S7-PN/ModbusTCP 协议转换器

用户手册

版本：V2.01
发布日期：11/2020
大连德嘉工控设备有限公司

目录

S7-PN/ModbusTCP 协议转换器

Apply to Honeywell FTE(Fault Tolerant Ethernet)、Emerson OHI(Ovation Highway Interface)、Network Isloation

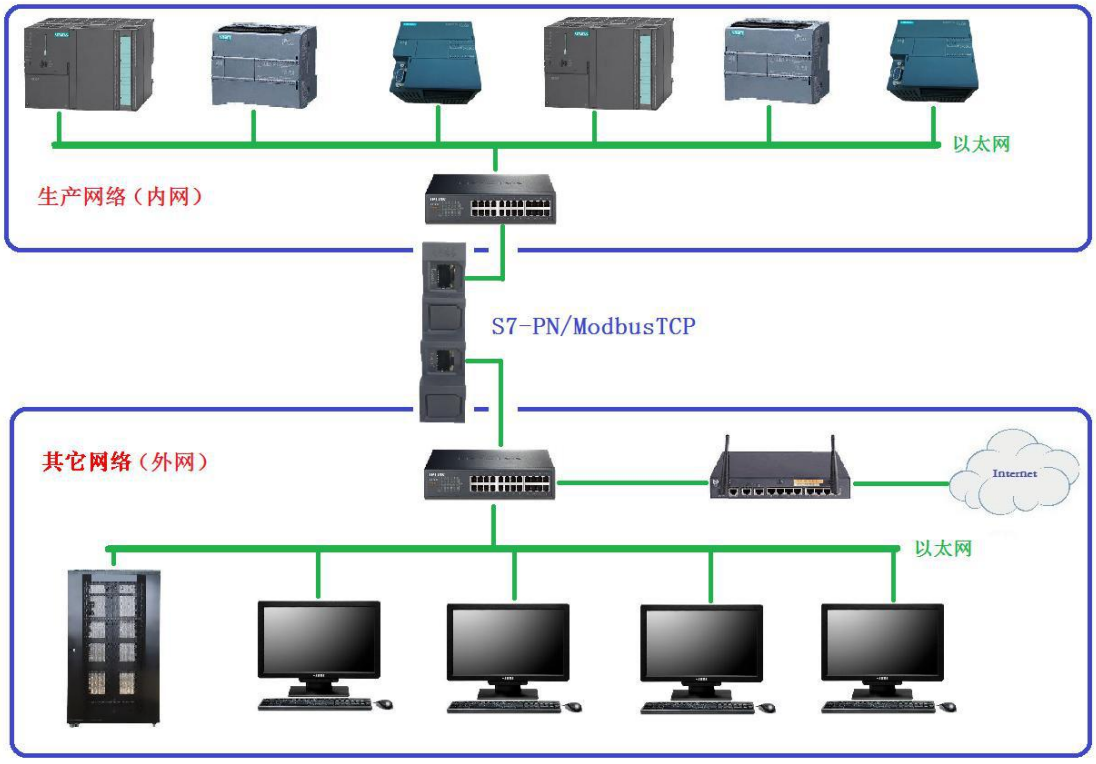
1 产品概述

S7-PN/ModbusTCP 协议转换器，它能将西门子 S7-300、S7-1200、S7-1500、S7-200 Smart、S7-200 CP243 等产品转换成 Modbus TCP 协议(服务端) 为电脑或其它系统提供 Modbus TCP 协议，通过网线读写西门子 PLC 中 DB 块(或是 V 区)数据，以及 Q 区、I 区状态值。

【网络隔离型】：西门子 PLC 与其它系统（ModbusTCP 侧）分处于两个独立的网络中，而该 S7-PN/ModbusTCP 转换器跨接这两个网络，是中间的网关，它具有隔离 PLC 与其它网络的功能，使 PLC 的网络与 ModbusTCP 侧的网络可运行在不同网段中，实现两个网络的彻底隔离，彼此独立。

PLC 是重要的生产控制设备，它的网络是不能随意与 DCS、MIS、或办公网络等其它系统网络直接相连的，这就需要该 S7-PN/ModbusTCP 做为网关隔离，将内网与外网实现硬件分割，同时能够进行数据安全交换，实现网络安全防护，不给工业病毒、互联网远程恶意攻击留有任何可乘之机。

同时也彻底切断网络攻击病毒在不同网络中的蔓延，另外网关型 S7-PN/ModbusTCP 转换器还具有连接霍尼韦尔的 FTE （Fault Tolerant Ethernet）、艾默生的 OHI(Ovation Highway Interface)的特殊网络功能。



Modbus TCP 功能码与西门子 PLC 数据的对应关系：

01 功能码：读取线圈、05 写单个线圈、15 写多个线圈(0xxxx)
　　地址［0, 1, 2, ..10 … ］对应西门子 PLC Q 区: [Q0.0, Q0.1, Q0.2, .. Q1.2….]
02 功能码：读取输入状态(1xxxx)
　　地址［0, 1, 2, ..10… ］对应西门子 PLC I 区: [I0.0, I0.1, I0.2, ..I1.2…..]
04 功能码：功能取消
03 功能码：读取保持寄存器、06 写单个寄存器、16 写多个寄存器(4xxxx)
　　地址［0, 1, 2, ..10… ］对应: DB 块中的 DBW0, DBW2, DBW4, ...DBW20….
或 V 区的 VW0, VW2, VW4, ... VW20…

注：如果对应的数据地址超出 DB 块的实际长度，将会出现全部或部分 DB 块数据不能被读写，例如：DB1 的长度为 100 字节，用 03 功能码读取，起始地址为 0，长度为 52，
这就是要读取 DB1 从 0 开始的 104 个字节，它超过了实际 DB1 块数据长度，就会出现读数据失败，并不是超出地址的数据读不到，而是整个 DB 块的数据都读不到！切记！
支持最大通讯数据为 1024 个字节。

产品外观：(网络隔离型)

2 参数设置

下边重点介绍网关型 S7-PN/ModbusTCP 转换器：

它有两个网口（LAN1 和 LAN3）。LAN1 用于连接西门子 PLC；LAN3 用于连接电脑或 DCS、MIS、霍尼韦尔的 FTE、艾默生的 OHI 等具有 Modbus TCP 协议的其它系统。

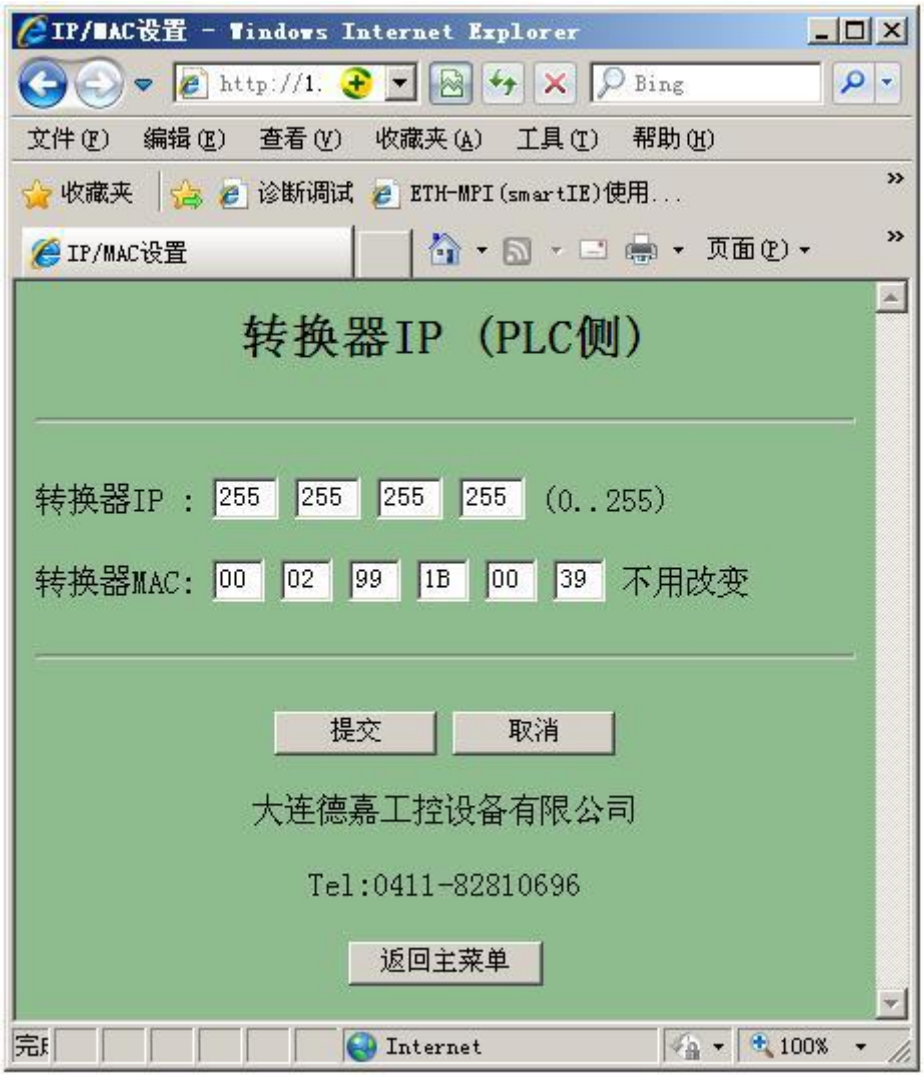
请注意这两个网口都要分别设置（出于安全考虑）

一、连接西门子 PLC 侧的网口（LAN1）设置：

1、首先用电脑通过网线连接 LAN1 的网口（或经过交换机与 LAN1 连接），如果不知道转换器的实际 IP 地址（或忘记了），你可以使用后门 IP 地址（192.168.1.222）来进入转换器设置页面，但该地址并不是真实地址，只能用来查看或修改实际 IP。

电脑本地网卡的 IP 地址请不要使用自动获取方式，而是将 IPV4 设成固定 IP 地址：如 192.168.1.100，如果是笔记本电脑请将无线网卡禁用（通过软件选择）；然后打开电脑中的微软 IE 浏览器（请不要使用其他公司的浏览器，比如 360、谷歌、搜狗等），在地址栏中直接键入 192.168.1.222（当然也可以使用它实际的 IP 地址，如 192.168.1.10），之后你就进入了 S7-PN/ModbusTCP 转换器（PLC 侧）的设置页面主菜单，如下图：

2、转换器的 IP 地址（PLC 侧）要与西门子 PLC 的 IP 地址处于同一段址中，即 IP 地址的前 3 段完全一样，第 4 段不一样（切记！千万不能一样），用鼠标点击“转换器 IP (PLC 侧)”，就进入了下面的 IP 设置页面，只需修改 IP，而 MAC 则无需改变。



3、再次回到主菜单，用鼠标点击“PLC 类型/块号及 IP”，就进入了 DB 块设置页面：

在该设置页面中选择所连的 PLC 的 IP 地址以及 PLC 类型，如果是 S7-300\1200\1500,还要填写用于通讯的 DB 块号，而 S7-200 或 smart 使用 V 区，DB 块号填‘1’

4、 再次回到主菜单，用鼠标点击“读写 PLC 速度/禁写”，就进入了速度设置页面：

该页面用于控制读写 PLC 速度(准确说是频率)及写保护，如果通讯数据量小，请选[100MS]；如果不对 PLC 进行写操作，请选 【全面禁止 Q 区、DB 区写入】

5、 如果想查看本产品的通讯状态，请回到主菜单，用鼠标点击“通讯检测故障诊断”，见下图：

二、连接 Modbus TCP 侧（如电脑或 DCS、MIS、霍尼韦尔的 FTE、艾默生的 OHI 等具有 Modbus TCP 协议的其它系统）的网口（LAN3）设置：

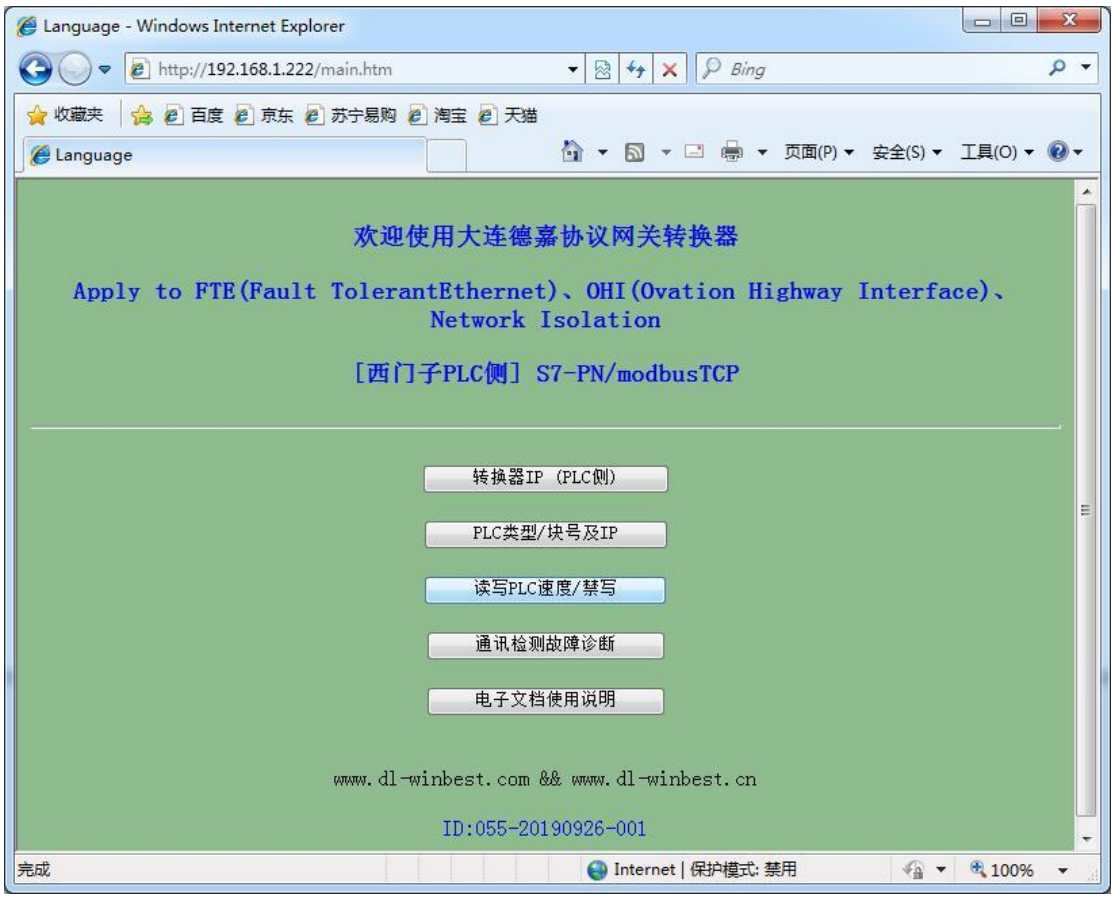
首先用电脑通过网线连接 LAN3 的网口（或经过交换机与 LAN3 连接），如果不知道转换器的实际 IP 地址（或忘记了），你可以使用后门 IP 地址（192.168.1.222）来进入转换器设置页面，但该地址并不是真实地址，只能用来查看或修改实际 IP。

电脑本地网卡的 IP 地址请不要使用自动获取方式，而是将 IPV4 设成固定 IP 地址：如 192.168.1.100，如果是笔记本电脑请将无线网卡禁用（通过软件选择）；然后打开电脑中的微软 IE 浏览器（请不要使用其他公司的浏览器，比如 360、谷歌、搜狗等），在地址栏中直接键入 192.168.1.222（当然你也可以使用它实际的 IP 地址，如 192.168.1.10），之后就进入了 S7-PN/ModbusTCP 转换器（ModbusTCP 侧）的设置页面主菜单，如下图：

转换器的 IP 地址（ModbusTCP 侧）要与电脑或 DCS、MIS、霍尼韦尔的 FTE、艾默生的 OHI 等具有 Modbus TCP 协议的设备 IP 地址处于同一段址中，既 IP 地址的前 3 段完全一样，第 4 段不一样（切记！千万不能一样），用鼠标点击“FTE/OHI/DCS 侧 IP 地址设置”，就进入了下面的 IP 设置页面：

3 实例演示

1、首先用电脑通过网线连接 LAN1 的网口（或经过交换机与 LAN1 连接），如果不知道转换器的实际 IP 地址（或忘记了），你可以使用后门 IP 地址（192.168.1.222）来进入转换器设置页面，但该地址并不是真实地址，只能用来查看或修改实际 IP。



2、转换器的 IP 地址（PLC 侧）要与西门子 PLC 的 IP 地址处于同一段址中，如：192.168.1.10，这里使用的是 CPU315-2 PN/DP，其 IP 地址为 192.168.1.30。

3、再次回到主菜单，用鼠标点击“PLC 类型/块号及 IP”，就进入了 DB 块设置页面，填入实际 S7-300PLC 的 IP 地址：192.168.1.30，DB 块号填入 00011，代表 DB11

4、如果想查看本产品的通讯状态，请回到主菜单，用鼠标点击“通讯检测故障诊断”

5、连接 Modbus TCP 侧设置，用电脑通过网线连接 LAN3 的网口（或经过交换机与 LAN3 连接），如果不知道转换器的实际 IP 地址（或忘记了），你可以使用后门 IP 地址（192.168.1.222）来进入转换器设置页面，但该地址并不是真实地址，只能用来查看或修改实际 IP。

6、转换器的 IP 地址（ModbusTCP 侧）设置，如：192.168.1.20（当然可以使用其他网段）

7、使用 Modbus Poll 调试软件测试如下，连接时，IP 填：192.168.1.20，端口号：502，选择 03 功能码（4xxxx），Modbus 寄存器地址从 0 开始读 10 个，可见通讯成功。