佛山STROMAG伺服维修

产品名称	佛山STROMAG伺服维修
公司名称	广州腾鸣自动化控制设备有限公司
价格	100.00/件
规格参数	
公司地址	广州市番禺区钟村镇屏山七亩大街3号
联系电话	15915740287

产品详情

佛山STROMAG伺服维修，佛山STROMAG伺服维修中心，南海STROMAG伺服维修中心，南海STROMAG伺服电机维修中心，顺德STROMAG伺服维修中心，顺德STROMAG伺服电机维修中心

佛山腾鸣自动化控制设备有限公司一直致力于工控产品维修，机电一体化设备维护，系统设计改造。具有一批知识扎实，实践经验丰富，毕业于华南理工大学、广东工业大学高等院校的维修技术精 英。维修服务过的企业，遍布全国。我们维修张力传感器、称重传感器、**计、变频器、直流调速器、PLC、触摸屏、伺服控制器、工控机、软启动器、UPS不间断电源等各种工业仪器。我们有大量工控产品配件，与合作客户长期维护服务，能快速维修客户故障，价格实惠。我们有大量二手PLC，伺服驱动器，变频器，直流调速器，变频器，触摸屏等工控产品出售，欢迎电询。

禅城区辖3个街道、1个镇：石湾街道、张槎街道、祖庙街道、南庄镇。区人民政府驻祖庙街道大福南路。

南海区辖1个街道(桂城街道)、6个镇(里水镇、九江镇、丹灶镇、大沥镇、狮山镇、西樵镇)。共67个村委会、182个居委会。 政府驻桂城街道。

3个维修服务点

地址1：佛山广州市番禺区钟村镇屏山七亩大街3号

地址2：肇庆市高新区（大旺工业园）

地址3： 佛山顺德大良凤翔办事处

开发区萝岗维修办事处：

黄埔区科学城维修办事处：

番禺区顺德大良凤翔维修办事处：

佛山南海禅城维修办事处：

佛山市南海区海八路

佛山三水办事处

维修品牌伺服:

鲍米勒伺服驱动器维修、PARKER伺服驱动器维修、施耐德伺服驱动器维修、ct伺服驱动器维修、力士乐伺服驱动器维修、安川伺服驱动器维修、MOOG伺服驱动器维修、LUST伺服驱动器维修、三菱伺服驱动器维修、西门子伺服驱动器维修、AB罗克韦尔伺服驱动器维修、三洋伺服驱动器维修、松下伺服驱动器维修、科尔摩根伺服驱动器维修、SEW伺服驱动器维修、ACS伺服驱动器维修、DEMAG伺服驱动器维修、B&R伺服驱动器维修、AMK伺服驱动器维修、太平洋伺服维修、NIKKI伺服驱动器维修、富士伺服驱动器维修、Baumuller伺服维修、EMERSON伺服维修、Schneider伺服维修、bosch rexroth伺服维修、yaskawa伺服维修、mitsubishi伺服维修、siemens伺服维修、Kollmorgen伺服维修、SANYO伺服维修、panasonic伺服维修、 YOKOGAWA伺服维修、PACIFIC SCIENTIFIC伺服维修、FUJI伺服维修、galil运动控制卡维修、库卡KUKA伺服维修、OSAI伺服驱动器维修、横河伺服驱动器维修、艾默生伺服维修、派克伺服维修、LENZE伺服维修、ELAU伺服维修、NORGREN伺服维修、BALDOR伺服维修、瑞恩伺服维修、RELIANCE ELECTRIC伺服维修、RELIANCE伺服维修、API CONTROLS伺服维修、SANMOTION伺服维修、TAMAGAWA伺服维修

STROMAG伺服维修常见故障：上电无显示，上电过电压报警，上电过电流报警，编码器故障，模块损坏，参数错误等故障。

随着工业化与信息化的融合推进，以及以太网技术在工业控制系统中的大量应用，病毒和木马对SCADA系统的攻击事件频发，直接影响到公共基础设施的安全，造成的损失不可估量。因此，目前国内外生产企业都是否重视工业控制系统的安全防护建设。但由于工控网络存在着特殊性，商用的信息安全技术无法完全适用，解决工业控制系统安全需要有针对性地实施特殊措施。

工业控制网络的安全漏洞

对工控系统而言，可能带来直接隐患的安全漏洞主要包括以下几种：

1、病毒与恶意代码

病毒泛滥也是总所周知的安全隐患。在全球范围内，每年都会发生数次大规模的病毒爆发，而全球现已发现数万种病毒，每天还会新生数十余种。除了传统意义上的具有自我复制能力、但必须寄生在其它实用程序中的病毒种类外，各种新型的恶意代码更是层出不穷，如逻辑炸弹、特洛伊木马、蠕虫等，它们往往具有更强的传播能力和破坏性。如蠕虫病毒和传统病毒相比，其大的不同在于可以进行自我复制，传统病毒的复制过程需要依赖人工干预，而蠕虫却可以自己独立完成，破坏性和生命力自然强大得多。

2、SCADA系统软件的漏洞

国家信息安全漏洞共享平台在2011年收录了100多个对我国影响广泛的工业控制系统软件安全漏洞，较2010年大幅增长近10倍，这些漏洞涉及西门子等国内外工业控制系统制造商的产品。

3、操作系统安全漏洞

PC与Windows的技术架构现已成为控制系统上位机/操作站的主流，而在控制网络中，操作站是实现与MES通信的主要网络结点，因此其操作系统的漏洞就成为了整个控制网络信息安全中的一个短板。

4、网络通信协议安全漏洞

随着TCP/IP协议被控制网络普遍采用，网络通信协议漏洞问题变得越来越突出。TCP/IP协议簇初设计的应用环境是美国国防系统的内部网络，这一网络是互相信任的，因此它原本只考虑互通互联和资源共享的问题，并未考虑也无法兼容解决来自网络中和网际间的大量安全问题。当其推广到社会的应用环境后，安全问题就发生了。所以说，TCP/IP在先天上就存在着致命的设计性安全漏洞。

5、安全策略和管理流程漏洞

追求可用性而牺牲安全，是很多工业控制系统存在的普遍现象，缺乏完整有效的安全策略与管理流程，也给工业控制系统信息安全带来了一定威胁。

应该采取的安全防护策略

工业控制系统的安全防护需要考虑每一个细节。从现场I/O设备、控制器，到操作站的计算机操作系统，工业控制网络中同时存在保障工业系统的工业控制网络和保障生产经营的办公网络，考虑到不同业务终端的安全性与故障容忍程度的不同，防御策略和保障措施应该按照等级进行划分，而实施分层次的纵深防御架构需要分别采取不同的对应手段，构筑从整体到细节的立体防御体系。

首先，可实施网络物理隔离。

根据公安部制定的《GA370-2001端设备隔离部件安全技术要求》的定义，物理隔离的含义是：公共网络和专网在网络物理连线上是完全隔离的，且没有任何公用的存储信息。物理隔离部件的安全功能应保证被隔离的计算机资源不能被访问(至少应包括硬盘、软盘和光盘)，计算机数据不能被重用(至少应包括内存)。

信息安全是一个体系防护的概念，网络物理隔离技术不可能解决所有信息安全问题，但能大大**网络的安全性和可控性，能彻底消除内部网络遭受外部网络侵入和破坏的可能性，从而大大减少网络中的不安全因素，缩小追踪网络中非法用户和黑客的范围。目前存在的安全问题，对网络隔离技术而言在理

论上都不存在，这就是各国政府和军方都大力推行网络隔离技术的主要原因。

网络隔离技术目前已经发展到了第五代。代隔离技术实际上是将网络进行物理上的分开，形成信息孤岛;第二代采用硬件卡隔离技术;第三代采用数据转发隔离技术;第四代采用的是空气开关隔离技术;而第五代隔离技术采用了安全通道隔离技术。基于安全通道的新隔离技术通过专用通信硬件和专有安全协议等安全机制，来实现内外部网络的隔离和数据交换，不仅解决了以前隔离技术存在的问题，还能有效地把内外部网络隔离开来，而且高效地实现了内外网数据的安全交换，透明支持多种网络应用，成为当前隔离技术的发展方向。

总的来说，网络隔离技术的主要目标是解决工业控制系统中的各种漏洞：操作系统漏洞、TCP/IP漏洞、应用协议漏洞、链路连接漏洞、安全策略漏洞等，网络隔离也是目前唯一能解决上述问题的安全技术。