# S7IsoTcp驱动协议

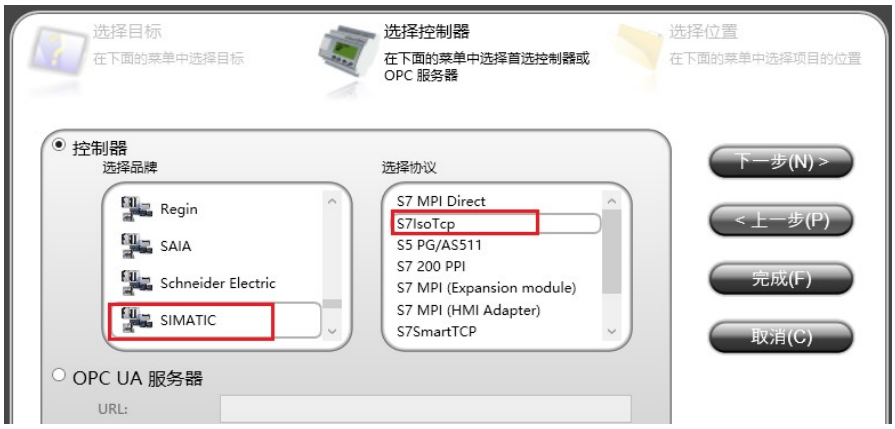
## 概述

本章节用于介绍如何和西门子SIMATIC S7控制器通过TCP/IP进行通信。控制器中项目程序的寻址方式采用常规SIMATIC方式（即绝对地址），不支持标签变量地址。

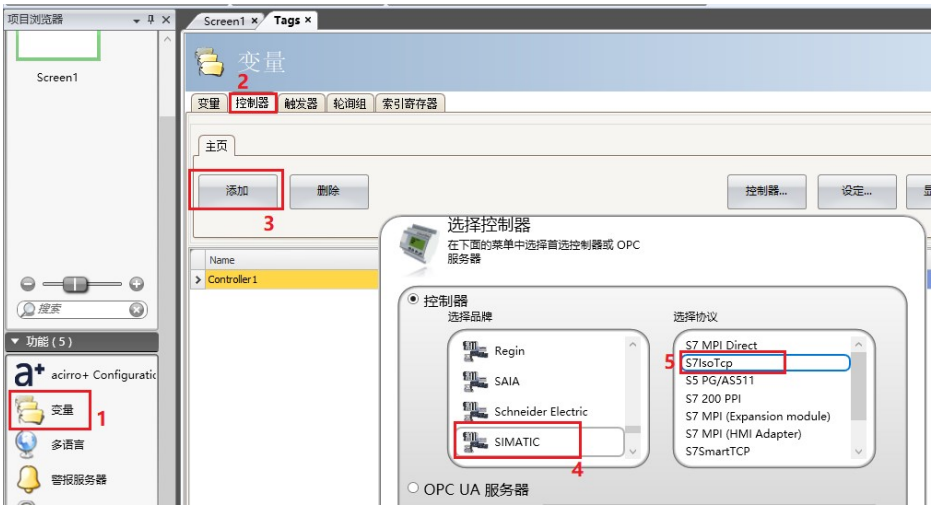
本驱动协议支持SIMATIC S7 200、300、400、1200和1500系列控制器。

## 控制器协议选择

创建新项目程序时，在“选择控制器”窗口选择“SIMATIC – S7IsoTcp”协议。



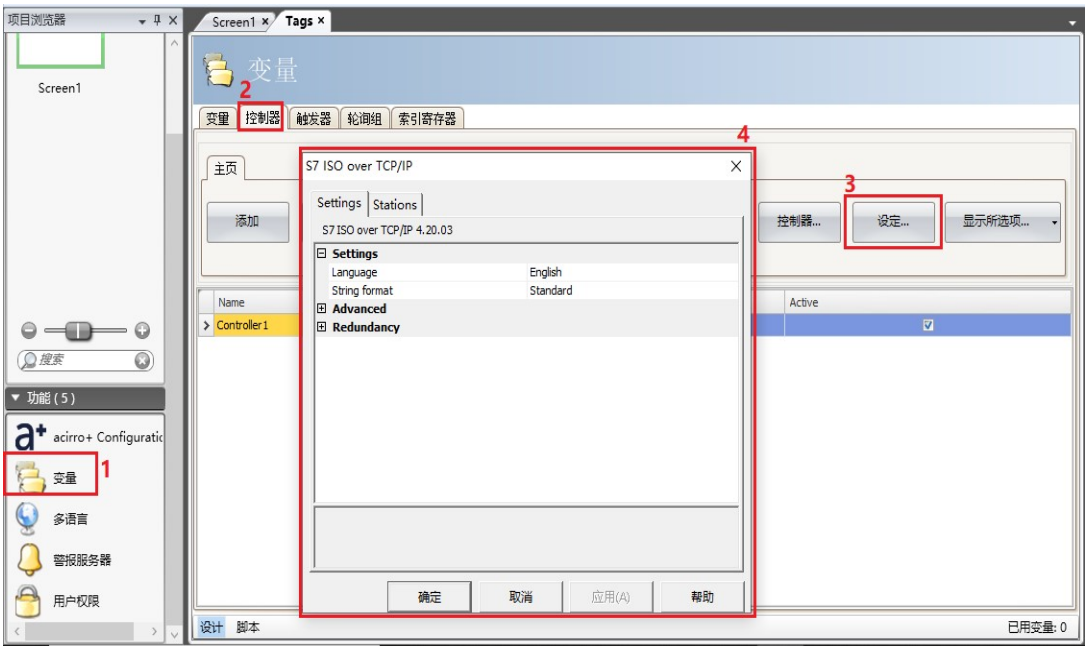

若在编辑项目程序过程需添加该驱动协议，则在iX Developer软件左侧的功能区“变量”设定对话框的“控制器”标签页中点击“添加”按钮进行添加。



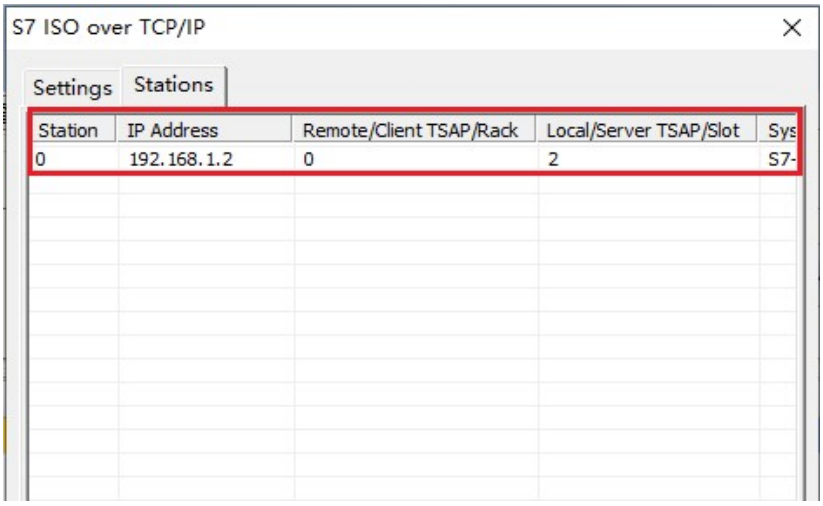
## 控制器通讯设定

在iX Developer软件左侧的功能区“变量”设定对话框的“控制器”标签页中点击“设定”按钮，在弹出的属性对话框中进行通讯参数设定。

在“设定”对话框中，有“Settings”和”Stations”2个设定标签页。

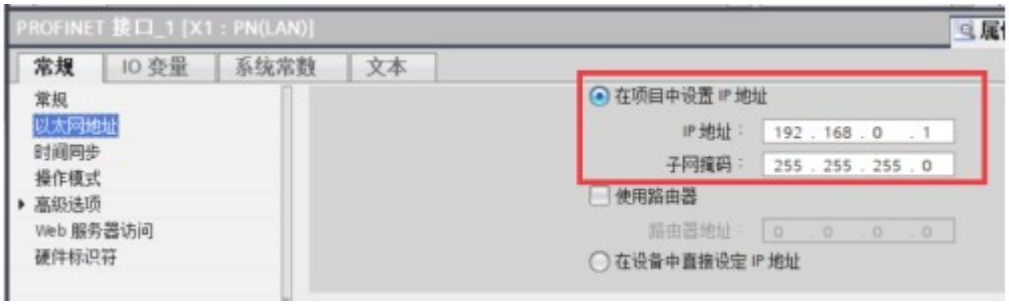



在“Stations”设定标签页中进行设定，在“IP address”处输入控制器的IP地址，“Local/Sever TSAP/Slot”处设定槽号，当和S7-1200/1500系列控制器通讯时，将Local/Sever TSAP/Slot”设定为“1”（默认是2，适用于S7-300/400）。

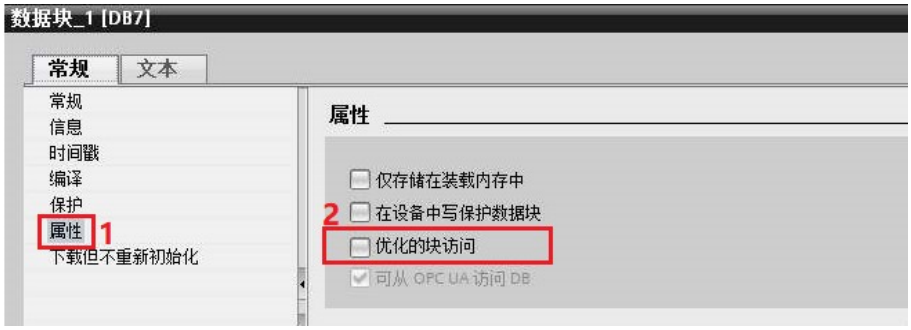


当和S7-1200/1500系列PLC通讯时，PLC博图软件侧设定需注意以下几点：

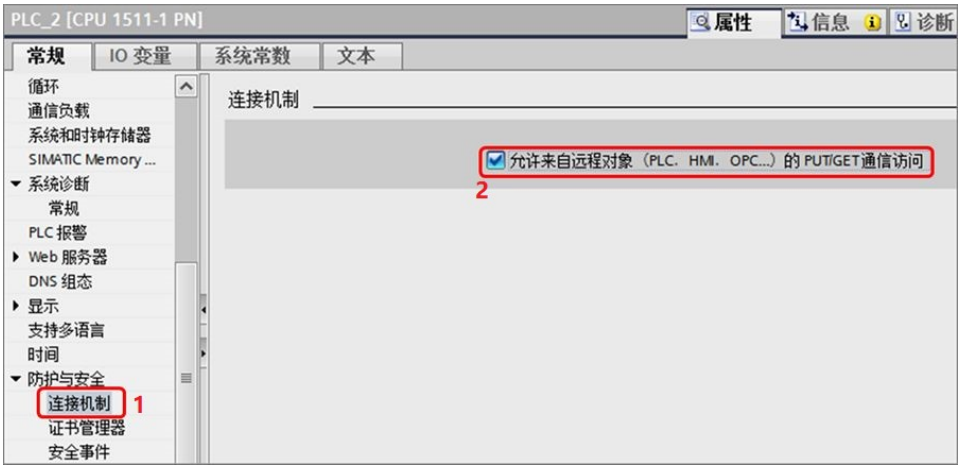
1. 在CPU处，右键选择【属性】→【常规】→【PROFINET接口】→【以太网地址】处设定PLC的IP地址。




2. 在程序中所使用的DB块处，右键选择【属性】→【属性】，然后取消勾选【优化的块访问】。




3. 在CPU属性处，【常规】→【保护】→【连接机制】处，勾选【允许从远程伙伴（PLC、HMI、OPC...）使用PUT/GET通信访问】。



**设定项说明**

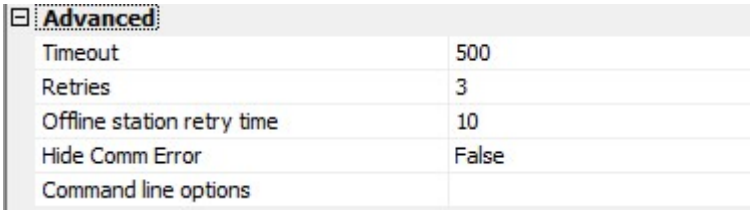
## 1. Settings设定标签页

### a. Settings




| 设定项 | 说明 |
|---|---|
| Language | 设定控制器数据类型寻址语言，共有2个选项：English和German。默认为English。 |
| String Format | 选择从控制器读/写字符串时要使用的字符串格式，可设定为“Standard”或“Siemens”格式。 |

### b. Advanced




| 参数项 | 说明 |
|---|---|
| Timeout | 通讯连接超时时间（ms）。 |
| Retries | 检测到通信错误之前的尝试重连次数。 |
| Offline station retry time | 发生通信错误后到尝试恢复通信的等待时间，单位：秒（s）。 |
| Hide Comm Error | 当通讯连接失败时，显示/隐藏通讯错误信息。 |
| Command line options | 设定传递给驱动程序的特殊命令。<br>有关此驱动程序的可用命令，请查阅命令相关章节。注意：命令章节内容并不适用于所有驱动。 |

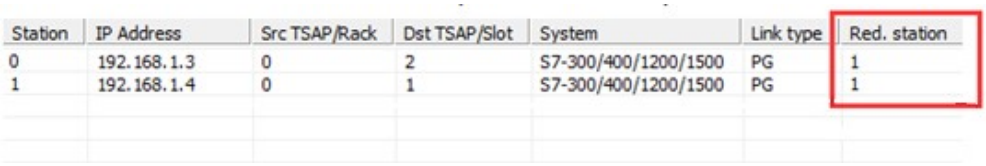
### c. Redundancy

在 S7IsoTcp协议的V4.15.06版本及以上增加了冗余功能。




| 参数项 | 说明 |
|---|---|
| Enable redundancy | 设定为True时，则开启冗余功能。 |
| Automatic redundant recovery | 设定为True时，当在使用冗余控制器时，驱动程序会去尝试与主控制器自动重连；否则可通过为变量定义“设备号:REDUNDANT_RESET”来用于手动触发重连动作； |
| Redundant recovery time | 当“Automatic redundant recovery“设定为True时，此处设定每次尝试与主控制器自动重连的时间间隔，单位为：秒。 |

当“Enable redundancy”设定为True时，在“Stations”标签页中可设定“Red.Station”冗余站号。

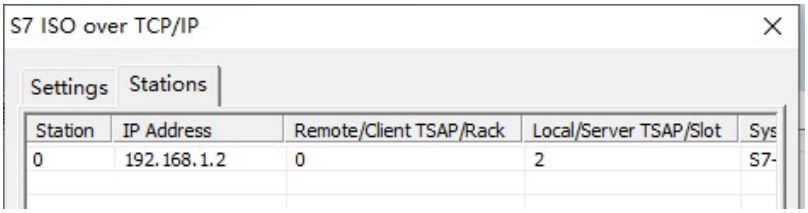


| Station | IP Address | Src TSAP/Rack | Dst TSAP/Slot | System | Link type | Red. station |
|---|---|---|---|---|---|---|
| 0 | 192.168.1.3 | 0 | 2 | S7-300/400/1200/1500 | PG | 1 |
| 1 | 192.168.1.4 | 0 | 1 | S7-300/400/1200/1500 | PG | 1 |

为各个不同IP的控制器站定义冗余站号，例如站号0为主站，站号1为冗余站，则站号0设定冗余站号为1，站号1设定冗余站号为1；运行中当站号0出现通信异常时，自动切换为与站号1通信。

### 2. Stations设定标签页

在“Stations”设定标签页中设定连接的控制器的站号、IP地址、机架号、槽号等想相关设定项。



最多可配置20个站。每个站都需设定IP地址、机架号、槽号、系统型号等设定项。
须注意：站号0为默认站号，必须设定。

| 参数项 | 说明 |
| --- | --- |
| Station | 设定站号 |
| IP Address | 设定外接控制器的IP地址 |
| Remote/Client TSAP/Rack | 设定外接控制器的机架号 |
| Local/Server TSAP/Slot | 设定外接控制器的槽号。当和S7-1200/1500系列控制器通讯时，须设定为“1”。 |
| System | 选择控制器系统，共2个选项：<br>当和带有CP243模块的S7-200建立通讯时，选择“S7-200”选项；<br>当和S7-300、400、1200或1500建立通信时，选择“S7-300/400/1200/1500”选项。 |
| Link type | 选则使用的连接的链路类型，共2个选项：<br>当控制器为S7-200时，按默认设定为PG即可；<br>当控制器为S7-300/400/1200/1500时，根据控制器端进行选择 PG（编程设备）还是OP（操作面板）。 |
| Red.station | 设定冗余控制器站号，只有当开启冗余功能时，才会再设定窗口显示并可进行设定。 |

注意：S7-200和S7-300/400/1200/1500系统的参数不同。请参见不同系统的说明。此外，S7-200参数以十六进制输入，S7-300/400/1200/1500参数以十进制格式输入。

**通讯电缆图**

若操作面板和外接控制器间通过HUB进行连接时，使用标准常规网线即可；若将操作面板直接连接到外接控制器时，必须使用5类或更高类的交叉网线。

**支持的寄存器**

支持的寄存器地址范围如下表所示。

| 寄存器 | 数据类型（德语） | 数据类型（英语） |
|---|---|---|
| 中间变量 | M | M |
| 输入变量 | E | I |
| 输出变量 | A | Q |
| 数据块 *1 | DB | DB |
| 定时器（只读） | T | T |
| 计数器（只读） | Z | C |
| 可变存储器 *2 | V | V |

*1 – 只有S7-300/400/1200/1500支持；*2 – 只有S7-200支持。

项目内存决定了SIMATIC S7中数据块（DB）的最大长度。HMI可以访问控制器中的所有数据DB块。

注意：如果试图访问未定义的数据块，控制器将停止通讯，显示报错信息。

所有数据类型都由字节区域组成。寻址总是以字节进行定义的，不管它是1位、16位还是32位。地址是十进制的，0~65535。

有关SIMATIC S7的说明信息，请参阅相应的控制器手册。

**数字量信号**

可以用字节的某个位来表示某个位地址。例如，I50.3表示输入字节50中的第3位。

| 数据类型（德语） | 数据类型（英语） |
|---|---|
| Exxxx.b | Ixxxx.b |
| Axxxx.b | Qxxxx.b |
| Mxxxx.b | Mxxxx.b |
| DBno.DBXyyyy.b | DBno.DBXyyyy.b |
| VXyyyy.b | VXyyyy.b |

yyyy= 0~8191

no = 数据DB块号

xxxx = 地址（最小值为0，最大值取决于控制器端）

b = 位地址，范围0~7

将数据类型E/I、A/Q和DB的位从HMI端写入控制器分三步完成：

1. 从控制器端向HMI端读取整个字节；
2. 在HMI端置位/复位当前位；

3. 将整个字节从HMI端写入到控制器端。

须注意：在HMI执行这三个步骤所需的时间内，控制器侧不能再更改当前字节中的其他位，因为该字节将被覆盖。

**模拟量信号**

关于字节，须在数据类型后加上后缀B。

| 数据类型（德语） | 数据类型（英语） |
|---|---|
| EBxxxx | IBxxxx |
| ABxxxx | QBxxxx |
| MBxxxx | MBxxxx |
| DBno.DBBadr | DBno.DBBadr |
| VBxxxx | VBxxxx |

xxxx = 地址（最小值为0，最大值取决于控制器端）
no = 数据DB块号
adr = 数据DB块内的字节地址

对于16位地址，须在数据类型后加上后缀W；例如，MW100表示内存字节100-101中的2个字节。

| 数据类型（德语） | 数据类型（英语） |
|---|---|
| EWxxxx | IWxxxx |
| AWxxxx | QWxxxx |
| MWxxxx | MWxxxx |
| DBno.DBWadr | DBno.DBWadr |
| Txxxx(只读) | Txxxx(只读) |
| Zxxxx(只读) | Cxxxx(只读) |
| VWxxxx | VWxxxx |

xxxx = 地址（最小值为0，最大值取决于控制器端）
no = 数据DB块号
adr = 数据DB块内的字节地址

对于32位数字，须在数据类型后加上后缀D；例如，MD100表示内存字节100-103中的4个字节。

| 数据类型（德语） | 数据类型（英语） |
|---|---|
| EDxxxx | IDxxxx |
| ADxxxx | QDxxxx |
| MDxxxx | MDxxxx |
| DBno.DBDadr | DBno.DBDadr |
| VDxxxx | VDxxxx |

xxxx = 地址（最小值为0，最大值取决于控制器端）
no = 数据DB块号
adr = 数据DB块内的字节地址

**数据块索引**

DB块中的地址可以使用索引来寻址，由当前索引寄存器的值来决定从哪个数据块的相应变量地址读/写数据。

例如：DB4I2.DBW10表示（4+I2索引寄存器的值）的DB数据块中DBW10这个地址。

**字符串格式**

本驱动协议支持两种不同的字符串格式：标准格式或西门子格式。“标准格式”将字符串的第一个字符存储在第一个字节中，第二个字符存储在第二个字节中等。而“Siemens格式”的最大字符串长度以字节0为单位，实际字符串长度以字节1为单位，字符串本身从字节2及以上开始。当使用“西门子格式”时，用户将看不到前两个字节，但可以通过直接寻址字节来访问它们。

注意：使用Siemens格式时，字符串长度扩展为字符串本身长度字节+两个字节。这意味着长度为10的字符串实际上将在控制器中读/写12个字节的数据。

**时间地址**

本驱动协议支持西门子时间格式。这些值作为32位变量地址读/写到控制器，但在HMI中以字符串形式显示，完整TOD字符串的语法为hh:mm:ss.mss，其中hh是小时，mm是分钟，ss是秒，mss是毫秒。小时、分钟和秒用两个字符表示，毫秒用三个字符表示。

要读/写TOD数据，必须在项目程序中添加字符串标签变量，地址必须以“TOD:”开头。该标签变量地址在PLC侧一定是一个32位地址。该字符串标签变量的长度取决于要读/写的TOD参数的数量。

例如：

以时间变量DB1.DBD4为例，当该TOD参数都需被读取时，则在HMI的项目程序中需添加“TOD:DB1.DBD4”这个变量地址，数据类型设定为“String”，字符串长度设定为12。如果十进制值45000500存储在变量地址中，则在HMI中将显示为字符串“12:30:00.500”。

以时间变量MD0为例，当该TOD参数中的“小时”和“分钟”需被读取时，则在HMI的项目程序中需添加“TOD:M0”这个变量地址，数据类型设定为“String”，字符串长度设定为5。如果十进制值66000000存储在变量地址中，则在HMI中将显示为字符串“18:20”。

以站号2的控制器的时间变量MD0为例，当仅读取该TOD参数的“小时”时，则在HMI的项目程序中需添加“2:TOD:M0”这个变量地址，数据类型设定为“String”，字符串长度设定为2。如果十进制值57600000存储在变量地址中，则在HMI中将显示为字符串“16”。

如果要将一天中的新时间值写入时间变量地址中，即可以以标准的TOD格式写入，也可以是写入hh、hh.mm、hh.mm.ss。

例如：

写入新的时间值以TOD标准格式时间：字符串输入为“12:30:45.500”。

只写入新的时间值“小时”和“分钟”：字符串输入为“15:20”。秒和毫秒由驱动程序自动填入0。

只写入新的时间值“小时”：字符串输入为“20”。其他参数由驱动程序自动填入0。

**站号管理**

对于与默认站号以外的其他站号的控制器进行通信时，站号作为标签变量的前缀。

例如：

2:MW8 表示为站号2的控制器的MW8这个地址。

5:DB1.DBW12 表示为站号5的控制器的DB1.DBW12这个地址。

08:03:10001 - 站号是8节点号为3的外接控制器的开关量输入地址10001。

**索引站号**

控制器站号可以进行索引，使用索引寄存器，以索引寄存器的值决定从哪个站读/写相关变量地址。

语法：索引寄存器：标签变量，如：I2:MW8。

索引寄存器范围为I0~I5。当索引寄存器的值无法找到对应的站号时，则会显示相关错误消

息。

**冗余变量**

当使用冗余功能时，有两个内部标签变量可用，分别是“REDUNDANT_RESET”和“STATION_CONNECTED”。

当“自动冗余恢复”设定为“禁用”时，可以使用“REDUNDANT_RESET”进行重置。当断开一个站点并激活冗余站点时，可以通过将冗余重置标签设置为1来尝试重新连接。该标签变量的值默认为0。

“STATION_CONNECTED”用于监视当前工作站是否已连接（标签值为1）或冗余工作站是否激活（该值设置为0）。

须注意：此标签变量仅在有指向站点的活动标记时更新。

这两个冗余标签变量都可以作为普通控制器标签进行站点寻址。

例如：

1:REDUNDANT_RESET　用于对站号为1的控制器进行重连。

4:STATION_CONNECTED　用于查看站号为4的控制器是否连接。

I2:REDUNDANT_RESET　用于对站号为I2索引寄存器的值的控制器进行重连。

**通信效率优化**

当信号在HMI端驱动和控制器之间进行传输时，所有信号不会同时传输。相反，它们会被分成包，每个包中有许多信号。通过减少必须传输的包的数量，可以提高通信速度。每个包中的信号数取决于所使用的驱动程序。

在“SIMATIC - S7IsoTcp”驱动协议中，不同的数据类型地址可以混合在一个包中，但位信号只能与其他位一起读取。

一个包中可以打包多少个读请求（称为任何指针）取决于所用的控制器。数组和字符串（数字表、图表和字符串对象）会以单独的包进行发送。

**错误消息**

外接控制器和操作面板间的通讯错误消息在操作面板上显示如下：

| 错误信息 | 描述 |
| --- | --- |
| Comm Err Stn X | 通讯错误，检查通讯设置、电缆连接和外接控制器的站号等。 |

| | |
|---|---|
| Comm error Y stn X | 和站号为X的外接控制器的通讯错误代码Y。(Y是控制器侧反馈的错误代码。) |
| comm error 240 stn X | 通讯错误，须在PLC软件侧勾选“允许从远程伙伴（PLC、HMI、OPC…）使用PUT/GET通信访问”。 |
| Bad device stn X | 使用控制的变量的数据类型错误，须检查在HMI侧用的控制器变量的数据类型是否和PLC侧定义的数据类型一致。 |
| comm error -32508 stn X | 通讯错误，检查通讯设置等，同时PLC侧对PLC程序进行（硬件+软件）完整编译后再下载。 |