宁夏回族自治区西门子授权供应商---西门子变频器银川市总代理

产品名称	宁夏回族自治区西门子授权供应商---西门子变频器银川市总代理
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PLC:西门子伺服电机 西门子触摸屏:西门子电缆 西门子变频器:西门子模块
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（仅限办公）
联系电话	13510737515 13185520415

产品详情

网络分段和单元保护可归纳如下：

单元 ”和“ 区域 ”的概念是出于安全的目的对网络进行分段隔离

通过设置信息安全网络组件，对“ 单元入口 ”进行访问控制

将没有独立访问保护机制的设备置于安全单元内加以保护，这种方式主要针对已经正常运行设备的改造

划分各个单元可以防止由于带宽限制造成的网络过载，保护单元内部的数据通信不受干扰

在各个单元内部不影响实时通信

在网络单元内部，对功能安全设备提供保护

在单元和单元之间通过建立安全通道实现安全通信

网络分段的单元防护理念是防止未经授权访问的一种防护措施。在安全单元内部的数据不受信息安全设备的控制，因此我们假设各分段网络内部是安全的，或者在各个单元内部部署了更进一步的安全措施，例如，保证交换机的端口安全。

各个安全单元的大小的划分主要取决于被保护对象所包含的内容，具有相同需求的组件可能会划分在一个安全单元以内。建议根据生产流程规划网络结构。这样可以保证网络分段时，各个网络单元之间通信数据量最少，同时，可以使防火墙配置的例外规则最小化。

为了保证性能需求，建议客户遵循如下针对网络规模和网络分段的规则：

一个 PROFINET IO 系统中的所有设备规划到一个网络单元中

设备和设备之间的通信数据量非常大的情况下，应该将它们规划到一个网络单元中

如果一台设备仅仅和一个网络单元之间存在数据通信，同时保护目标是一致的，则应该将该设备和网络单元合并到一个网络单元

3、远程访问的安全

越来越多的工厂通过互联网被直接地连接到了一起。由于远程服务、远程应用和监控安装在世界各地的机械设备的需求，远程的工厂通过移动网络(GPRS，UMTS，LTE)被连接起来。

这种情形，安全访问尤其重要。借助搜索引擎、端口扫描或者自动化的脚本，黑客无需努力就可以很容易得发现不安全的访问节点。这就是通信节点为什么要身份认证，数据的传输需要加密且数据的完整性必须保证。特别是对于工厂的关键基础设施访问。未经授权人员的访问，机密数据的读取和控制命令参数的修改都可能导致相当大的破坏，环境的污染及人员的伤害。

VPN的机制提供身份认证，加密和完整性保护，已被证明可以提供有效保护功能。西门子的Internet安全产品支持VPN连接，因此可以安全地传输通过互联网或移动网的控制访问数据。

正常的情况下，设备认证证书和值得xinlai的IP地址或域名名称通过防火墙的规则来阻止或允许。VPN设备和SCALANCE S防火墙使用特定用户防火墙规则赋予访问用户的权限。在这种情况下用户使用他们的名字和密码登陆Web界面，由于每个授权的用户被分配了特殊的防火墙规则，给用户根据其访问权限获得相应的访问能力。优势在于可以清楚地跟踪在特定时间对系统的访问情况。

带有三个端口的SCALANCE S623防火墙给系统集成商、OEM和最终用户提供了种解决方案。一方面，设备制造商出于远程维护的目的需要访问安装在最终用户那里的机器；但另一方面，最终用户的IT部门不愿意外部访问机器所连接的整个网络。通过SCALANCE S623，机器可以连接到工厂网络并且使用第三个端口连接防火墙到Internet。这样可以从Internet访问机器但从Internet访问工厂网络是被拒绝的。因此，技术服务人员可以远程访问机器设备但不能访问工厂网络（见图6）。

图6、 不能访问工厂网络情况下远程访问工厂设备

三、系统完整性

确保系统完整性被视为安全理念的第三大支柱。这意味着自动化系统和控制器组件，SCADA和HMI系统，需要防止未经授权的访问和恶意软件或者需要满足特殊需求，如专有知识保护。

1、 在工厂网络中保护基于PC的系统

就像办公网络的电脑系统防止恶意软件和通过安装更新和补丁来消除操作系统或用户软件已暴露的弱点一样。在工厂网络中的工业计算机和基于PC的控制系统也需要相应的保护措施。在办公环境已经证明的保护系统（如病毒扫描器）也可以被使用。因为病毒扫描器无法检测到所有的病毒，无力阻止更新病毒模板之前的型病毒，特别在自动化环境中不能及时的更新软件例如需要24/7操作期。所以根据情况来选择。

使用一种所谓的白名单软件可以替代病毒扫描器。白名单只允许运行用户定义的程序列表。如果一个用户或恶意软件试图安装一个新的程序，白名单会拒绝来防止对系统的破坏。

作为一个工业软件的制造商，西门子支持被测试过且兼容的病毒扫描器或白名单软件。

2、 控制层级的保护

我们已经拥有计算机和网络采取保护的知识。但对于特殊的设备及专有系统又如何保护呢？如何保护一个可编程控制器（PLC）和不使用商用操作系统或运行了数年甚至数十年的老版本系统的操作员站？

第三方的安全软件针对此是不能提供解决方案。访问此类设备系统的功能几乎不可能或访问的功能非常有限。对于控制层级的安全方案，自动化硬件制造商被要求提供相应的安全机制和提供用户特殊系统的安全设置项。同时，鼓励用户询问制造商是否有安全机制和如何激活并设置安全选项。

对控制层级的保护的实质是确保现场控制器的可用性和对知识产权的保护。由于自动化与IT的互连及集成不断增加，访问保护和防止操纵的要求在生产的工厂也发生着变化。这是现代控制系统不可缺少的部分。西门子新一代的控制器S7-1500已经集成了此功能。除此之外，西门子控制提供的功能还有密码保护、程序块保护和复制保护等确保工厂网络安全。

各个功能块可以得到保护，也就意味着未经授权的人无法访问功能块的内容及对功能块的算法的复制和修改。同时通过版权保护防止对设备的仿制。程序块与存储卡序列号的绑定使得被保护的程序只能运行在合法的机器设备中。这些功能有助于保护机器设备制造商的投资和维护他们的技术优势。