

可编程控制器PC通讯组件使用说明

1.0 通讯组件概述

通讯组件用于PC与可编程控制器(PLC)、智能仪表等进行数据通讯,适用于基于PC高级语言的工业自动化控制系统。组件采用动态链接库文件(*.DLL)的形式,在PC系统的项目工程里引用该组件,调用相应的属性与方法函数,即可快速实现PC与PLC的高效数据交换。

DLL通讯组件无须安装,直接复制到工程文件目录,方便打包安装部署;无须任何配置,直接调用函数,与应用开发无缝衔接;多年工程经验的软件团队开发测试,经过本公司及客户的海量实际工程应用检验,稳定可靠;采用稳定高效的内部协议,无须编写PLC内部程序配合,直接访问PLC的内存,通讯响应快速;内建动态管理的多独立线程连接,同时支持外部应用的多线程结构调用;兼容WINDOWS系统下的所有开发环境,包括各种版本的VB.NET、C#、VC++,以及DEIPHI、VB、LabView等;支持几乎所有PLC的CPU自带通讯口、通讯扩展模块。

2.0 通讯组件分类

2.1 串口通讯组件 适用于RS232、RS485、RS422三种常用的串行通讯方式,一般为设备数量不多,通讯实时性要求不高的场合;

2.2 网口通讯组件 基于工业以太网,包括有线和无线通讯方式,通过交换机可实现无限拓扑,数据传输效率高。

2.3 网口透传组件 基于网络透传模块DTU(本公司有售),即PC通过网络方式,透传串口协议,将没有网络通讯功能的设备实现网络化通讯。

3.0 数据类型

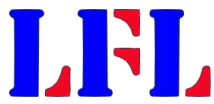
通讯组件能对PLC的输入、输出端口,以及内部中间继电器存储区域、内部数据存储区域,以及扩展存储区域进行读写操作,常用数据类型如下:

INT16:	16位有符号整数;	DINT32:	32位有符号整数;
UINT16:	16位无符号整数;	HEX32:	32位16进制字符;
BIN16:	16位二进制字符串;	REAL32:	32位单精度浮点数据;
CHAR8:	8位单个字符(ASCII);	BYTE8:	8位单字节数据;
STRING:	字符串数据(ASCII);	BOOL1:	1位布尔数据;



4.0 常用DLL组件名称对应表(更多组件库可直接咨询QQ:532011903)

序号	品牌与厂商	PLC系列及协议	接口类别	组件DLL名称
1	西门子 SIEMENS	S7-300/S7-400	以太网	WinTepS7. DLL
2		S7-1200/S7-1500	以太网	WinTepS7_1K. DLL
3		S7-200 Smart	以太网	WinTepS7_Smart. DLL
4		S7-200 CP2	以太网	WinTepS7_CP2. DLL
5		S7-300/S7-400 MPI	串口	WinS7_MPI. DLL
6		S7-200/Smart PPI	串口	WinS7_PPI. DLL
7		S7-300/S7-400	网络透传	TransS7_MPI. DLL
8		S7-200/Smart	网络透传	TransS7_PPI. DLL
9	欧姆龙 OMRON	全系列FINS-TCP协议	以太网	FinsTCP. DLL
10		全系列FINS-UDP协议	以太网	FinsUDP. DLL
11		全系列FINS-串口协议	串口	FinsCom. DLL
12		全系列HOSTLINK协议	串口	HostLink. DLL
13		全系列FINS协议	网络透传	TransFins. DLL
14	三菱 MITSUBISHI	FX系列编程口	串口	ComFxPLC. DLL
15		FX3U以太网适配器	以太网	EntFxPLC_ADP. DLL
16		FX5U系列	以太网	EntFxPLC. DLL
17		FX系列编程口	网络透传	TransFxCom. DLL
18		Q系列编程口	串口	ComQsPLC. DLL
19		Q系列MELSEC协议	以太网	EntQsPLC_ASC. DLL
20		Q系列MELSOFT协议	以太网	EntQsPLC. DLL
21		Q系列编程口透传	网络透传	TransQsCom. DLL
22	基恩士 KEYENCE	KV1000/3000/5000	串口	KvComPLC. DLL
23		KV1000/3000/5000	以太网	KvEntPLC. DLL
24		KV1000/3000	网络透传	TransKvCom. DLL
25	施耐德、台达、	全系列	以太网	ModbusTCP. DLL
26	罗克韦尔、等	全系列	网络透传	TransModRTU. DLL
27	Modbus兼容	全系列	串口	ModbusRTU. DLL



5.0 函数与参数

5.1 函数参数

[EntLink] 设置PC、PLC的通讯参数，建立与PLC的以太网连接；

参数: pcIP, String, 本地地址，即PC端的IP地址

pcPort , Uint16, 本地端口，即PC端的网络端口，默认为0；

plcIP , String , 远程地址，即PLC的IP地址

plcPort , Uint16, 远程端口，即PLC的通讯端口

Rack , Uint16, PLC的机架号码(西门子PLC参数)

Slot , Uint16, PLC的CPU的插槽号码(西门子PLC参数)

Handle, Integer , DLL组件返回网络中PLC的连接句柄，多PLC网络时通过该句柄区分操作不同的PLC，（以太网组件的输入输出型参数，即传地址方式的形式参数）

SN , String, 调用序列号码，可联系本公司获取

OverTime, Uint16, 通讯超时时间限制，毫秒单位，默认1000

返回值: Int16, 函数执行结果，见本手册5.3详细说明。

[ComLink] 设置PC、PLC的通讯参数，建立与PLC的串口连接；

参数: CommPort, Uint16, 联接PLC的PC通讯端口

CommRate, Int32, 与PLC通讯的速率

DataBit, Uint16, 通讯数据位数

StopBit, Uint16, 数据的停止位数

Parity, PrtType, 数据校验方式

Station, Uint16, PLC的站号码

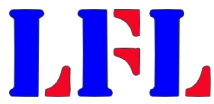
OverTime, Uint16, 通讯超时时间限制，毫秒单位

SN , String, 调用序列号码，通过联系本公司获取

返回值: Int16, 函数执行结果，见本手册5.3详细说明

[DeLink] 断开与PLC的连接，释放之前连接所用的资源；

参数: Handle, Integer , 通过EntLink函数获取的网络中PLC的句柄



返回值: Int16, 函数执行结果, 见本手册5.3详细说明

[CmdRead] 批量读取PLC的数据;

参数: Handle, Integer, 通过EntLink函数获取的网络中PLC的句柄

Memory, PlcMemory, PLC数据区域枚举, 见本手册5.2详细说明

ValType, DataType, 数据类型枚举, 见本手册5.2详细说明

Block, Uint16, DB块的号码, 非DB数据为0 (西门子PLC参数)

Address, Uint16, 要读取的存储区域起始地址

Count, Uint16, 要读取的数量, 以ValType对应的数据类型为单位

ReData(), Object/String, 读取到的数据 (传地址方式的形式参数)

返回值: Int16, 函数执行结果, 见本手册5.3详细说明

[CmdWrite] 批量写入数据到PLC;

参数: Handle, Integer, 通过EntLink函数获取的网络中PLC的句柄

Memory, PlcMemory, PLC数据区域枚举, 见本手册5.2详细说明

ValType, DataType, 数据类型枚举, 见本手册5.2详细说明

Block, Uint16, DB块的号码, 非DB数据为0 (西门子PLC参数)

Address, Uint16, 要写入的存储区域起始地址

Count, Uint16, 要写入的数量, 以ValType对应的数据类型为单位

Data(), Object/String, 要写入PLC的数据 (传地址方式的形式参数)

返回值: Int16, 函数执行结果, 见本手册5.3详细说明

[Bit_Test] 以Bit(位)的方式读取一个位的状态;

参数: Handle, Integer, 通过EntLink函数获取的网络中PLC的句柄

Memory, PlcMemory, PLC数据区域枚举, 见本手册5.2详细说明

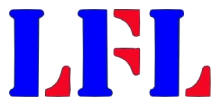
Block, Uint16, DB块的号码, 非DB数据为0 (西门子PLC参数)

Address, Uint16, 要读取的位所在的字或字节地址

Bit, Uint16, 要读取的位在Address中的位号码

State, Boolean, 读取到的位的状态 (传地址方式的形式参数)

返回值: Int16, 函数执行结果, 见本手册5.3详细说明



[Bit_Set] 以Bit(位)的方式设置其状态为ON(True);

参数: Handle, Integer , 通过EntLink函数获取的网络中PLC的句柄
Memory , PlcMemory, PLC数据区域枚举, 见本手册5.2详细说明
Block , Uint16, DB块的号码, 非DB数据为0(西门子PLC参数)
Address , Uint16, 要设置的位所在的字或字节地址
Bit, Uint16, 要设置的位在Address中的位号码
返回值: Int16, 函数执行结果, 见本手册5.3详细说明

[Bit_Reset] 以Bit(位)的方式复位其状态为OFF(False);

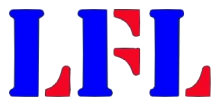
参数: Handle, Integer , 通过EntLink函数获取的网络中PLC的句柄
Memory , PlcMemory, PLC数据区域枚举, 见本手册5.2详细说明
Block , Uint16, DB块的号码, 非DB数据为0(西门子PLC参数)
Address , Uint16, 要复位的位所在的字或字节地址
Bit, Uint16, 要复位的位在Address中的位号码
返回值: Int16, 函数执行结果, 见本手册5.3详细说明

[CmdReadString] 读取PLC中的字符串;

参数: Handle, Integer , 通过EntLink函数获取的网络中PLC的句柄
Memory , PlcMemory, PLC数据区域枚举, 见本手册5.2详细说明
Block , Uint16, DB块的号码, 非DB数据为0(西门子PLC参数)
Address , Uint16, 要读取的存储区域起始地址
PlcDataSize , Uint16, PLC内定义的存放字符的最大字符数
返回值: String, 正常时为读到的字符串, 异常时为空

[CmdWriteString] 写入字符串到PLC;

参数: Handle, Integer , 通过EntLink函数获取的网络中PLC的句柄
Memory , PlcMemory, PLC数据区域枚举, 见本手册5.2详细说明
Block , Uint16, DB块的号码, 非DB数据为0(西门子PLC参数)
Address , Uint16, 要写入的存储区域起始地址
PlcDataSize , Uint16, PLC内定义的存放字符的最大字符数



Data , String, 要写入到PLC的符数, 长度应 \leq PlcDataSize

返回值: String, 正常时为读到的字符串, 异常时为空

[DataConvert] 数据类型转换函数;

参数: SourType, DataType, 数据类型枚举, 见本手册5.2详细说明

SourData , Object, 需要转换的源数据

DestType , DataType, 数据类型枚举, 见本手册5.2详细说明

DestData , Object, 转换后的目标数据 (传地址方式的形式参数)

StartByte , Int16, 目标数据从源数据取数的起始字节 (可选参数)

返回值: Int16, 函数执行结果, 见5.3详细说明。

[SetDataBit] 设置一个整形数值中的某一个位的状态, 返回设置后的数值;

参数: Data, Integer , 整形数值

Bit , Int16, 位号码, 最低位为0

SetVal , Boolean, 位的ON(True)/OFF(False)状态

返回值: Integer, 指定的位的状态改变后的数据

[GetDataBit] 获取一个整形数值中某个位的状态;

参数: Data, Integer , 整形数值

Bit , Int16, 位号码, 最低位为0

返回值: Boolean, 指定的位的ON(True)/OFF(False)状态

5.2 枚举结构体参数说明:

--PlcMemory 要操作的PLC的内存区域类型:

DI: 数字输入端口;

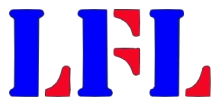
DQ: 数字输出端口;

CIO: 输入输出区域(欧姆龙);

MR: 内部中间继电器区域;

WR: 内部中间继电器W区域(欧姆龙);

DR: 内部数据寄存器D区域、DB数据块(西门子)



ER: 扩展数据E区域(欧姆龙、基恩士);

HR: 保持区域H区域(欧姆龙、Modbus)

SR: 状态寄存器S区域

AI: 模拟量输入区域

AQ: 模拟量输出区域

--DataType 读写的数据类型:

0 BOOL1: 1位布尔型数据;

1 INT16: 16位有符号整数;

2 UINT16: 16位无符号整数;

3 DINT32: 32位有符号整数;

4 HEX32: 32位16进制字符;

5 REAL32: 32位单精度浮点数据;

6 BIN16: 16位二进制字符串;

7 CHAR8: 8位单个字符(ASCII)

8 BYTE8: 8位单字节数据;

9 STRING: 多个字符或数字组成的字符串(ASCII)

--PrtType 串口通讯的校验方式

None: 无校验

Odd: 奇校验

Even: 偶检验

5.3 返回值说明:

0 执行成功;

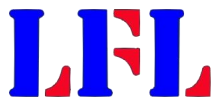
-1 IP地址或端口参数错误;

-2 网络连接错误;

-3 连接参数错误导致连接失败(如Rack>7、Slot>15等);

-4 PLC握手连接异常;

-5 PLC握手无响应;

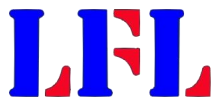


- 6 PLC握手响应错误;
- 10 读数据超过最大数据量限制;
- 11 读数据时数据发送异常;
- 12 读数据时PLC响应超时;
- 13 读数据PLC返回格式错误;
- 14 读数据PLC返回数据错误;
- 15 读数据PLC返回数据校验错误;
- 18 PLC的网络句柄解析错误;
- 19 PLC的网络句柄数据错误;
- 20 写数据超过最大数据量限制;
- 21 写数据时数据发送异常;
- 22 写数据PLC响应超时;
- 23 写数据PLC返回格式错误;
- 24 写数据PLC返回数据错误;
- 25 写数据PLC返回数据校验错误;
- 28 PLC的网络句柄解析错误;
- 29 PLC的网络句柄数据错误;
- 31 数据转换时源数据处理错误;
- 32 数据转换时目标数据处理错误;
- 41 位操作函数的参数错误;
- 70 PLC内存区域的功能受限制;
- 80 PC系统中无网卡;
- 81 PC的IP地址格式错误;
- 82 PLC的IP地址格式错误;
- 83 PING命令返回错误;
- 99 连接序列号错误或测试次数超过试用限制;

6.0 组件使用步骤

6.1 基本步骤

- a. 复制DLL、OCX文件到需要用到该组件的工程项目目录下;



- b. 注册DLL、OCX文件 (VS. NET平台的DLL程序集组件不用注册);
- c. 在项目开发环境里引用DLL文件, 不同的开发环境引用方式有区别, 具体参见所用语言的帮助文档;
- d. 参照例程定义、实例化通讯组件, 编写相关通讯代码;

6.2 DLL注册方法

VS. NET平台的DLL程序集组件不用注册, ActiveX的COM组件 (*.dll/*.ocx) 须要在系统下注册才能正常使用, 注册的方法主要有两种:

- a. 代码注册: 用Windows提供的Shell命令, Shell “regsvr32 \s ” + 组件的完整路径及文件名称;
- b. 手动注册: 同时按下 “Win” 键 + “R” 建, 在弹出的运行对话框中输入 “Regsvr32 ” + 空格 + 组件的完整路径及文件名称, 然后点 “确认” 按钮; Windows7 及以上的系统下注册, 建议对用户账户作以下设置:

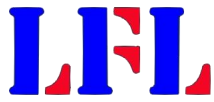
控制面板->用户账号和家庭安全->用户账户->更改用户账户控制设置, 把滑竿拖到最下面, 即 “从不通知”。

Windows7 及以上系统64位注册方法:

- a. 在C:\Windows\SysWOW64\下新建目录 (以 regdll 为例), 复制需要注册的dll到这个目录下 (以WinTcpS7.dll为例);
- b. 点击开始, 在 “搜索程序和文件” 里键入cmd, 然后在搜索出来的cmd菜单上右键, 以管理员的权限运行;
- c. 此时cmd提示符为C:\Windows\System32, 键入:
Regsvr32 C:\Windows\ SysWOW64\regdll\WinTcpS7.dll
- d. 按回车键, 然后提示注册成功 (注意此时使用的是syswow64目录下的regsvr32.exe, 而不是system32下的regsvr32.exe)。

6.3 开发注意事项

- a. 函数调用顺序: EntLink/ComLink → 相关功能函数→DeLink。
- b. 任何函数返回值为负数时: DeLink→ 延时 (500ms左右) → EntLink/ComLink。
- c. 本说明文档为所有DLL通讯组件的公共版文档, 不同PLC的程序集函数名称相同, 参数结构相似, 具体函数以函数接口文档和范例为准。



7.0 技术支持

本公司提供的通讯组件DLL程序集、OPC Server开发包SDK程序集等方便同行的资源都是在公司项目上多次成功应用过的，稳定性、可靠性以及开发的方便性都已经得到充分的验证。

本公司提供各类工业自动化软件定制开发服务，包括生产执行系统、物料系统，以及自动化设备与生产线监控、数据采集项目等，欢迎交流咨询。

E-Mail: liuflamp@126.com

QQ: 5320 11903

TEL: 159 7219 9489

微信: lflzdh

上海埃菲尔自动化系统有限公司

<http://www.aihe-tech.com>