# SIEMENS华南区广东惠州市西门子(授权)一级总代理

| | |
|---|---|
| 产品名称 | SIEMENS华南区广东惠州市西门子(授权)一级总代理 |
| 公司名称 | 广东湘恒智能科技有限公司 |
| 价格 | .00/件 |
| 规格参数 | 西门子变频器:西门子触摸屏<br>西门子伺服电机:西门子PLC<br>西门子直流调速器:西门子电缆 |
| 公司地址 | 惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房 |
| 联系电话 | 18475208684 18475208684 |

# 产品详情

01.工控安全研究

按照普渡模型搭建研究环境，分别以S7300和S71500PLC为研究对象 ,通过PC01安装的TIA V16和 STEP7 V5.6软件、操作站安装力控软件与PLC进行通信，通过PLC编程软件进行工程组态下载，启停控制操作，上位机进行数据读取写入操作来搭建通讯协议研究环境。需要注意：S71500和上位机需要设置允许连接的保护功能，方能正常通讯。

STEP 7是PLC组态软件，具有以下功能：硬件配置和参数设置、通讯组态、编程、测试、启动和维护、文件建档、运行和诊断功能等。通过新建项目向导
选择对应的CPU型号，本例为CPU315-2PN/DP,根据提示完成项目建立。在硬件组态页面 编辑好CPU的IP地址，完成软件和硬件工程组态。配置好PC/PG接口后，将PLC与PC直连后即可将程序下装到PLC中。

3、TIA Portal编程博途将所有自动化软件工具集成在统一的开发环境中，它是shijiedi一款将所有自动化任务整合在一个工程设计环境下的软件。目前更新到V18,产品更新换代很快，对操作系统和硬件性能要求较高。

4、S7协议通过wireshark 截包分析可知，通讯过程中一共解析出两种协议，S7 comm 和 s7 comm plus。s7 300 和 Step 7 或上位机之间为 S7 comm，S71500 和 TIA V16 之间为s7 comm plus，S71500和上位机通讯协议为 S7 comm。

s7comm是西门子工业自动化控制系统使用的协议之一。它是一种基于ISO-on-TCP协议的实时以太网通信协议。s7comm协议的设计目的是在西门子控制器之间传输数据（读/写数据或以各种方式进行诊断）。

s7comm plus协议是一种扩展版的s7comm协议,它支持更gaoji的功能和更好的性能。s7comm plus协议使用COTP协议进行身份验证，并使用加密算法进行密钥交换。经过实际验证，目前绝大数国产触摸屏软件和上位机软件支持S7 Comm协议对西门子PLC的数据访问，而S7 Comm plus目前仍局限于西门子高版本固件的设备间的通讯访问。

02.

六方云工控实验室专家认为，S7协议虽然作为一种私有非公开的协议，但是由于西门子广泛应有领域使其工业现场最为常用实时数据传输协议，虽然S7 comm plus协议推出升级了S7协议，安全性得以提高，但是前述研究，S7 comm plus 应用范围较小。目前S7 Comm 协议仍然是安全防护的重点。攻击者可以通过简单的身份鉴别攻击，结合钓鱼网站、挂马网站等攻击形式，进一步滥用此漏洞，这可能会导致工业控制网络连接变得不再安全，并造成重要数据的泄露。

图为六方云工控防火墙对S7协议的防护界面，支持对S7协议功能码的深度防护，尤其是值域控制，敏感操作，上传，下载，启停等重点功能码。针对此类威胁，建议采用专业的工控防火墙系统进行防护。六方云工控防火墙能够智能识别和防护各种恶意攻击，提供黑、白名单策略相结合的防护机制以及深度解析工控协议功能，来有效地防止已知和未知的恶意攻击行为，从而极大地降低了工控系统面临的安全风险。除此之外，还可以增强身份验证和访问控制等安全措施，如使用强密码、多因素认证等方式来保障系统的安全性。同时在设计、部署和维护工控系统时，需要遵循相关行业标准和实践需求，以确保系统的安全性和可靠性。