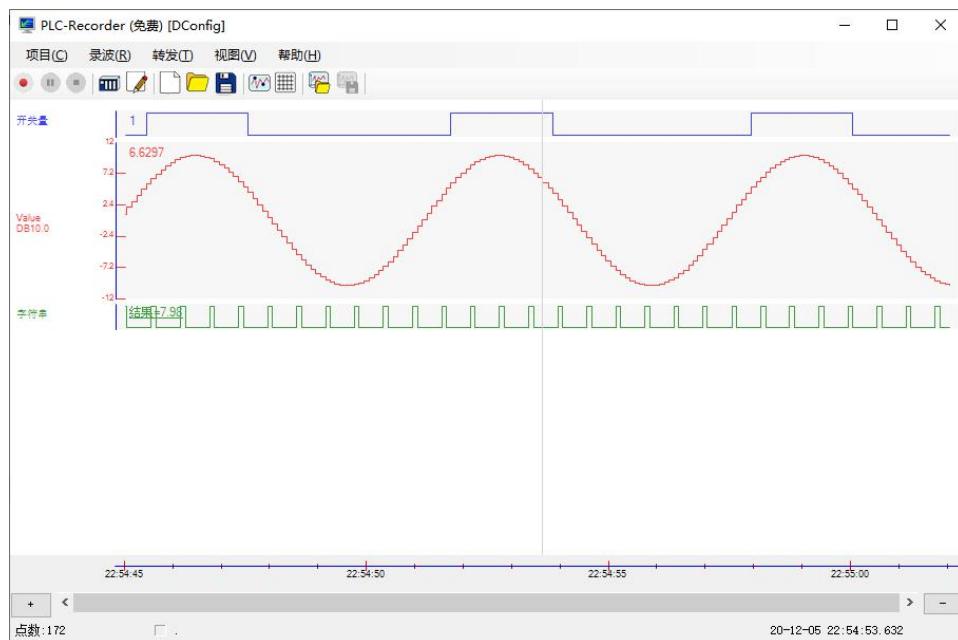


图 7.1 历史数据显示主界面

点击可以显示或者取消显示数据点标志，你如果需要精确查看采集时刻，该功能是必要的。

显示和分析

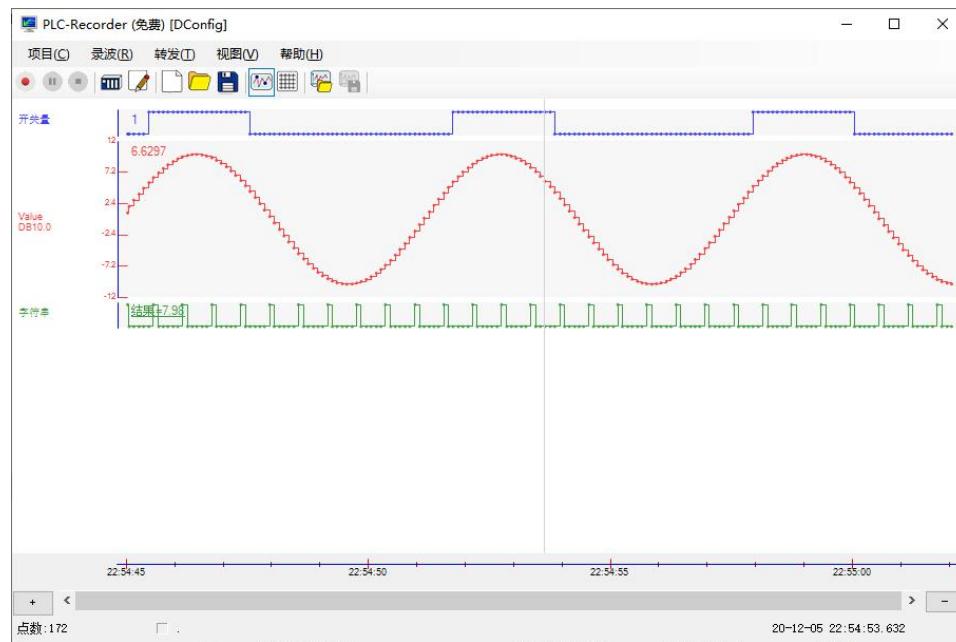


图 7.2 显示数据点的示意图

点击 ，将显示网格线。

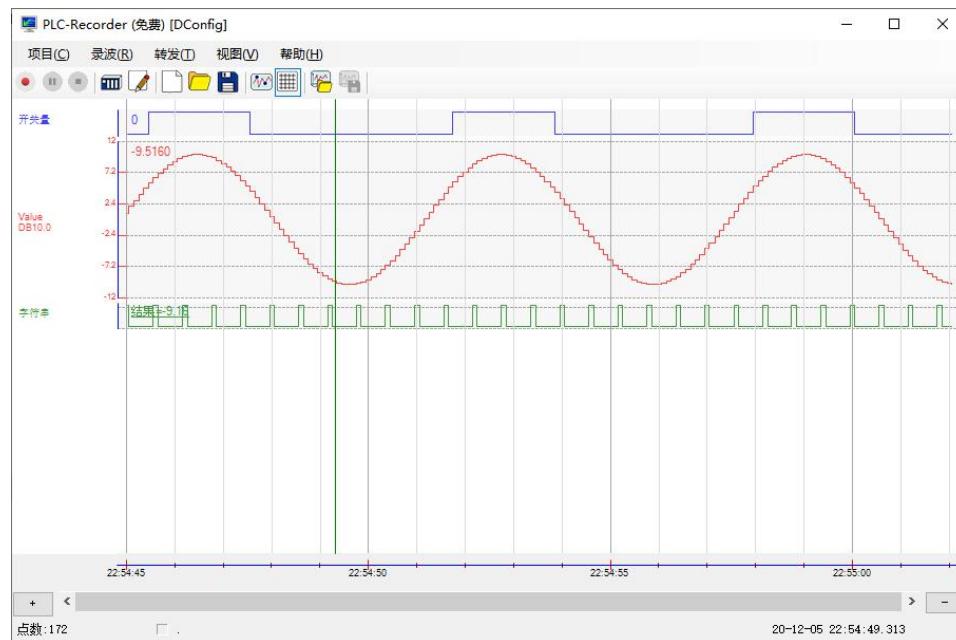


图 7.3 显示网格的示意图

通过菜单 “视图-开关量实心” 可以实现开关量的实心显示 (bar 图)：

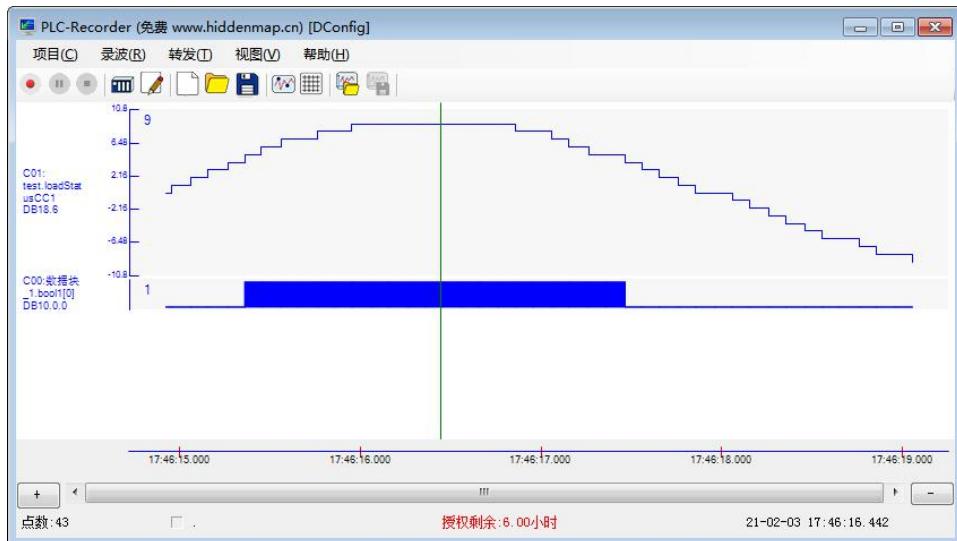


图 7.4 开关量实心显示的效果

在曲线上点击鼠标，将显示光标，然后在显示区域的右侧显示该点左侧的数值。窗口右下角显示光标所在的时间。

右下角为光标处的详细时间。

底部滚动条用户曲线显示窗口的移动，“+”按钮用于放大窗口，“-”按用于缩小窗口（窗口最小 100ms）。可以通过滚动条来移动曲线窗口，也可以通过点击曲线外左右侧的区域来实现移动。

7.3. 曲线高度的拖拽

对于实时曲线或者停止录波后的曲线，都可以通过拖拽曲线底部（红框的黄色区域）来调整曲线的高度，拖拽部位如下：

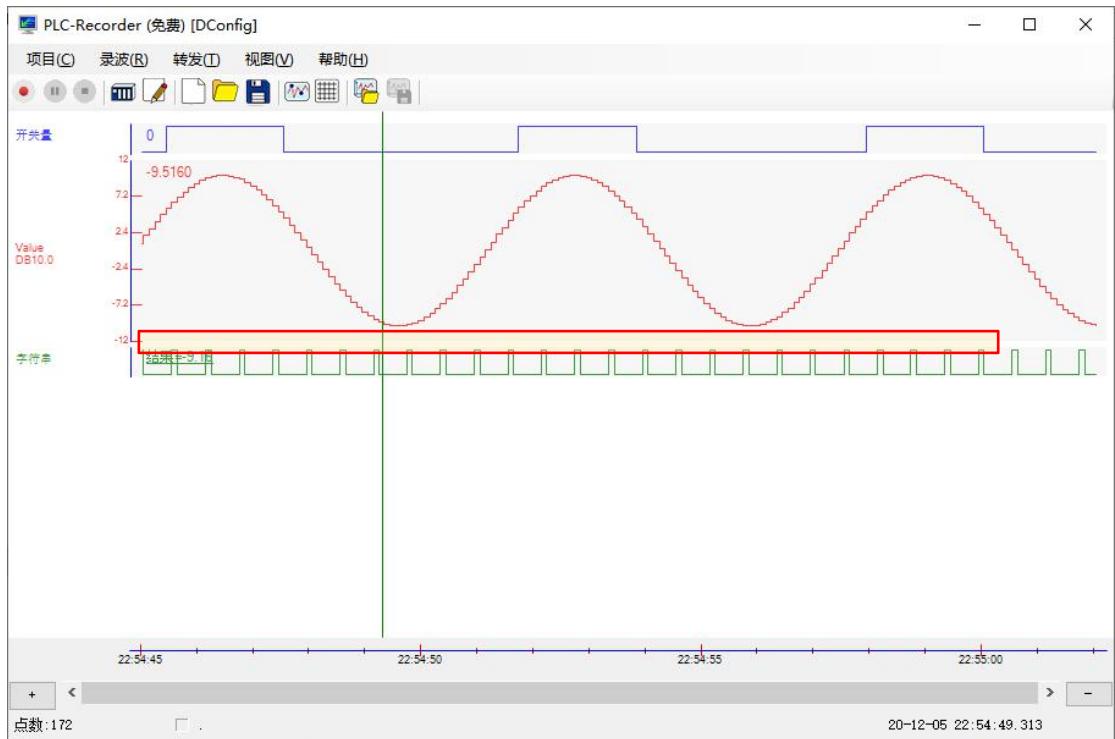


图 7.5 曲线高度拖拽示意图

布尔型变量曲线（包括字符串的曲线）的高度固定，不可被拖拽。

拖拽后，会提示保存配置文件。

7.4. 显示格式

变量显示格式包括曲线是否显示的选择，如果显示，则[颜色](#)、[比例尺](#)、[高度](#)、[Y轴范围](#)等信息可以通过变量配置界面进行调整。

曲线的高度和字体可以通过显示菜单里的条目进行调整。

显示格式可以保存在项目文件中或者打开的数据文件中。

7.5. Y 轴局部自适应功能

在“视图”->“Y 轴选择全局极值”，选择后，Y 轴的最大最小值将根据全部数据进行评估。不选择时，Y 轴的最大最小值将根据当前窗口范围内的数据进行评估。

该功能同样适用于录波过程中的窗口调整。

8. 文件管理

如果磁盘的格式为 FAT32，在标准文件名的情况下，目录最多能容纳 21884 个文件（如果每小时产生一个文件，则可存储 910 天的录波数据）。如果文件名称带有项目信息，则文件名会变长，则目录能容纳的文件数量将急剧减少。

如果磁盘的格式为 NTFS，则可以容纳 4294967295 个文件，因此，可不必在意。

软件不自动清理磁盘，如果文件目录内文件数量超过了容量限制，或者磁盘容量不足，都可能导致写入失败，因此，请及时清理数据记录目录里的文件。

注意及时清理日志目录里的文件（位于本软件运行目录的 logs 子目录）。

9. 快捷键

快捷键	功能
Alt+F4	程序退出
Ctrl+1	启动录波
Ctrl+2	暂停滚动
Ctrl+3	停止录波
Ctrl+4	通道设置
Ctrl+5	变量设置
Ctrl+8	X 窗口放大
Ctrl+9	X 窗口缩小
Ctrl+K	图片拷贝
Ctrl+L	长图拷贝
Ctrl+N	项目文件：新建
Ctrl+O	项目文件：打开
Ctrl+S	项目文件：保存
F1	打开帮助文件
Ctrl+F12	项目文件：另存

10. 常见问题 (FAQ)

10.1. 连接问题

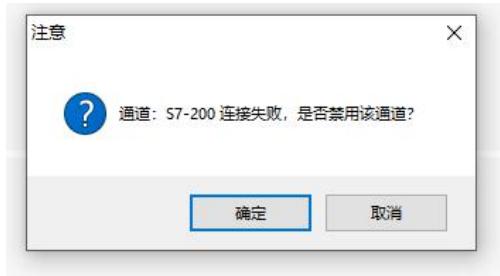
10.1.1. 如何确认 PLC 是否可以访问？

大部分情况下，可使用 PING 命令来确认，只要能 PING 通，就可能建立通讯连接。在某些情况下，虽然无法 PING 通，照样可以建立通讯。

10.1.2. 如何判断连接是否成功？

连接时首先与设备建立通讯，然后进行变量校验，都成功后，开始进行数据采集。

如果连接没有建立，等待一段时间后就会报出连接错误：



如果选择“确认”，这个通道就会被禁用，以后不再进行连接，如果需要再次打开，可以到通道配置里进行设置。

如果连接成功，将不进行提示，直接进行变量校验，任何一个变量发生读取错误时，都会报出来，这时候就需要进行变量修改。变量读取错误的常见问题：1、变量地址错误（不存在，或者超范围）；2、变量类型错误。有些设备、有些变量是无法校验的，比如 AB 的某个变量可以用位读取，也可以用整型读取，PLC 都会返回值，这时候就需要用户自行区分了。如果为了校验通讯，则可以只建一个最可能没有问题的变量进行测试，对于西门子，可以选择：M0.0 这个一直存在的变量。

完全正确地建立连接后，有 3 处明显特征：1 处的数字在变化；2 处的波形在走动；3 处的时间在增加。



10.1.3. 连接失败怎么办?

如果配置正确，绝大部分情况下，软件会与 PLC 设备顺利建立连接。但是，有时候会出现第一次无法连接的情况，尤其是一些老型号的设备，或者系统、网络繁忙的时候，出现的概率会较高，这时候请尝试再连接。

10.2. 系统

10.2.1. 录波时，软件的 CPU 负荷占用过大，甚至卡顿

减少录波时软件 CPU 负荷的措施：

- 1) 开始录波时，将窗口最小化，最好是直接关闭(右下角有图标，可以随时恢复)。
- 2) 减少录波时在线显示的变量数量。
- 3) 减少显示窗口的时间跨度(通过右下角的“-”按钮)。
- 4) 以管理员身份运行。

说明

卡顿是显示处理不及时导致的，不影响数据采集。

10.2.2. 如何使软件永久获得管理员权限？

在部分系统中，数据文件关联、开机项的修改，可能都需要管理员权限。本软件未自动申请管理员权限，因此，用户如希望长期以管理员身份运行，则可以按如下步骤设置：

步骤 1：打开本软件所在目录，找到本软件的可执行文件“PLCRecorder.exe”。

步骤 2：在文件上点击鼠标右键，选择“属性”->“兼容性”->勾选“以管理员身份运行此程序”。

步骤 3：确认。

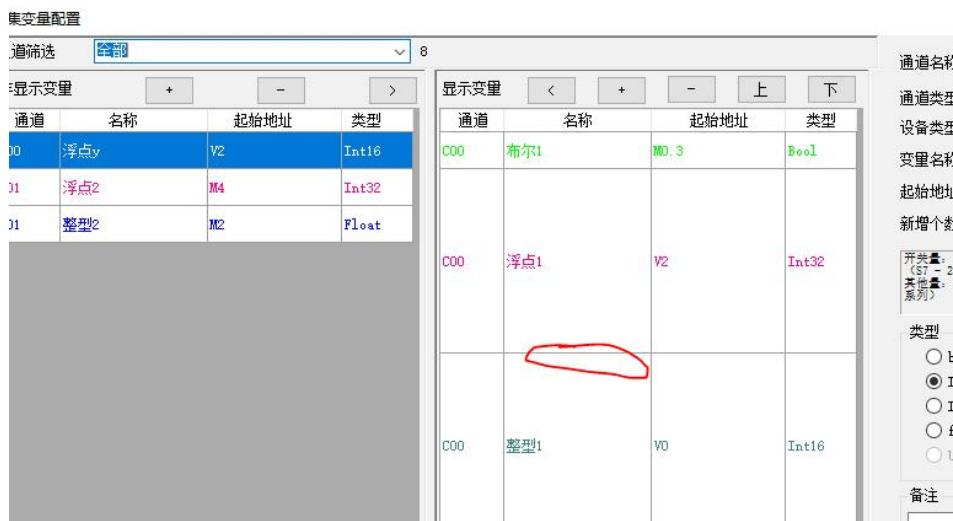
10.2.3. Windows XP SP2 下的安装方法

- 1) 安装 KB893803-v2-x86
- 2) 安装 dotnetfx35
- 3) 安装 dotNetFx40_Client_x86_x64
- 4) 安装 .NET Framework 4.0
- 5) 解压本软件。

10.3. 图形操作

10.3.1. 如何修改变量在波形上的高度？

在变量配置页面的显示变量列表里拖拉变量底部的边线，或者在主界面进行曲线高度的拖拽。



10.3.2. 如何测量信号的长度？

请用离线分析软件 Ana 来进行处理。

10.3.3. 如何将数据导入 excel？

请用离线分析软件 Ana 来进行处理。

10.3.4. 如何合并多个波形文件？

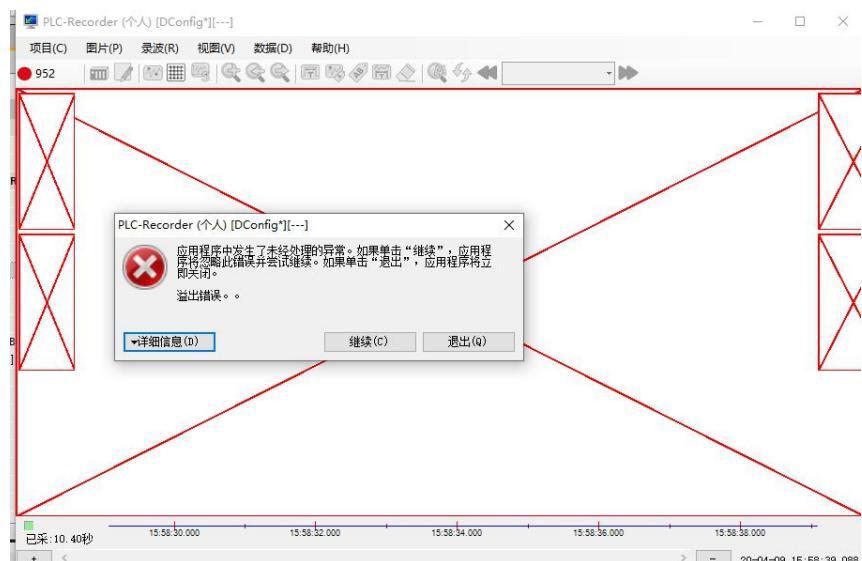
请用离线分析软件 Ana 来进行操作。

10.4. 窗口显示大红叉，怎么办？

如下图的显示崩溃，软件已经在极力避免了，但是还无法杜绝，一般出现的原因是数据类型错误，录波时无法检查出来，会采集回来非常极端的值，导致显示控件无法处理而崩溃。

比如：我们用 DB1.0 采集变量时，PLC 里是 DINT，则是 32 位变量，如果录波软件里用 DOUBLE 去采集，则会把后面 32 位一起采集回来而可能出错（不是必然出错）。

所以，如果遇到这种情况：**请首先仔细核对数据类型。**



11. 软件版本更新说明

版本	更新内容
V1.8.2	2021-2-3 <ul style="list-style-type: none">● 增加西门子 STEP7、博图项目数据块内变量导入功能。● 开关量可实心显示 (bar 图)。● 转发优化：增加了仅转发，不本地存储的功能。● 基恩士变量访问格式优化，大部分变量可以按照 PLC 内的格式进行访问。● 松下驱动优化。● 欧姆龙 CIP 访问优化。● 变量配置窗口优化：数据类型上动态提示 PLC 内的对应类型。● 修正其他已经发现的错误。
V1.8.1	2021-1-16 <ul style="list-style-type: none">● 增加录波时，窗口置顶的选项。● 变量窗口优化。● 修正临时文件的一些错误。
V1.8.0	2021-1-1 <ul style="list-style-type: none">● 授权机制变化，详见产品购买页面；● 通道计数以激活的为准；● 点位搜索优化；● 变量检查优化，不允许地址为空的变量。
V1.7.4	2020-12-11 <ul style="list-style-type: none">● 修正导入的错误。
V1.7.3	2020-12-5 <ul style="list-style-type: none">● 触发记录错误修正；● 系统优化：通道逻辑优化；● 增加异常终止后，暂存数据的自动恢复功能；● 界面优化：数值放置在标签区域，按照设定位数进行显示，取消曲线右侧的数值区域。
V1.7.2	2020-11-15 <ul style="list-style-type: none">● 支持台达、汇川 PLC 的 Modbus TCP 访问；● 罗克韦尔 (AB) 驱动优化：增加变量类型在线检查、允许硬件内容和局部变量访问；● 曲线高度调整：除了在变量界面，还可以在主界面拖拽曲线底部来实现；● 变量界面优化：地址错误提示方式优化、● 系统优化：减少多曲线时卡顿的程度、修正无激活通道时可能出现的错误；● 界面优化：增加各界面的“取消”功能、开关量高度自动修正等。

版本	更新内容
V1.7.1	<p>2020-10-29</p> <ul style="list-style-type: none"> ● 倍福驱动优化：提高了稳定性、速度及容错能力，支持字符串变量。 ● 标准 Modbus TCP 提供数据格式选择，增加适应能力。 ● 支持蓝普峰 PLC。 ● 变量管理优化：增加自动配色功能，完善变量管理功能。
V1.7.0	<p>2020-10-6</p> <ul style="list-style-type: none"> ● 支持字符串变量的录波（支持西门子、三菱、欧姆龙、基恩士、松下，及其他支持三菱协议的 PLC。变量配置页面适应性优化）； ● 支持三菱 FxSerialTcp 协议（国产 AMSAMOTION 艾莫迅 PLC）； ● 转发功能优化：增加是否转发原始值的选择； ● 松下地址表达方式优化； ● 历史数据文件打开优化； ● 增加暂停波形滚动的功能； ● 变量重名检查、地址重复检查优化、变量导入优化； ● 主界面优化：用户选择是否显示开关量的地址信息；字体优化；启停按钮优化等。
V1.6.2	<p>2020-7-15</p> <ul style="list-style-type: none"> ● 自动纠正文件关联错误； ● 增加历史文件列表； ● 西门子支持 64 位整型变量（针对 S7-1500）； ● 变量界面优化，减少混淆； ● 其他已知 bug 的修正。
V1.6.1	<ul style="list-style-type: none"> ● 修正 byte 变量存储的 bug； ● 录波界面优化：bool 型变量不显示地址；只有一个通道时，不显示通道编号。
V1.6.0	<ul style="list-style-type: none"> ● 支持转发功能； ● 增加 AB micro800 的支持； ● AB 默认值修改。
V1.5.0	<ul style="list-style-type: none"> ● 与离线分析软件分离； ● 欧姆龙默认端口修改为 9600； ● 支持轻度定制功能； ● 软件可以缩小为右下角图标，更少打扰。

版本	更新内容
V1.4.0	<ul style="list-style-type: none"> ● 内部变量存储结构改变，减少大数据量时的内存占用，提高处理大数据量的能力； ● 解决修改批注后，窗口自动滚动的问题； ● 图片拷贝的快捷键从 Ctrl-C 调整为 Ctrl-K； ● 数据文件组织方式添加每日一个文件夹的选项，实现按日组织文件； ● 变量添加时，高度为默认值； ● 西门子读取优化，减少读取时间； ● 西门子 S7-1200 通道的默认参数修改； ● 非显示变量列表和加载列表可以通过输入部分字符来进行快速筛选； ● 修复录波停止、软件关闭时，文件记录的错误； ● 修正欧姆龙结果解析的错误； ● 修正负荷占用大时，采集时间更新慢的错误； ● 修正 Y 轴局部极值的小错误； ● 各 PLC 变量检查出错时，同时显示底层错误信息，方便查找原因。
V1.3.3	<ul style="list-style-type: none"> ● 纠正西门子变量地址自动修正时的错误； ● 纠正非装载变量保存时的错误； ● 纠正历史数据导出时的错误； ● 升级驱动库：三菱支持变量类型增加、欧姆龙开关量访问的修正（欧姆龙的请谨慎使用）。
V1.3.2	<ul style="list-style-type: none"> ● 变量导入时，进行语法检查和地址转化； ● 增加处理大数据量的能力，可以操作约 1G 的数据量（非压缩后的文件大小），可用内存不足时，进行提示； ● 根据变量个数进行文件保存周期的自动优化，尽量避免单文件的巨量数据； ● 解决波形显示小 bug，波形算法优化，波形显示和操作更安全； ● 进行变量地址重复的检查、变量配置逻辑优化； ● 允许不同通道的变量重名。
V1.3.1	<ul style="list-style-type: none"> ● 变量导出优化
V1.3.0	<ul style="list-style-type: none"> ● 增加开机自启动、自动录波开启、自动关机、循环录波的功能。 ● 增加变量的导入和导出功能。 ● 增加变量装载和卸载的功能。 ● 界面优化、采集内核优化。

版本	更新内容
V1.2.0	<ul style="list-style-type: none"> ● <u>多文件操作</u>; ● <u>增加多种记录模式</u>; ● <u>采集内核优化</u>; ● 西门子 S7-1500 默认槽号修改为 1; ● <u>仿真增加斜线功能</u>; ● <u>搜索增加边沿检测功能</u>; ● 文件格式修改，全面采用压缩模式; ● <u>采集计时模式修改</u>; ● 授权机制调整：离线功能全部免费; ● <u>界面优化</u>。
V1.1.4	<ul style="list-style-type: none"> ● 支持倍福 PLC 设备; ● 优化通道管理、变量管理的逻辑; ● 解决时钟倒拨时的问题; ● 通道提醒的优化; ● 增加 <u>Y 轴局部自适应的功能</u>; ● 数据文件自动保存时，重名不再覆盖; ● 授权细分为个人版和商业版。
V1.1.3	<ul style="list-style-type: none"> ● 修正通道管理、变量管理中的一些错误; ● 通道管理画面里显示通道的变量数量。
V1.1.2	<ul style="list-style-type: none"> ● 修正初始化通道中参数的错误; ● 变量管理和检查优化。
V1.1.1	<ul style="list-style-type: none"> ● 添加 S7-200 的设备类型 ● 文件保存、变量管理的优化
V1.1.0	<ul style="list-style-type: none"> ● 松下、基恩士 PLC 支持 (MC 协议) ● 增加硬件授权功能 ● 快速浏览优化、采集优化、界面优化
V1.0.1	<ul style="list-style-type: none"> ● 波形显示内容优化
V1.0.0	基础版本

附录 1 各品牌设备的地址规范

1. AMSAMOTION 艾莫迅

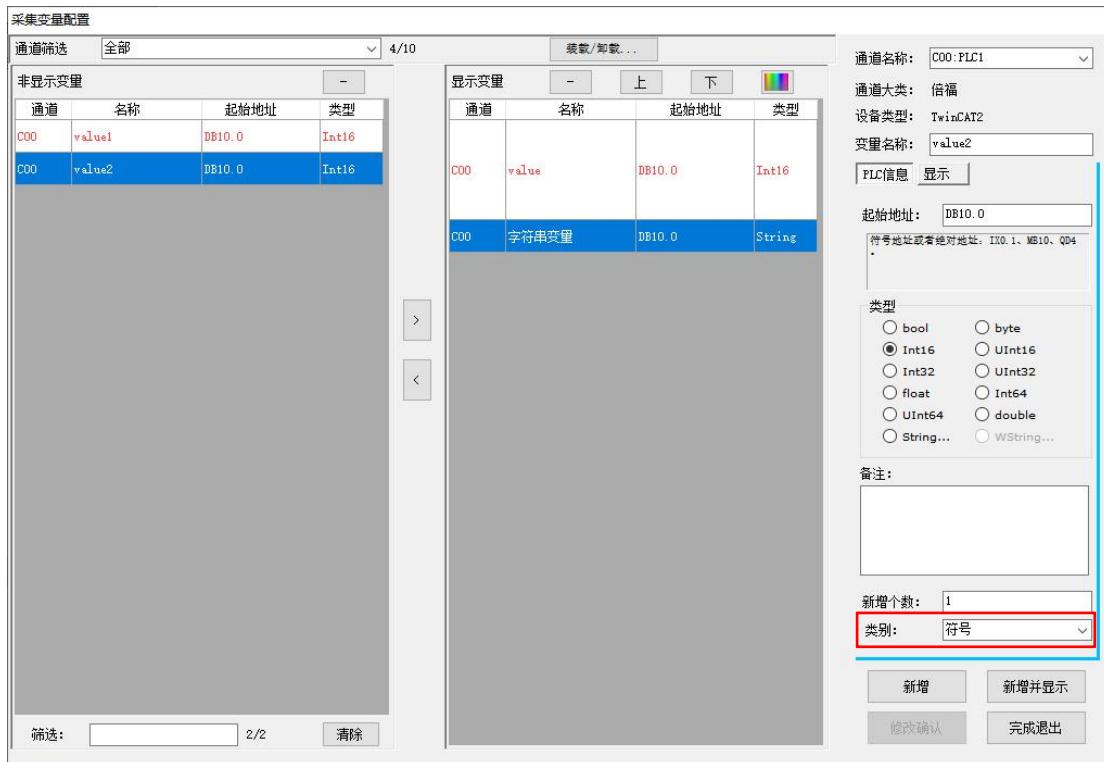
协议和地址格式，请参考三菱 FxSerialTcp 协议。该协议无需设置，默认开启，但不可与编程软件等同时在线。

默认通道参数：



2. Beckhoff 倍福

支持 TwinCAT2 和 TwinCAT3。支持 2 种地址类型，选择位置：



2.1. 符号地址:

本软件最推荐的地址方式，格式：对于全局变量 “.ABC”，对于局部变量：“程序名.ABC”，比如，main.a1。

对于数组的访问，例如：mainarry[1]。

对于结构（用户定义类型），例如：main.ut1.ab。

- ✓ 不区分大小写。
- ✓ 不带引号。

2.2. 绝对地址:

格式样例：IX0.1、MX10.1、QX0.2、IB10、MB10、QB10、IW12、MW12、QW12、ID4、MD4、QD4。

2.3. 默认通道参数



TwinCAT2 的 4 个 PLC 端口分别为：801、811、821、831

TwinCAT3 的 4 个 PLC 端口分别为：851、852、853、854

如果本软件安装在本地（与 PLC 在同一个系统内），则 Target NetId 可以设置为空。

如果不在此本地，则需要正确设置，相关信息参考“[倍福通讯设置示意](#)”章节。。

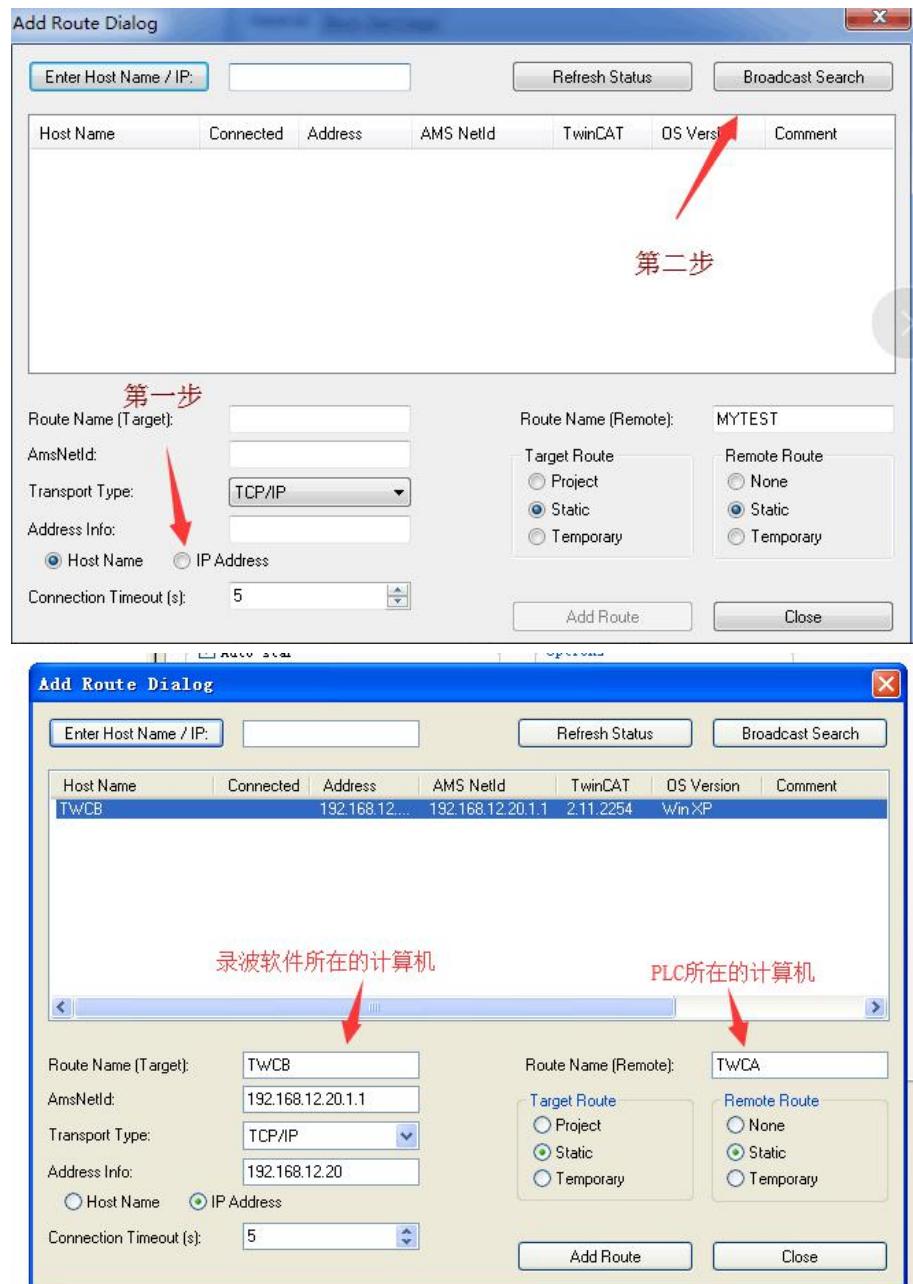
其他请参考倍福手册。

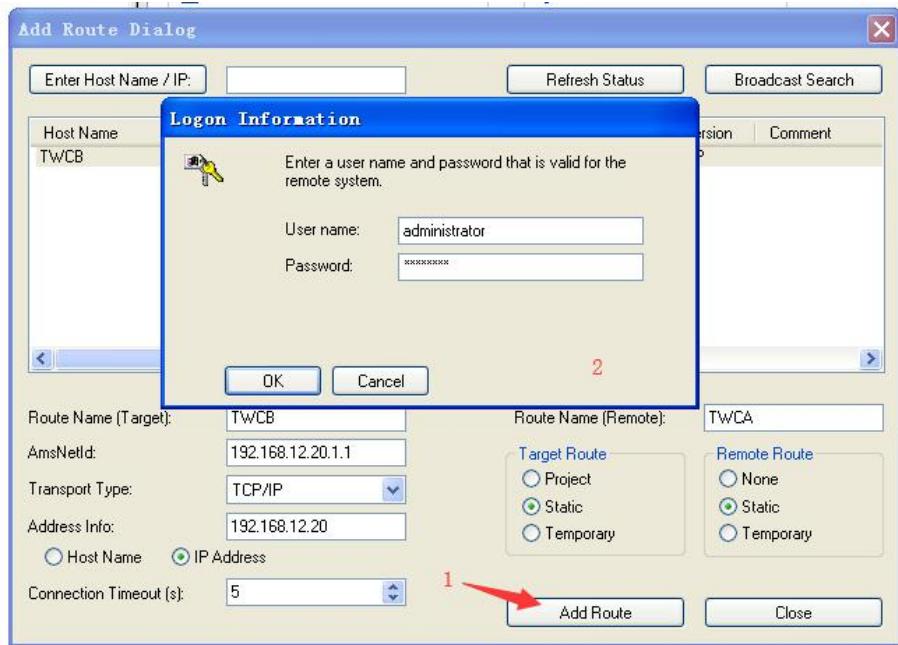
2.4. 倍福通讯设置示意

倍福 ADS 通讯需要在 PLC 所在电脑上设置路由，假设 PLC 所在电脑的 IP 地址是 192.168.12.10，录波软件所在电脑的 IP 地址是 192.168.12.20，则配置步骤如下（都是在 PLC 所在电脑上操作）：

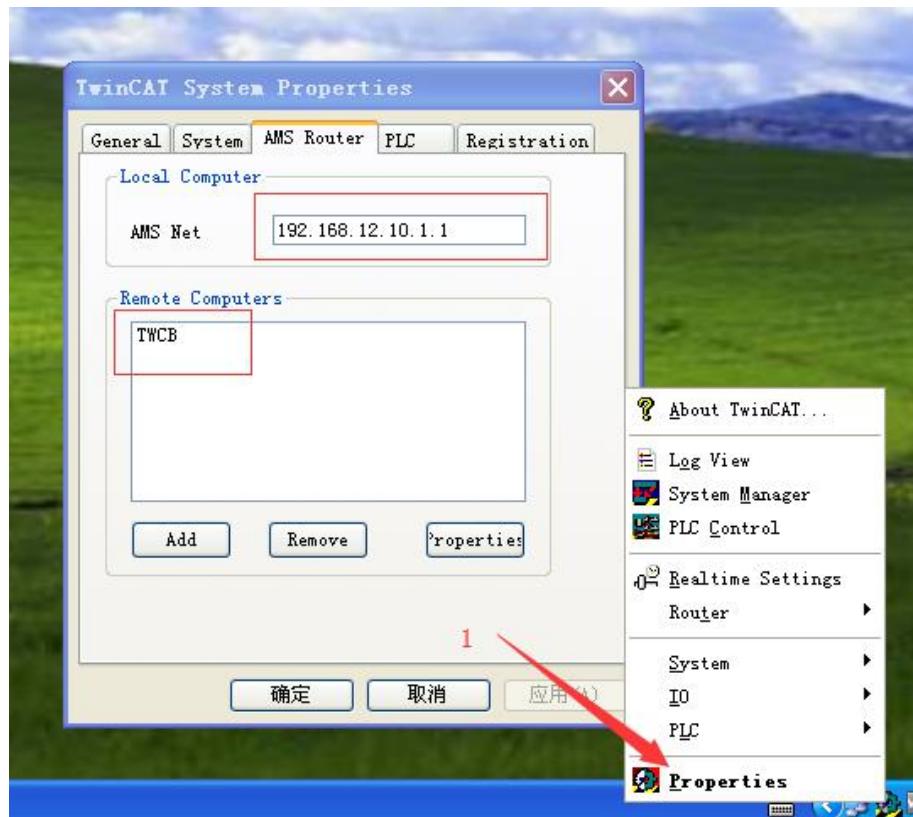
- 1) 打开 system manager
- 2) 在 Actions 菜单里选择 “Choose Target System” ->Search (Ethernet)
- 3) 搜索：

附录 1 各品牌设备的地址规范





4) 查看路由地址：确保已经匹配

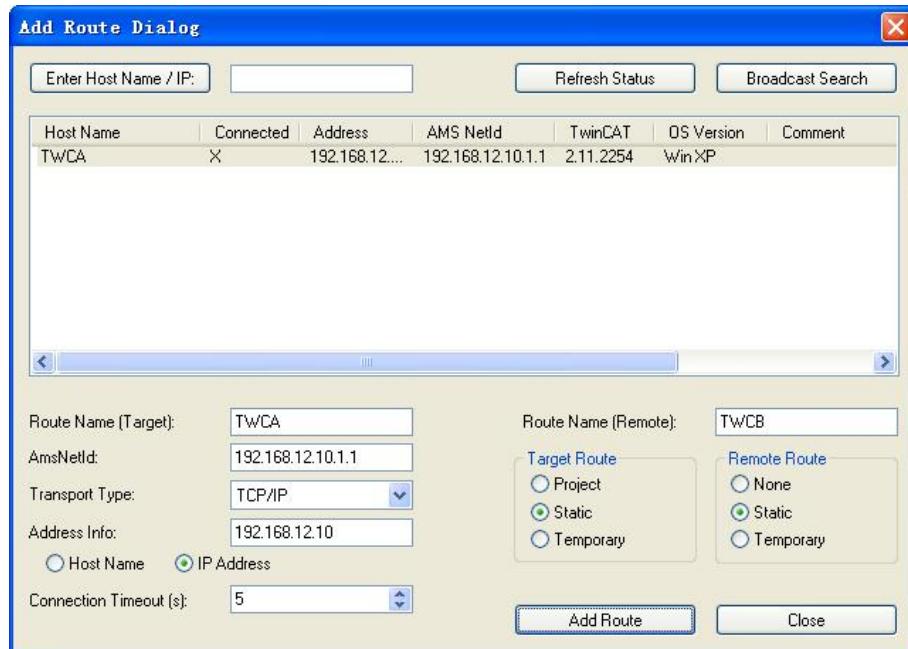


5) 通道配置：



“:801”仅指 TwinCAT2 的 PLC1，其他 PLC 依次对应 811、821、831，NC 为 500。TwinCAT3 对应的端口为 851 等。

配置完成后，在两侧的计算机里都能看到该新增条目，如果是在录波软件所在的计算机配置路由，步骤同上，但是结果如下：



2.5. 倍福通讯 ADS 通讯的一些经验

- ✓ ADS 通讯不是一个实时的通讯协议。
- ✓ 本地 ADS 通讯时间远小于远程 ADS 通讯时间。
- ✓ 降低基时间(Base Time，在 system manager 里面设置)的设置值可以适当的提升通讯速度。
- ✓ 较高的 CPU 占用率会严重降低通讯速度。
- ✓ 通讯时间和 PLC task 时间没有直接联系。

- ✓ 一次 ADS 通讯请求本机约为 1ms 左右, 远程约为 15ms 左右, 如 CPU 占用率过高 (例如 50%以上), 则可能大于 50ms。:

2.6. 故障代码

Member Name	Description
NoError	No Error. Error code: 0(0x000).
InternalError	Internal Error. Error code: 1(0x001).
NoRTime	No Rtime. Error code: 2(0x002).
LockedMemoryError	Allocation locked memory error. Error code: 3(0x003).
MailBoxError	Insert mailbox error. Error code: 4(0x004).
WrongHMsg	Wrong receive HMSG. Error code: 5(0x005).
TargetPortNotFound	Target port not found. Error code: 6(0x006).
TargetMachineNotFound	Target machine not found. Error code: 7(0x007).
UnknownCommandID	Unknown command ID. Error code: 8(0x008).
BadTaskID	Bad task ID. Error code: 9(0x009).
NoIO	No IO. Error code: 10(0x00A).
UnknownAmsCommand	Unknown AMS command. Error code: 11(0x00B).
Win32Error	Win 32 error. Error code: 12(0x00C).
PortNotConnected	Port is not connected. Error code: 13(0x00D).
InvalidAmsLength	Invalid AMS length. Error code: 14(0x00E).
InvalidAmsNetID	Invalid AMS Net ID. Error code: 15(0x00F).
LowInstallLevel	Low Installation level. Error code: 16(0x010).
NoDebug	No debug available. Error code: 17(0x011).
PortDisabled	Port disabled. Error code: 18(0x012).
PortConnected	Port is already connected. Error code: 19(0x013).
AmsSyncWin32Error	AMS Sync Win32 error. Error code: 20(0x014).
SyncTimeOut	AMS Sync timeout. Error code: 21(0x015).
AmsSyncAmsError	AMS Sync AMS error Error code: 22(0x016).
AmsSyncNoIndexMap	AMS Sync no index map. Error code: 23(0x017).
InvalidAmsPort	Invalid AMS port. Error code: 24(0x018).

Member Name	Description
NoMemory	No memory. Error code: 25(0x019).
TCPSendError	TCP send error. Error code: 26(0x01A).
HostUnreachable	Host unreachable. Error code: 27(0x1B).
NoLockedMemory	Router: no locked memory. Error code: 1280(0x500).
MailboxFull	Router: mailbox full. Error code: 1282(0x501).
DeviceError	error class <device error> Error code: 1792(0x700).
DeviceServiceNotSupported	Service is not supported by server. Error code: 1793(0x701).
DeviceInvalidGroup	Invalid index group. Error code: 1794(0x702).
DeviceInvalidOffset	Invalid index offset. Error code: 1795(0x703).
DeviceInvalidAccess	Reading/writing not permitted. Error code: 1796(0x704).
DeviceInvalidSize	Parameter size not correct. Error code: 1797(0x705).
DeviceInvalidData	Invalid parameter value(s). Error code: 1798(0x706).
DeviceNotReady	Device is not in a ready state. Error code: 1799(0x707).
DeviceBusy	Device is busy. Error code: 1800(0x708).
DeviceInvalidContext	Invalid context (must be in Windows). Error code: 1801(0x709).
DeviceNoMemory	Out of memory. Error code: 1802(0x70a).
DeviceInvalidParam	Invalid parameter value(s). Error code: 1803(0x70b).
DeviceNotFound	Not found (files, ...). Error code: 1804(0x70c).
DeviceSyntaxError	Syntax error in command or file. Error code: 1805(0x70d).
DeviceIncompatible	Objects do not match. Error code: 1806(0x70e).
DeviceExists	Object already exists. Error code: 1807(0x70f).
DeviceSymbolNotFound	Symbol not found. Error code: 1808(0x7010).
DeviceSymbolVersionInvalid	Symbol version is invalid. Error code: 1809(0x711).
DeviceInvalidState	Server is not in a valid state. Error code: 1810(0x712).
DeviceTransModeNotSupported	ADS transmode is not supported. Error code: 1811(0x713).
DeviceNotifyHandleInvalid	Notification handle is invalid. Error code: 1812(0x714).
DeviceClientUnknown	Notification client not registered. Error code: 1813(0x715).
DeviceNoMoreHandles	No more notification handles. Error code: 1814(0x716).

Member Name	Description
DeviceInvalidWatchsize	Size for watch to big. Error code: 1815(0x717).
DeviceNotInitialized	Device is not initialized. Error code: 1818(0x718).
DeviceTimeOut	Device has a timeout. Error code: 1817(0x719).
DeviceNoInterface	Query interface has failed. Error code: 1818(0x71A).
DeviceInvalidInterface	Wrong interface required. Error code: 1819(0x71B).
DeviceInvalidCLSID	Class ID is invalid. Error code: 1820(0x71C).
DeviceInvalidObjectID	Object ID is invalid. Error code: 1821(0x71D).
ClientError	Error class <client error> Error code: 1856(0x740).
ClientInvalidParameter	Parameter at service is invalid. Error code: 1857(0x741).
ClientListEmpty	Polling list is empty. Error code: 1858(0x742).
ClientVariableInUse	Variable connection is already in use. Error code: 1859(0x743).
ClientDuplicateInvokeID	Invoke ID already in use. Error code: 1860(0x744).
ClientSyncTimeOut	Timeout has elapsed. Error code: 1861(x745).
ClientW32OR	Error in win32 subsystem. Error code: 1862(0x746).
ClientTimeoutInvalid	Timeout value is invalid. Error code: 1863(0x747).
ClientPortNotOpen	Ads port is not opened. Error code: 1864(0x748).
ClientNoAmsAddr	No AMS addr. Error code: 1865(0x749).
ClientSyncInternal	An internal in ADS sync has occurred. Error code: 1872(0x750).
ClientAddHash	Hash table overflow. Error code: 1873(0x751).
ClientRemoveHash	There are no more symbols in the hash table. Error code: 1874(0x752).
ClientNoMoreSymbols	There are no more symbols in cache. Error code: 1875(0x753).
ClientSyncResInvalid	An invalid response has been received. Error code: 1876(0x754).
ClientSyncPortLocked	Sync port is locked. Error code: 1877(0x755).
ClientQueueFull	Client queue is full

说明

更多代码请参考倍福手册。

3. DELTA 台达

3.1. 地址对照表

类别	范围	长度	本软件 访问地址	各系列有效范围		
				ES/EX/SS	SA/SX/SH	EH
S	0~1023	bit	0000~1023	0~127	0~1024	0~1024
X	0~377 (8 进制)	bit	101024~101279	0~177	0~177	000~377
Y	0~377 (8 进制)	bit	101280~101535			
T	0~255	bit word	1536~1791 401536~401791	0~127	000~255	000~255
M	0~1535	bit	2048~3583	0~1279	0~4095	0000~4095
M	1536~4095	bit	45056~47615			
C	0~199	16-bit	3584~3783 403584~403783	0~127	0~199	0~199
	200~255	32-bit	3784~3839 403784~403839	232~255	200~255	200~255
D	0~4095	word	404096~408191	0~1311	0~4999	0000~9999
D	4096~9999	word	436864~442767			

3.2. 默认通道参数



4. Keyence 基恩士设备

支持 MC(Binary) 和 MC(ASCII) 协议的 KV-7500/7300、KV-5500/5000/3000、KV-Nano 等：

4.1. 地址对照表

注意：粗体的地址前缀与 PLC 内部不同，请按照“地址代号”里的格式输入。

地址名称	地址代号	示例	地址进制	字操作	位操作	PLC 内部变量范围 (各 PLC 可能不同)
输入继电器	RX	RX100,RX115	10	√	√	R00000~R99915
输出继电器	RY	RY100,RY115	10	√	√	R00000~R99915
链接继电器	B	B100,B1AB	10	√	√	B0000~B7FFF
内部辅助继电器	MR	MR100,MR215	10	√	√	MR00000~MR99915
锁存继电器	LR	LR100,LR200	10	√	√	LR00000~LR99915
控制继电器	CR	CR100,CR200	10	√	√	CR0000~CR7915
控制存储器	CM	CM100,CM200	10	√	×	CM0000~CM5999
数据存储器	DM	DM100,DM200	10	√	×	DM00000~DM65534
扩展数据存储器	EM	EM100,EM200	10	√	×	EM00000~EM65534
文件寄存器	FM	FM100,FM200	10	√	×	FM00000~FM32767
文件寄存器	ZF	ZF100,ZF1A0	10	√	×	ZF000000~ZF524287
链路寄存器	W	W100,W1A0	16	√	×	W0000~7FFF
定时器（当前值）	TN	TN100,TN200	10	√	×	T0000~T3999
定时器（接点）	TS	TS100,TS200	10	√	√	T0000~T3999
计数器（当前值）	CN	CN100,CN200	10	√	×	C0000~C3999
计数器（接点）	CS	CS100,CS200	10	√	√	C0000~C3999

4.2. 默认通道参数

<div style="border-bottom: 1px solid #ccc; padding-bottom: 10px;"> 通道修改 </div> <div style="margin-top: 10px;"> 通道类型: 基恩士 通道名称: PLC1 IP/ID: 192.168.0.1 协议类别: MC(Binary) 端口号: 5000 </div> <div style="margin-top: 20px;"> 采集周期: <input type="text" value="10"/> ms <input checked="" type="checkbox"/> 激活 </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="取消"/> <input type="button" value="保存并退出"/> </div>	<div style="border-bottom: 1px solid #ccc; padding-bottom: 10px;"> 通道修改 </div> <div style="margin-top: 10px;"> 通道类型: 基恩士 通道名称: PLC1 IP/ID: 192.168.0.1 协议类别: MC(ASCII) 端口号: 6000 </div> <div style="margin-top: 20px;"> 采集周期: <input type="text" value="10"/> ms <input type="checkbox"/> 激活 </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="取消"/> <input type="button" value="保存并退出"/> </div>
--	--

5. INOVANCE 汇川

5.1. 地址对照表 (H3U、H5U、XP 系列)

类别	范围	长度	本软件 访问地址	各系列有效范围		
				H3U	H5U	XP
M	0~7999	bit	0~7999	0~7679	0~7999	0~3071
M	8000~8511	bit	8000~8511	8000~8511	-	8000~8511
SM	0~1023	bit	9216~10239	0~1023	-	-
B	0~32767	bit	12288~45055	-	0~32767	-
S	0~4095	bit	57344~61439	0~4095	0~4095	0~999
T	0~511	bit	61440~61951	0~511	-	0~255
C	0~255	bit	62464~62719	0~255	-	0~255
X	0~1777 (8 进制)	bit	63488~64511	0~377	0~1777	0~377
Y	0~1777 (8 进制)	bit	64512~65535	0~377	0~1777	0~377
D	0~8511	word	400000~408511	0~8511	0~7999	0~8511
SD	0~1023	word	409216~410239	0~1023	-	-
R	0~32767	word	412288~445055	0~32767	0~32767	-
T	0~511	word	461440~461951	0~511	-	0~255
C	0~199	word	462464~462663	0~199	-	0~199
C	200~255	Dword	463232~463343	200~255	-	200~255

5.2. 地址对照表 (AM400_800)

包括 AM400、AM400_800、AC800 等。

类别	范围	长度	本软件 访问地址				
QX	0.0~8191.7	bit	0~65535				
IX	0.0~8191.7	bit	100000~165535				
MW	0~63335	word	300000~365535				
按bit 寻址	按Byte 寻址	按Word 寻址	按DWord 寻址				
QX0.0 QX0.1 QX0.2 QX0.3 QX0.4 QX0.5 QX0.6 QX0.7 QX1.0 QX1.1 QX1.2 QX1.3 QX1.4 QX1.5 QX1.6 QX1.7 QX2.0 QX2.1 QX2.2 QX2.3 QX2.4 QX2.5 QX2.6 QX2.7 QX2.8 QX2.9 QX3.1 QX3.2 QX3.3 QX3.4 QX3.5 QX3.6 QX3.7 QX4.0	QB0 QB1 QB2 QB3 QB4	QW0 QW1 QW2	QD0 QD1	MX0.0 MX0.1 MX0.2 MX0.3 MX0.4 MX0.5 MX0.6 MX0.7 MX1.0 MX1.1 MX1.2 MX1.3 MX1.4 MX1.5 MX1.6 MX1.7 MX2.0 MX2.1 MX2.2 MX2.3 MX2.4 MX2.5 MX2.6 MX2.7 MX3.1 MX3.2 MX3.3 MX3.4 MX3.5 MX3.6 MX3.7 MX4.0	MB0 MB1 MB2 MB3 MB4	MW0 MW1 MW2	MD0 MD1

寻址规则

5.3. 默认通道参数

附录 1 各品牌设备的地址规范



6. MITSUBISHI 三菱设备

6.1. MC(Binary)、MC(ASCII)协议

支持 PLC: Q06UDV、FX5U、Q02、L02 等, 起始地址格式:

地址名称	地址代号	示例	地址进制	字操作	位操作	备注
内部继电器 (位存储器)	M	M100,M200	10	×	√	以位编号
输入继电器	X	X100,X1A0	16	×	√	以位编号
输出继电器	Y	Y100,Y1A0	16	×	√	以位编号
锁存继电器	L	L100,L200	10	×	√	以位编号
报警器	F	F100,F200	10	×	√	以位编号
边沿继电器	V	V100,V200	10	×	√	以位编号
链接继电器	B	B100,B1A0	16	×	√	以位编号
步进继电器	S	S100,S200	10	×	√	以位编号
数据寄存器	D	D1000,D2000	10	√	×	以字编号
链接寄存器	W	W100,W1A0	16	√	×	以字编号
文件寄存器 (扩展寄存器)	R	R100,R200	10	√	×	以字编号
ZR 文件寄存器	ZR	ZR100,ZR2A0	16	√	×	以字编号
变址寄存器	Z	Z100,Z200	10	√	×	以字编号
定时器的触点	TS	TS100,TS200	10	×	√	以位编号
定时器的线圈	TC	TC100,TC200	10	×	√	以位编号
定时器的当前值	TN	TN100,TN200	10	√	×	以字编号
累计定时器的触点	SS	SS100,SS200	10	×	√	以位编号
累计定时器的线圈	SC	SC100,SC200	10	×	√	以位编号
累计定时器的当前值	SN	SN100,SN200	10	√	×	以字编号
计数器的触点	CS	CS100,CS200	10	×	√	以位编号
计数器的线圈	CC	CC100,CC200	10	×	√	以位编号
计数器的当前值	CN	CN100,CN200	10	√	×	以字编号
特殊寄存器	SM	SM0-SM2047	10	×	√	以位编号
特殊寄存器	SD	SD0-SD2047	10	√	×	以字编号

6.2. A1E 协议

支持 PLC: FX3U(C)等, 起始地址格式:

地址名称	地址代号	示例	地址进制	字操作	位操作	备注
内部继电器	M	M100,M200	10	×	√	以位编号
输入继电器	X	X10,X20	16	×	√	以位编号
输出继电器	Y	Y10,Y20	16	×	√	以位编号

地址名称	地址代号	示例	地址进制	字操作	位操作	备注
报警器	F	F100,F200	10	×	√	以位编号
链接继电器	B	B100,B1A0	16	×	√	以位编号
步进继电器	S	S100,S200	10	×	√	以位编号
数据寄存器	D	D1000,D2000	10	√	×	以字编号
链接寄存器	W	W100,W1A0	16	√	×	以字编号
文件寄存器	R	R100,R200	10	√	×	以字编号
定时器的触点	TS	TS100,TS200	10	×	√	以位编号
定时器的线圈	TC	TC100,TC200	10	×	√	以位编号
定时器的当前值	TN	TN100,TN200	10	√	×	以字编号
计数器的触点	CS	CS100,CS200	10	×	√	以位编号
计数器的线圈	CC	CC100,CC200	10	×	√	以位编号
计数器的当前值	CN	CN100,CN200	10	√	×	以字编号

6.3. FxSerialTcp 协议

支持 PLC: FX3U(C)等, 起始地址格式:

地址名称	地址代号	示例	地址进制	字操作	位操作	备注
内部继电器	M	M100,M200	10	×	√	以位编号
输入继电器	X	X10,X20	16	×	√	以位编号
输出继电器	Y	Y10,Y20	16	×	√	以位编号
报警器	F	F100,F200	10	×	√	以位编号
链接继电器	B	B100,B1A0	16	×	√	以位编号
步进继电器	S	S100,S200	10	×	√	以位编号
数据寄存器	D	D1000,D2000	10	√	×	以字编号
链接寄存器	W	W100,W1A0	16	√	×	以字编号
文件寄存器	R	R100,R200	10	√	×	以字编号
定时器的触点	TS	TS100,TS200	10	×	√	以位编号
定时器的线圈	TC	TC100,TC200	10	×	√	以位编号
定时器的当前值	TN	TN100,TN200	10	√	×	以字编号
计数器的触点	CS	CS100,CS200	10	×	√	以位编号
计数器的线圈	CC	CC100,CC200	10	×	√	以位编号
计数器的当前值	CN	CN100,CN200	10	√	×	以字编号

6.4. 默认通道参数

附录 1 各品牌设备的地址规范

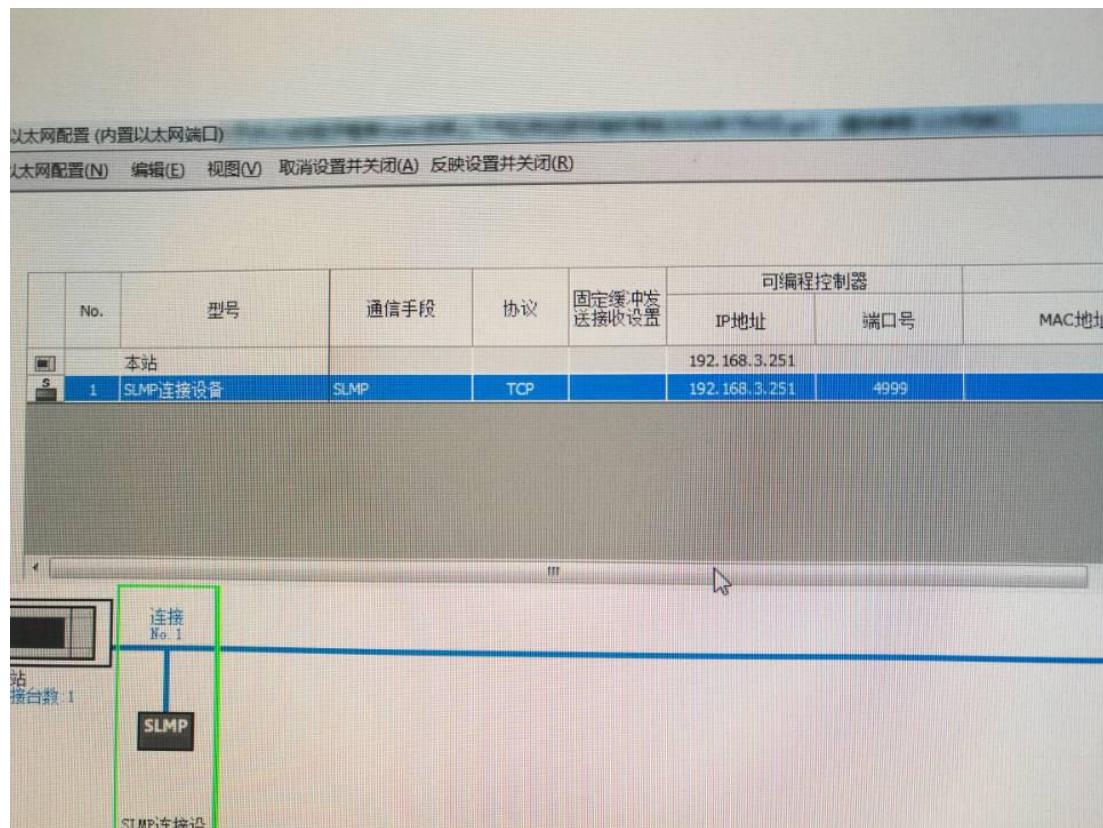


6.5. 三菱 PLC 设置示意

6.5.1. 以 GX Works3 为示例, fx5u 的配置如下



附录 1 各品牌设备的地址规范



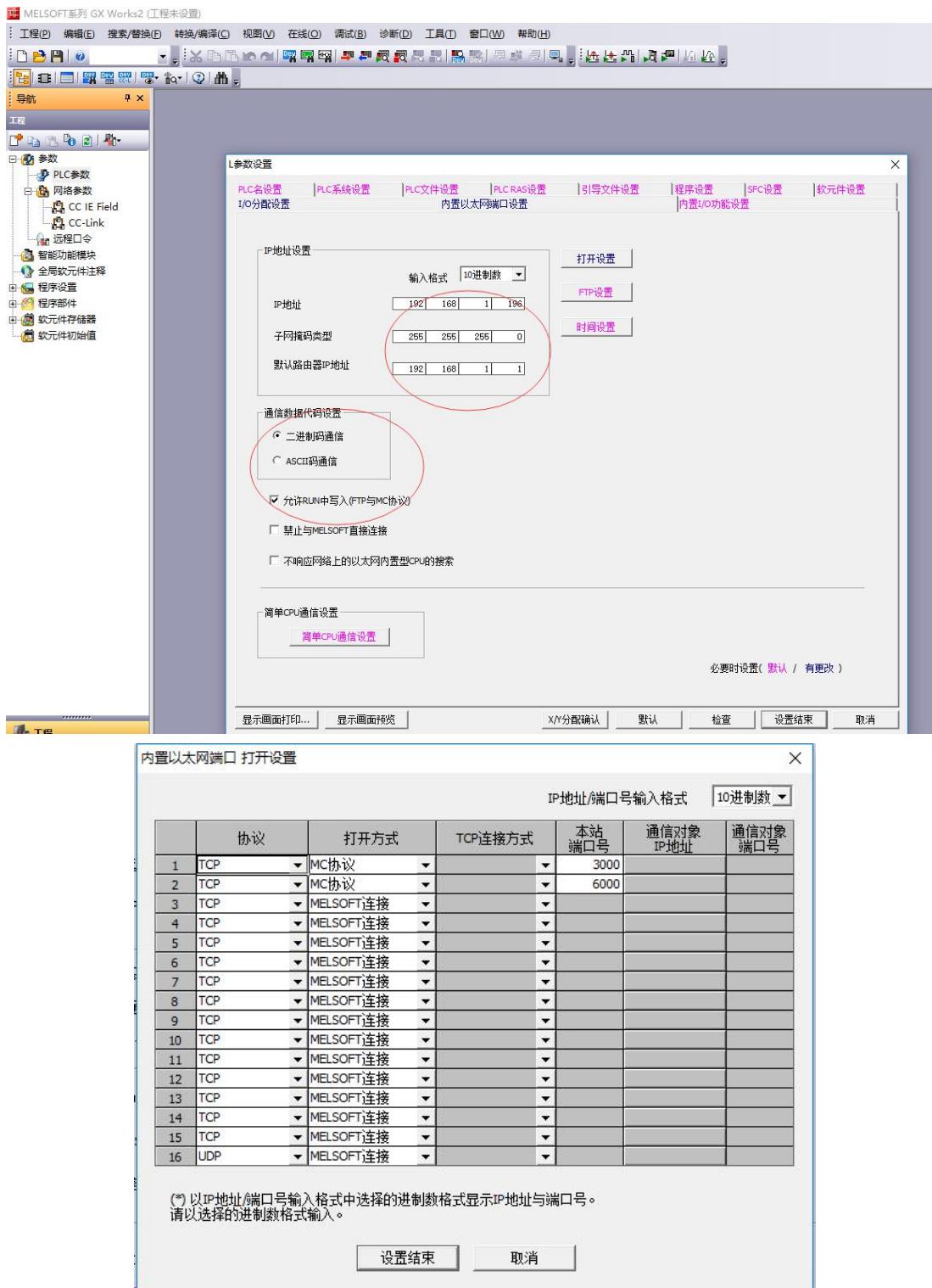
(感谢 山楂 提供的图片)

说明

为使配置生效，需要在线修改后，对于 PLC 重新上电，才能生效（断电时间请保持 7-10 秒）。

6.5.2. 以 GX Works2 为示例，测试 PLC 为 L02CPU

附录 1 各品牌设备的地址规范



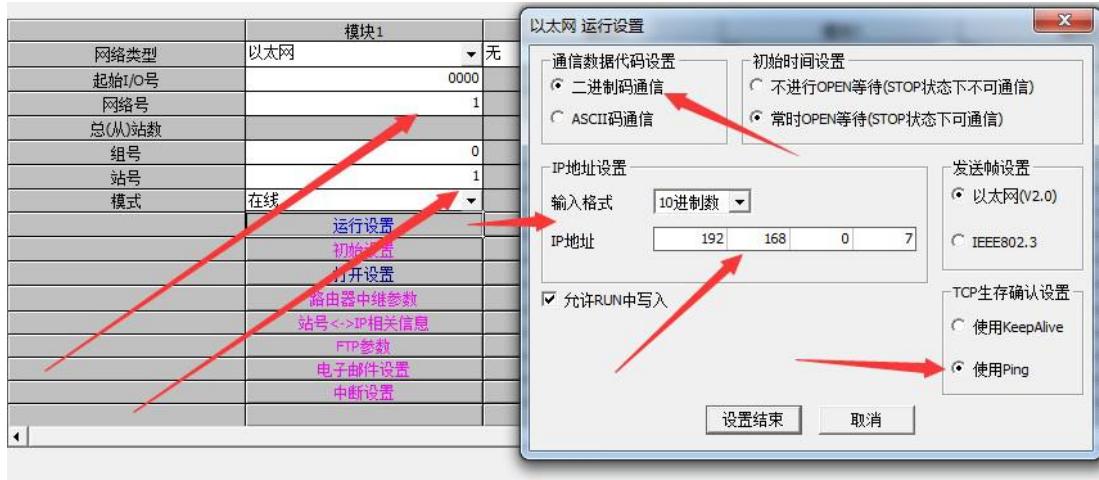
说明

为使配置生效，需要在线修改后，对于 PLC 重新上电，才能生效（断电时间请保持 7-10 秒）。

6.5.3. 以 GX Works2 为示例，添加以太网模块，型号为 QJ71E71-100

组态里添加完成后进行以太网的参数配置，此处需要注意的是：参数的配置对接下

来的代码中配置参数要一一对应



说明

在 PLC 的以太网模块的配置中，无法设置网络号为 0，也无法设置站号为 0，所以此处均设置为 1。

打开设置：

在上图中的打开设置选项，进行其他参数的配置，下图只是举了一个例子，开通了 4 个端口来支持读写操作：(本软件只需要读取 PLC 数据，因此，可以减少端口数量)。



端口号设置规则：

为了不与原先存在的系统发生冲突，您在添加自己的端口时尽量使用您自己的端口。

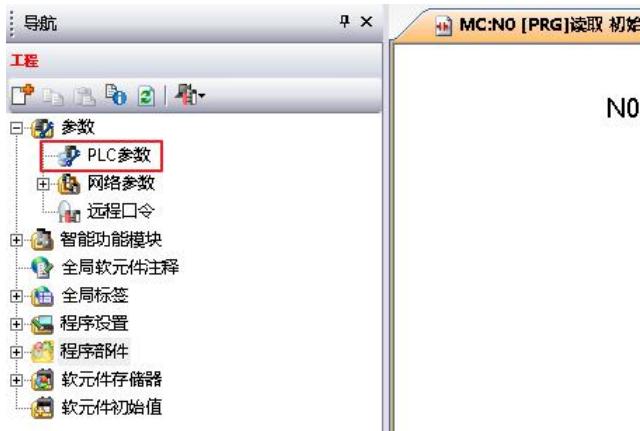
如果您的网络状态不是特别稳定，读取端口使用 2 个，一个受阻切换另一个读取可以提升系统的稳定性。

说明

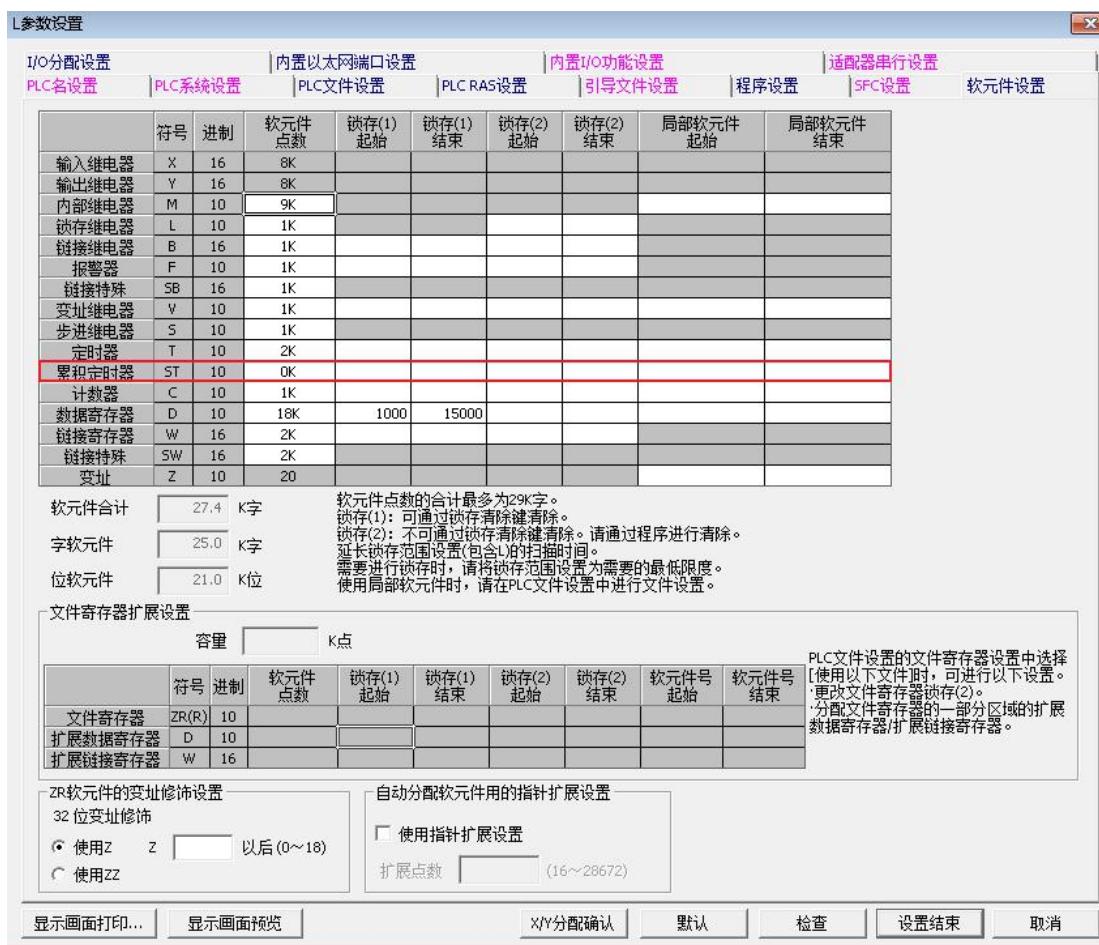
为使配置生效，需要在线修改后，对于 PLC 重新上电，才能生效（断电时间请保持 7-10 秒）。

6.5.4. 启用累计定时器的方法

点击“参数” => “PLC 参数” => “软元件设置”。给累计定时器一栏分配点数为“1k”，范围是 0-999。设置完毕点击检查，没有错误软件会弹窗提示无错误，无误就是设置完成，点击“设置结束”保存设置并关闭设置画面。



进入界面



启用前

	符号	进制	软元件点数		锁存(1)		锁存(2)		局部软元件起始		局部软元件结束	
			起始	结束	起始	结束	起始	结束	起始	结束	起始	结束
输入继电器	X	16	8K									
输出继电器	Y	16	8K									
内部继电器	M	10	9K									
锁存继电器	L	10	1K									
链接继电器	B	16	1K									
报警器	F	10	1K									
链接特殊	SB	16	1K									
变址继电器	V	10	1K									
步进继电器	S	10	1K									
定时器	T	10	2K									
累积定时器	ST	10	1K	0	999							
计数器	C	10	1K									
数据寄存器	D	10	18K	1000	15000							
链接寄存器	W	16	2K									
链接特殊	SW	16	2K									
变址	Z	10	20									

软元件占有的合计最多为29K字。

启用后

说明

为使配置生效，需要在线修改后，对于 PLC 重新上电，才能生效（断电时间请保持 7-10 秒）。

6.5.5. 设置文件寄存器 ZR 的方法

在参数设置界面点击“PLC 文件设置”。在“文件寄存器”一栏选中“使用以下文件”，“文件名”那里填写 ZR，容量填写 128k 或者 120k 都可以。设置完毕点击“检查按钮”。然后再点击“软元件设置”。在弹出的窗口中“文件寄存器扩展设置”那里照着图上的红色框选设置即可，设置完毕，点击“检查”，软件提示没有错误之后再点击“设置结束”。

编译程序，保存一下，下载一遍程序（下载的时候勾选参数和程序），下载完毕，PLC 断电 10 秒钟，然后上电即可。

附录 1 各品牌设备的地址规范



“PLC 文件设置”界面

文件寄存器扩展设置

容量 120 K点									
	符号	进制	软元件点数	锁存(1)起始	锁存(1)结束	锁存(2)起始	锁存(2)结束	软元件号起始	软元件号结束
文件寄存器	ZR(R)	10	1K			0	1023	ZR0	ZR1023
扩展数据寄存器	D	10	118K					D18432	D139263
扩展链接寄存器	W	16	1K					W800	WBFF

ZR软元件的变址修饰设置
 32位变址修饰
 使用Z Z [] 以后 (0~18)
 使用Z2
自动分配软元件用的指针扩展设置
 使用指针扩展设置
 扩展点数 [] (16~28672)

PLC文件设置的文件寄存器设置中选择
 [使用以下文件时]，可进行以下设置。
 ·更改文件寄存器锁存(2)。
 ·分配文件寄存器的一部分区域的扩展数据寄存器/扩展链接寄存器。

“软元件设置”界面

说明

为使配置生效，需要在线修改后，对于 PLC 重新上电，才能生效（断电时间请保持 7-10 秒）。

7. 标准 Modbus-TCP 设备

7.1. 通用说明

以位为单位的变量：

线圈：00000(1)-99999 (不超过 5 位) (功能码：01)

离散寄存器：100000(1)-199999 (6 位) (功能码：02)

以字为单位的变量：

保持寄存器：400000(1)-499999 (6 位) (功能码：03)

输入寄存器：300000(1)-399999 (6 位) (功能码：04)

说明

对于短地址的设备，线圈地址可以直接使用，其他地址需要在首位（首位用于识别设备里的存储区域）后加“0”来补足 6 位。比如，原地址为 3012，则此处的地址应该改变为 300012。

7.2. 默认通道参数



8. Omron 欧姆龙设备

8.1. Fins-TCP 协议

字操作，例如：D20、C20、W20、H20、A20。

位操作：字地址.位地址 (0-15)，比如：D20.7、E0.0.7

地址名称	地址 代号	示例	地址 进制	字 操作	位 操作	备注
DM 区域	D	D100,D200	10	√	√	以字编号
CIO 区域	C	C100,C200	10	√	√	以字编号
工作区域	W	W100,W200	10	√	√	以字编号
保持位区域	H	H100,H200	10	√	√	以字编号
辅助位区域	A	A100,A200	10	√	√	以字编号
EM 区域	E	E0.0,EF.200,E10 .100	10	√	√	以字编号

8.2. CIP 协议

直接输入变量名称即可，不做语法检查，可参考 [AB 的地址规范](#)。

所有需要外部访问的变量，请在 PLC 里进行网络公开。

适用 PLC：NX701-1600 等。

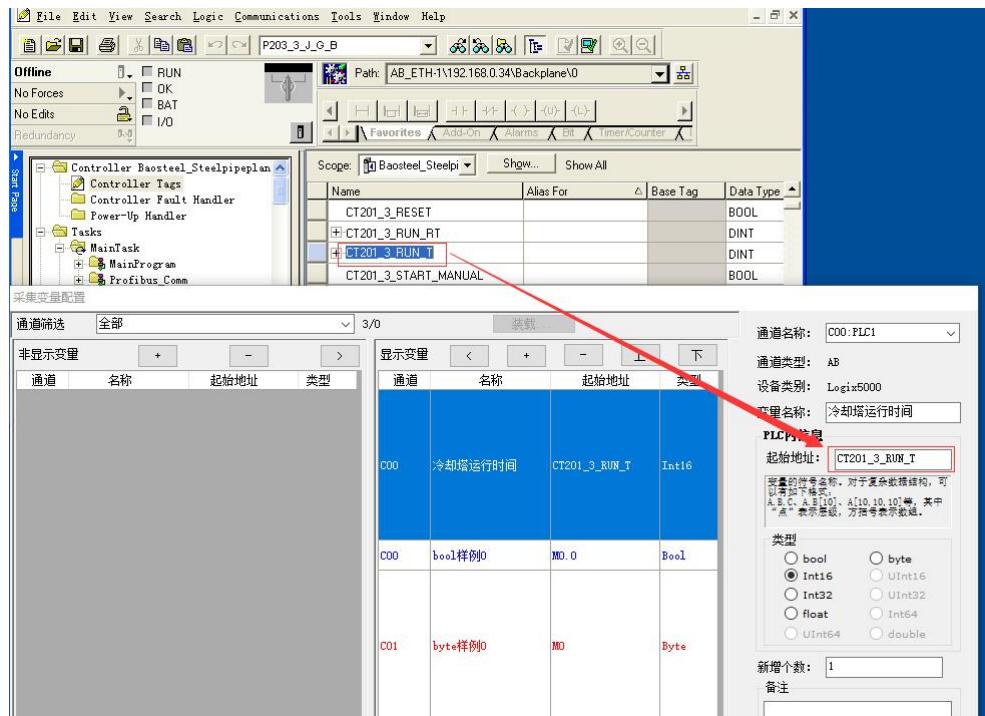
8.3. 默认通道参数



9. Rockwell 罗克韦尔 (AB) 设备

9.1. 地址规范

支持 PLC: ControlLogix 5000、Micro800 系列。



变量的起始地址是指变量在 PLC 内部的符号名称 (Tag 表里的 Name 部分), 不区分大小写 (软件自动转成大写)。在 Logix Designer 软件 (version 21.00.00 及以上) 和 RSLogix 5000 软件 (version 18.00.00 及以上) 可以设置变量是否允许外部访问, 请确保所有需要采集的变量都被设置为“读写”或者“只读”。

变量寻址的有效字符:

- ✓ 字母 (a 至 z, A 至 Z)
- ✓ 数字 (0 到 9)
- ✓ 下划线 (_))。

对于全局变量: 符号地址可以是简单地址, 如 force。也可以是复杂数据结构, 起始地址可以有如下格式: A.B.C、A.B[10]、A[10,10,10]、Local:1.l.Data0 等, 其中 “.” 表示层级, 方括号表示数组。

如需访问局部变量, 起始地址的规范如下: Program:mainprogram¹⁾.a²⁾。

注:

¹⁾ 程序名称。

²⁾ 局部变量表里的变量, 其地址规则同全局变量, 比如: Program:mainprogram.A.B[10]。

请确保各变量的数据类型与 PLC 内的类型一致，以免转换出错。

说明

- 1、如果无法直接访问某模块特定的变量，例如，输入和输出模块上的数据。可尝试使用控制器中的变量别名代替。
- 2、对于整型的变量（byte、int、dint 等），PLC 内部可以直接访问变量的位，但是，对外是不允许的，还需按照 byte、int、dint 等格式进行访问。如果在 PLC 内给这些变量的位起一个别名，则可以通过该别名变量进行外部访问。

9.2. 默认通道参数



10.RunPower 蓝普峰

RPC2000 系列



11. Panasonic 松下设备

11.1. Mewtocol 协议

触点地址的输入的格式说明如下：

位操作：非位地址用 10 进制表示，位用 16 进制 0-F 表示

地址名称	地址代号	示例	非位地址进制	字操作	位操作
外部输入继电器	X	X10,X1F	10	×	√
外部输出继电器	Y	Y0,Y10F	10	×	√
内部继电器	R	R0,R10F	10	×	√
定时器	T	T0,T100	10	×	√
计数器	C	C0,C100	10	×	√
链接继电器	L	L10,L10F	10	×	√

数据地址的输入的格式说明如下：

地址名称	地址代号	示例	地址进制	字操作	位操作
数据寄存器 DT	D	D0,D100	10	√	×
链接寄存器 LD	LD	LD0,LD100	10	√	×
文件寄存器 FL	F	F0,F100	10	√	×
目标值 SV	S	S0,S100	10	√	×
经过值 EV	K	K0,K100	10	√	×
索引寄存器 IX	IX	IX0,IX100	10	√	×
索引寄存器 IY	IY	IY0,IY100	10	√	×

说明

1、需要在 PLC 里启用该协议，且确保该连接不被其他设备通讯占用。



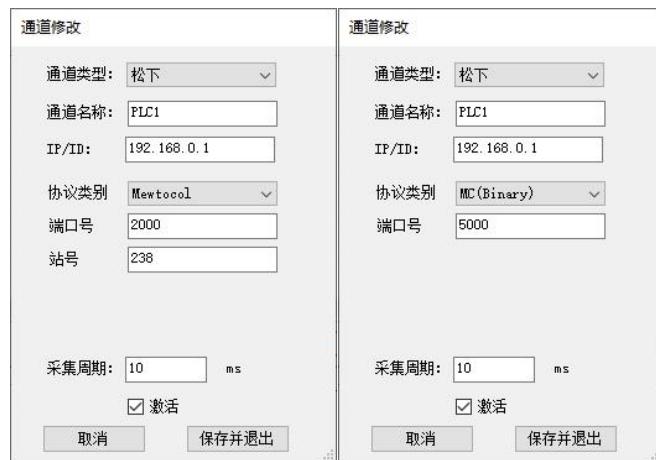
11.2. MC(Binary)

地址的输入的格式说明如下：

位操作：非位地址用 10 进制表示，位用 16 进制 0-F 表示

地址名称	地址 代号	示例	地址范围	字 操作	位 操作
输入继电器	X	X0000,X100F	X0000 ~ X109F	√	√
输出继电器	Y	Y0000,Y100F	Y0000 ~ Y109F	√	√
链接继电器	L	L0000,L100F	L0000 ~ L0127F	√	√
内部继电器	R	R0000, R100F	R0000 ~ R511F, R9000 ~ R951F	√	√
数据存储器	D	D100,D200	D0 ~ D65532, D90000 ~ D90999	√	✗
链路寄存器	LD	LD0,LD100	LD0 ~ LD255	√	✗
定时器（当前值）	TN	TN100,TN200	TN0 ~ TN1023	√	✗
定时器（接点）	TS	TS100,TS200	TS0 ~ TS1023	√	√
计数器（当前值）	CN	CN100,CN200	CN0 ~ CN1023	√	✗
计数器（接点）	CS	CS100,CS200	CS0 ~ CS1023	√	√

11.3. 默认通道参数

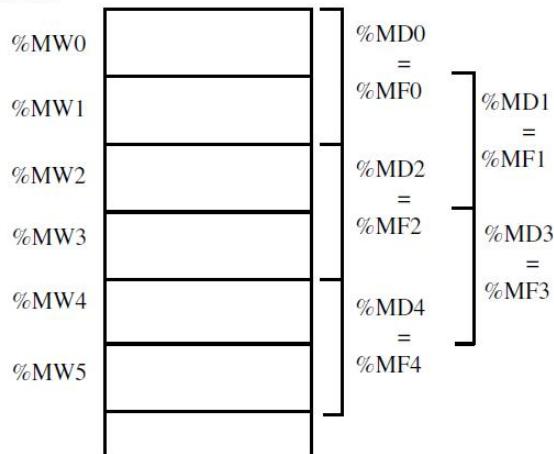


12. Schneider 施耐德

施耐德各型 PLC 原生支持 Modbus-TCP 协议，且各 PLC 内部地址类型与本软件的地
址类型对应关系都一样（可参考下述任意 PLC 的地址范围），可能的不同：首地址是否
从 0 开始及字节顺序（经过测试的都是 CDAB 顺序）。因此，如果需要对于下述之外
的 PLC 进行录波，请首先验证本类型的 PLC 首地址是否从 0 开始。

内存组织图如下：

内存组织：



12.1. Quantum (昆腾)

12.1.1. 地址范围：

PLC 内地址示例	本软件的对应地址	本软件地址范围
DI: %I127	100127	100001~165535
DO: %Q417 M (位): %M	417	1~65535
MW: %MW417	400417	400001~465535
IW: %IW3	300003	300001~365535

说明

1、具体地址范围由用户在 PLC 内定义确定（见下图的红色区域）



12.1.2. 默认通道参数

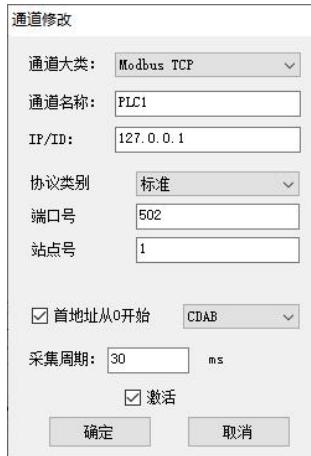


12.2. Premium (奔腾系列)

12.2.1. 地址范围:

PLC 内地址	本软件的地址	本软件地址范围
DI: %I127	100127	100000~165535
DO: %Q417	417	0~65535
MW: %MW417	400417	400000~465535

12.2.2. 默认通道参数

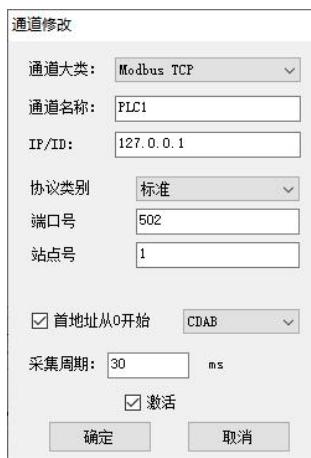


12.3. M580

12.3.1. 地址范围:

PLC 内地址	本软件的地址	本软件地址范围
M (位): %M	417	0~65535
MW: %MW417	400417	400000~465535

12.3.2. 默认通道参数



13.SIEMENS 西门子设备

13.1. 地址规范

支持的地址区域包括：I、Q、M、DB、V（对于 S7-200、S7-200SMART）。不支持T和C区域信息。

起始地址的表达方式包括两种：模糊方式和准确方式。举个例子：我们习惯的MD4就是一种模糊方式，它可能表示长整型、也可能表示浮点数。

对于准确方式，变量在 PLC 里的地址由本栏的起始地址和后面的类型来唯一确定。比如，MD4 的准确表达可能是：起始地址 M4，类型：float。

在起始地址栏里，可以输入模糊地址，输入后，可能的数据类型将变成红色，供选择。同时，将自动选择第一个可能的类型，你也可以手动修改类型。同时，**地址将转变成准确表达方式，这也是最终使用的地址格式。**接受的模糊地址：IBx、IWx、IDx、QBx、QWx、QDx、MBx、MWx、MDx、DBx.DBBy、DBx.DBWy、DBx.DBDy、DBx.DBXy.z

对于 S7-200、S7-200SMART，还包括：VBn、VWn、VDn

字符串的模糊格式：VBn、MBx、DBx.DBBy 等。

模糊方式不能涵盖 PLC 的很多新数据类型，因此，建议尽量使用准确方式。

西门子的变量地址采用了按照字节编号（地址可重叠），因此，要非常注意地址的编号，下图以 M 区域为例，非常详细地说明了字节编号、位编号、字编号、双字编号的原则：

											BYTE																				
											WORD																				
											DWORD																				
x31	x30	x29	x28	x27	x26	x25	x24	x23	x22	x21	x20	x19	x18	x17	x16	x15	x14	x13	x12	x11	x10	x9	x8	x7	x6	x5	x4	x3	x2	x1	x0
b3					b2					b1					b0																
w1										w0																					

图 12.1 西门子字节编号的原则示意图

13.2. 默认通道参数

附录 1 各品牌设备的地址规范

<div style="border: 1px solid #ccc; padding: 5px;"> <p>通道修改</p> <p>通道类型: 西门子</p> <p>通道名称: PLC1</p> <p>IP/ID: 192.168.0.1</p> <p>设备类型 S7-200</p> <p>框架号 0</p> <p>插槽号 0</p> <p>端口号 102</p> <p>采集周期: 10 ms <input checked="" type="checkbox"/> 激活</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>通道修改</p> <p>通道类型: 西门子</p> <p>通道名称: PLC1</p> <p>IP/ID: 192.168.0.1</p> <p>设备类型 S7-200Smart</p> <p>框架号 0</p> <p>插槽号 0</p> <p>端口号 102</p> <p>采集周期: 10 ms <input checked="" type="checkbox"/> 激活</p> </div>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>通道修改</p> <p>通道类型: 西门子</p> <p>通道名称: PLC1</p> <p>IP/ID: 192.168.0.1</p> <p>设备类型 S7-1200</p> <p>框架号 0</p> <p>插槽号 1</p> <p>端口号 102</p> <p>采集周期: 100 ms <input checked="" type="checkbox"/> 激活</p> </div>
<input type="button" value="取消"/> <input type="button" value="保存并退出"/>		
<input type="button" value="取消"/> <input type="button" value="保存并退出"/>		
<input type="button" value="取消"/> <input type="button" value="保存并退出"/>		

13.3. 其他相关信息

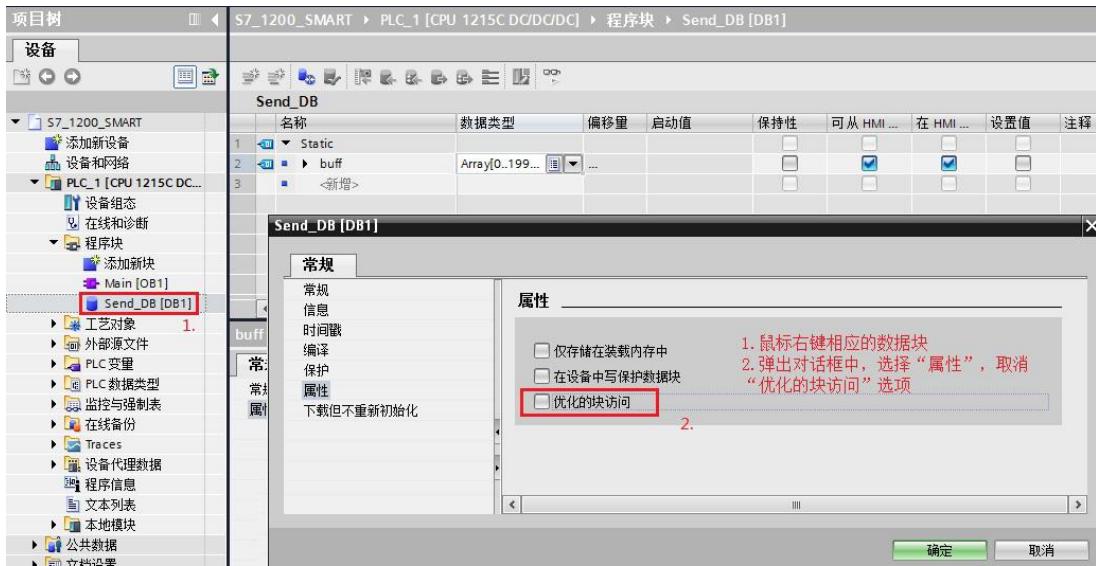
13.3.1. S7-1200 与 S7-1500 的特殊设置

- ✓ CPU 需设置成允许远程伙伴的 PUT/GET 通信访问（界面类似下面）



- ✓ 如果要访问 DB 块，则 DB 块需设置成非优化地址访问：

附录 1 各品牌设备的地址规范



13.3.2. 如何访问西门子的 T 和 C 变量

对于西门子传统的 T 和 C 变量，目前还没有办法进行这两个类型的读取，如需采集，建议在 PLC 内部，将欲读取的内容先读入本软件能访问的区域（比如 M、DB、V 等），然后用本软件去读取后者。

对于 IEC 定时器、IEC 计数器、Time 等变量，可以通过偏移量访问其内部各元素：

数据块_1					
	名称	数据类型	偏移量	起始值	监视
10	wstring1	WString	28.0	WSTRING#''	???
11	wstring2	WString	540.0	WSTRING#''	???
12	timer	IEC_TIMER	1052.0		
13	PT	Time	1056.0	T#0ms	???
14	ET	Time	1060.0	T#0ms	???
15	IN	Bool	1064.1	false	???
16	Q	Bool	1064.2	false	???
17	t1	Time	1068.0	T#0ms	
18	t2	Time	1072.0	T#0ms	
19	c	IEC_COUNTER	1076.0		
20	CU	Bool	1076.0	false	
21	CD	Bool	1076.1	false	
22	R	Bool	1076.2	false	
23	LD	Bool	1076.3	false	
24	QU	Bool	1076.4	false	
25	QD	Bool	1076.5	false	
26	PV	Int	1078.0	0	
27	CV	Int	1080.0	0	
28	<新增>				

13.3.3. 如何访问 LOGO!?

请用 S7-200SMART、S7-200 或者 S7-1200 驱动尝试一下。

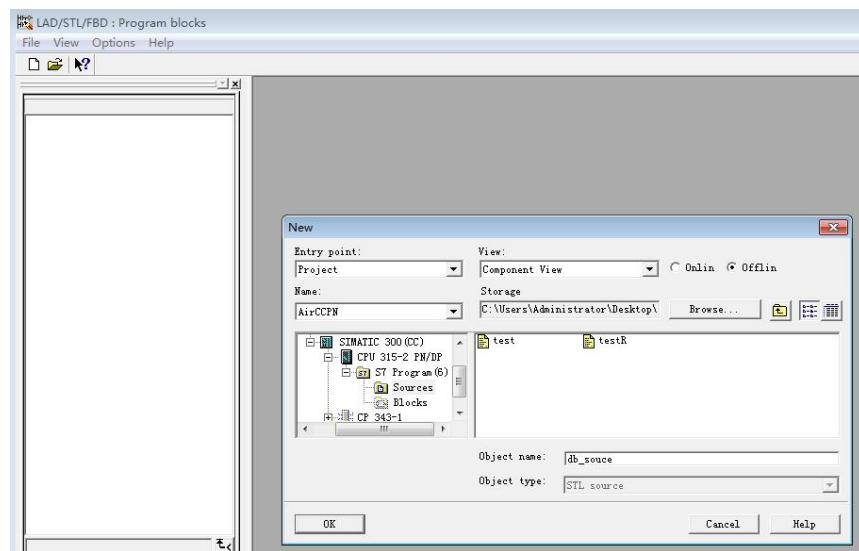
13.3.4. STEP7 数据块变量导入步骤

步骤 1. 打开 STEP7 的持续编辑器，选择里面的 “Generate Source...”：

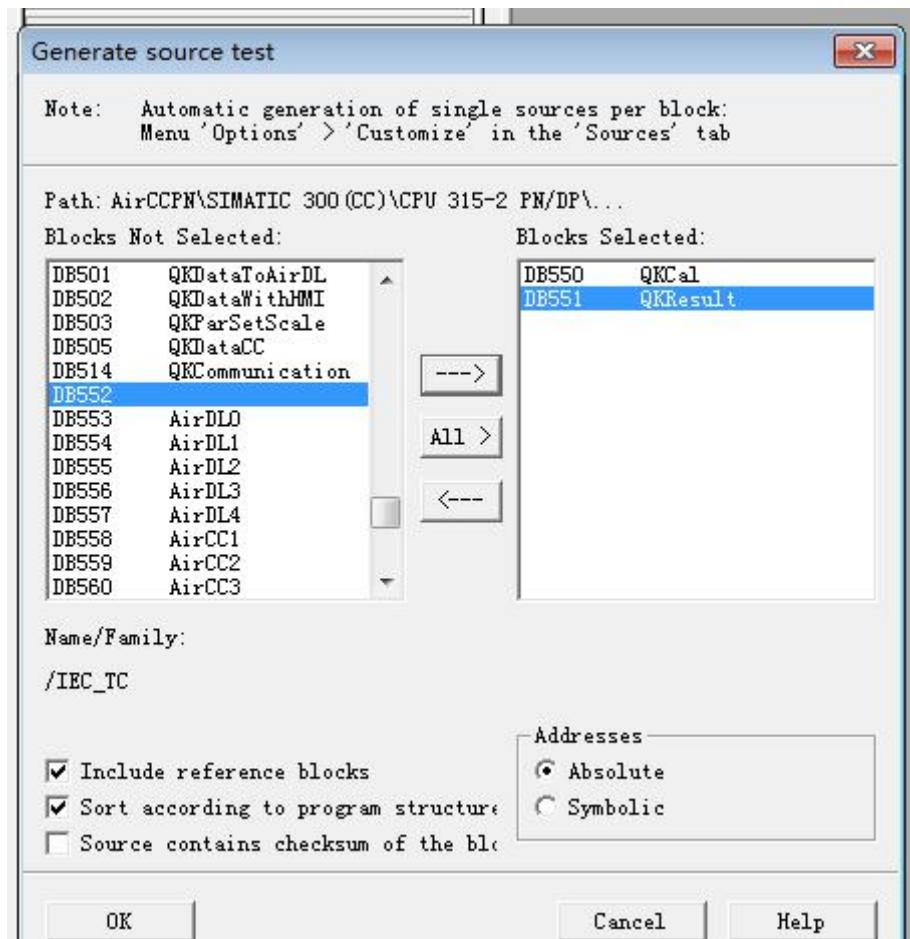
附录 1 各品牌设备的地址规范



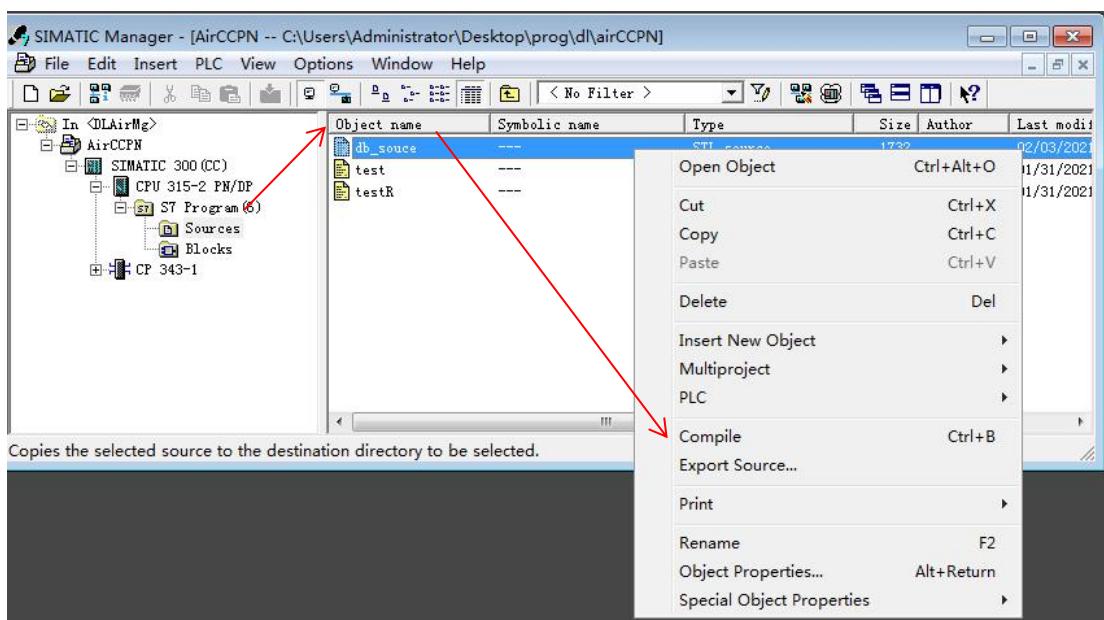
步骤 2. 创建一个源程序，此处为 db_source:



步骤 3. 选择需要导出的 DB 块 (可以选择多个)，勾选左下角的两个选项，确认后开始导出：

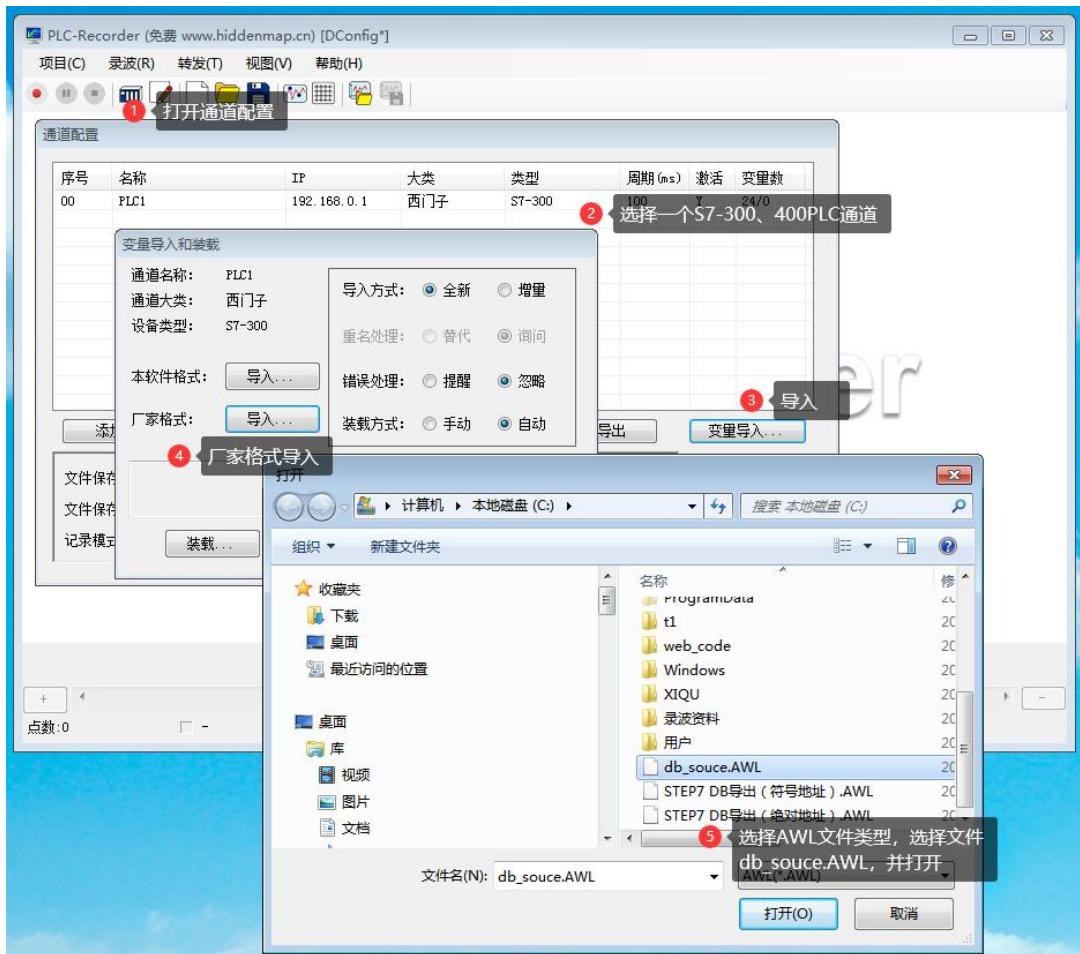


步骤 4. 将源程序进行输出，获得 db_source.AWL:



步骤 5. 打开录波软件，并进行导入操作：

附录 1 各品牌设备的地址规范

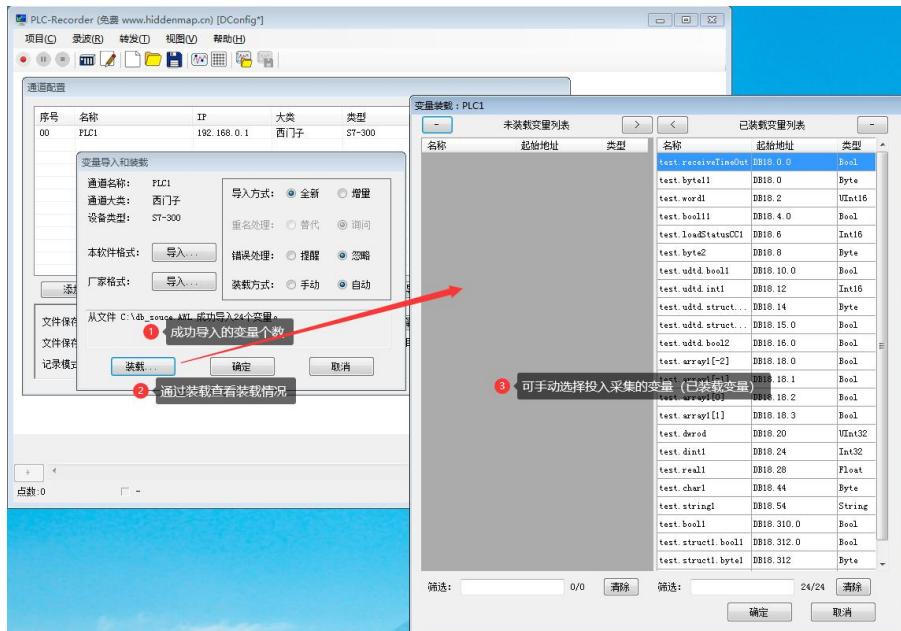


步骤 6. 确定 DB 块编号 (如果是符号地址, 则需要该步骤)



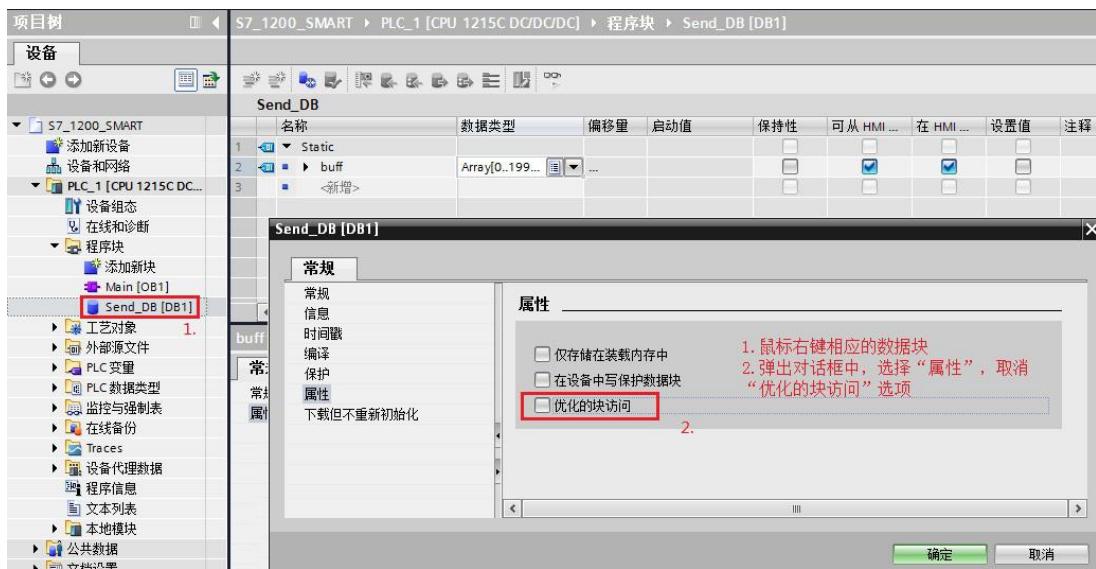
步骤 7. 进行装载确认

附录 1 各品牌设备的地址规范



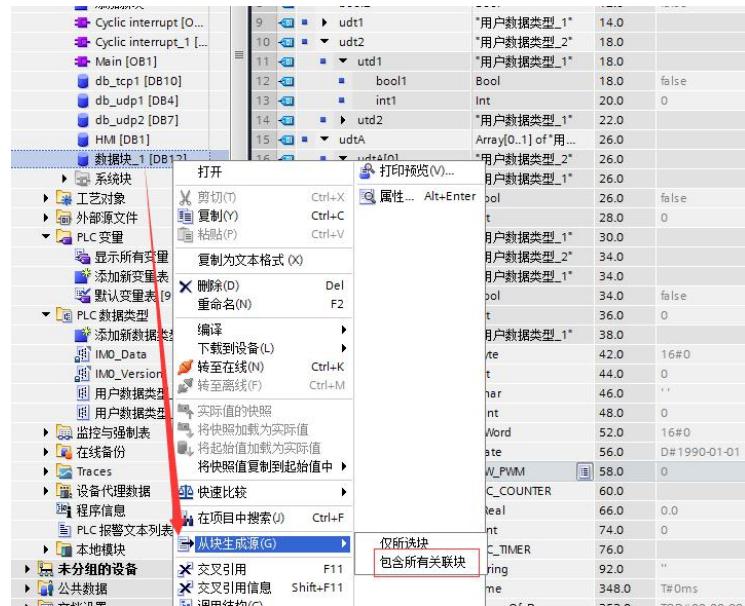
13.3.5. 博图数据块变量导入步骤

步骤 1. 将待导出的 DB 块取消优化访问

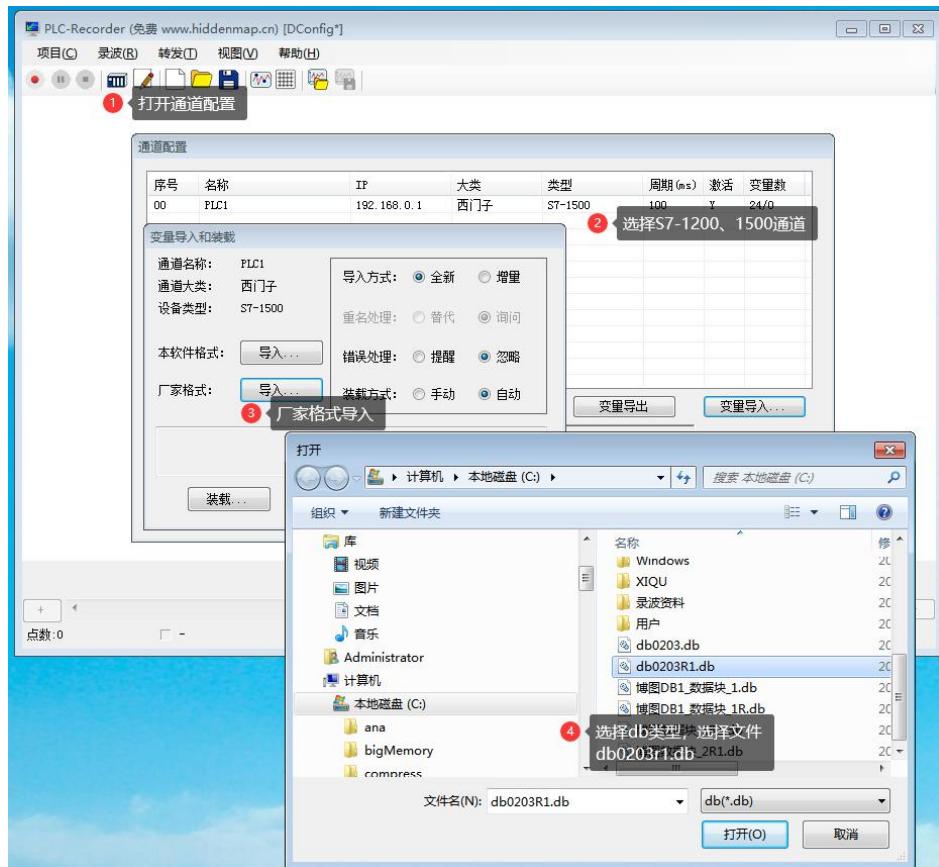


步骤 2. 在博图里选择待导出的 DB 块 (可以选择多个), 右键进行导出, 注意选择 “包含所有关联块”:

附录 1 各品牌设备的地址规范



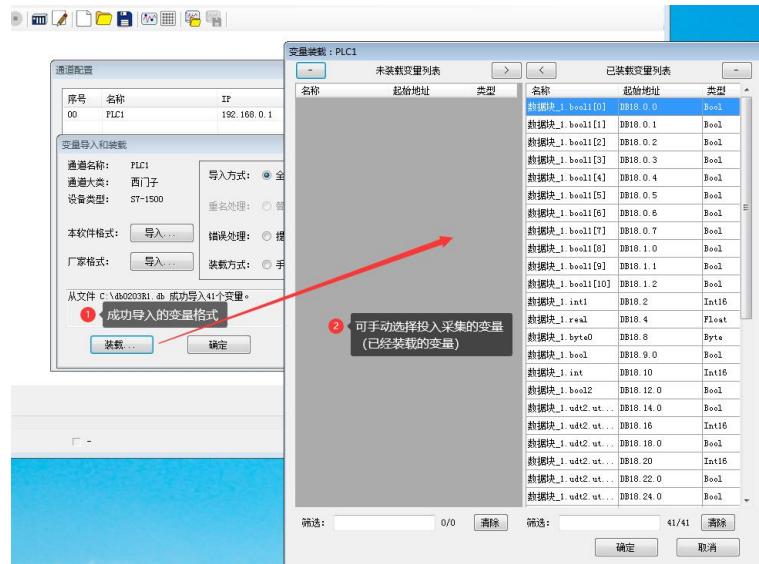
步骤 3. 导入



步骤 4. 确定 DB 块编号



步骤 5. 进行装载确认



附录 2 变量导出文件格式

列序号	列名称	含义及格式
1	名称	变量的名称
2	地址	变量的地址
3	类型	数据类型: bool、byte、Int16、UInt16、Int32、UInt32、float、Int64、UInt64、double、string、wstring
4	备注	变量说明
5	k	
6	b	变量标定因子: $y=kx+b$
7	显示最大值	
8	显示最小值	
9	小数位	非 bool 类型时，显示的小数点后数字的位数。
10	单位	
11	颜色	颜色的名称或者成分组成
12	是否在线显示	
13	显示高度	以像素为单位
14	显示顺序	
15	装载状态	
16	字符串长度	
17	字符串结构	

附录 3 转发信息交互的过程

步骤	功能	服务器	方向	客户端	备注
①	建立连接		<-	主动建立连接	自动维持心跳。
②	客户端验证	如果非法，则拒绝	<-	发送验证信息	可选：可与后续查询、验证的步骤合并执行。
③		发送结果信息	->		
④	读取设备和变量信息		<-	发送读取请求	可选（带有验证信息）
⑤		发送信息结果	->		
⑥	订阅变量		<-	发送订阅通知	带有验证信息
⑦		反馈订阅结果	->		
⑧	单次更新		<-	请求全部变量值	主要用于第一次更新
⑨		发送全部变量的值	->		
⑩	周期更新	更新变化的变量值	->	根据变量名称进行数值更新	

注：**黑体下划线**的为关键步骤，不可缺少。

附录 4 转发电文格式

功能	方向	功能码	详细信息	接收方响应
客户端验证	Server<-Client/Browser	FC=10	ID =abc(string) 识别信息	服务器根据 IP 地址、ID 判断是否合法。
	Server->Client/Browser	FS=10	<u>RESULT</u> =(int) 1: 成功 2: 失败, 原因见 REASON 3: 服务器的原因, 需要重新订阅 <u>REASON</u> =失败原因(string)	
读取设备和变量信息	Server<-Client/Browser	FC=20	ID =abc(string) 识别信息 (第一次请求时使用)	若未验证, 则进行一次验证。 若验证通过, 则反馈设备和变量信息。
	Server->Client/Browser	FS=20	<u>listChanel</u> :通道列表 每个通道包括(通道编号 CID (int)、通道名称 TNAME (string)、设备大类 BIGTYPE (string)、设备类别 DEVICETYPE (string)、采样周期 CYCLE (double)) <u>listTagInfo</u> :变量列表 每个变量包括(通道编号 CID (int), 变量名称 TNAME (string)、变量类型 TYPE (string)、变量说明 COMMENT (string))	

功能	方向	功能码	详细信息	接收方响应
订阅变量	Server<-Client/Browser	FC=30 全新订阅 FC=31 增量订阅	COUNT =n(string) 订阅变量的数量 listTIB :订阅变量数组, 元素为 TAG0..n-1 。 TAG 包括 (通道编号 CID (int), 变量名称 TNAME (string)) CYCLE =abc(double) 扫描周期 (ms) ID =abc(string) 识别信息 (第一次请求时使用)	若未验证, 则进行一次验证。 若验证通过, 依据变量内容判断订阅变量是否合法, 并反馈信息。 如果成功, 则服务器建立订阅变量列表, 包括旧值的存储位置, 并依据扫描周期启动线程。
	Server->Client/Browser	FS=30 或 31	RESULT =(int) 1: 成功 2: 失败, 原因见 REASON REASON =失败原因(string)	如果订阅成功, 服务器会立即发送一次所有变量的当前值。后续仅更新变化的值。
单次更新	Server<-Client/Browser	FC=40		
	Server->Client/Browser	FS=40	COUNT =(int) 更新的数量 listTV :更新变量数组, 元素为 TAGV0..n-1 。 TAGV 包括 (通道编号 CID (int), 变量名称 TNAME (string), 变量类型 TYPE (string), 值 VALUE (string))	
周期更新	Server->Client/Browser	FS=41	COUNT =(int) 更新的数量 listTV :更新变量数组, 元素为 TAGV0..n-1 。 TAGV 包括 (通道编号 CID (int), 变量名称 TNAME (string), 变量类型 TYPE (string), 值 VALUE (string))	
其他错误	Server->Client/Browser	FS=1	RESULT =(int) 2: 失败, 原因见 REASON REASON =失败原因(string)	

注：

- 1、**黑体下划线**的为 JSON 里的 KEY。
- 2、**TYPE** 的可能值： "Bool"、 "Int16"、 "UInt16"、 "Int32"、 "UInt32"、 "Int64"、 "UInt64"、 "Float"、 "Double"、 "Word"、 "Byte"、 "String"、 "WString"
- 3、**VALUE** 的值与 **TYPE** 有密切关系， "Bool" 的 True 用“ 1” 表示， False 用“ 0” 表示。其他类型是对应类型变量的直接十进制输出。客户端要求不严格时，可以全部还原成双精度格式（可能导致 "Int64"、 "UInt64" 类型变量丢失精度）。如果需要准确还原变量的范围和精度，请用对应类型进行还原。

最后编辑：2021 年 2 月 3 日