[以太网]

基于以太网自动化系统的安全登录

若要在生产车间里使用IT技术设备，就要考虑生产车间的工作环境和条件。利用基于以太网基础的网络设备，可以把生产车间里一个个单独的加工中心组成一个网络，并利用安全防护功能防止非法人员登录这一网络。

文 / Ingo Hilgenkamp

在许多生产车间里，使用基于以太网技术的控制网络是自动化技术的重要推动力，而这一自动化技术系统以生产管理所使用的以太网标准为主导。在生产车间中推广使用以太网技术，也为自动化带来了新的课题，例如安全保护和路由选择。

现场总线系统，例如Interbus或者Profibus，由于其所使用的通讯技术协议、驱动系统、应用程序以及其封闭式的网络结构有着很好的登录保护，通过以太网技术的网络，使得生产车间原来一个个独立的生产设备能够有机地整合在一起，在最佳生产成本的情况下实现生产，并利用其安全保护功能防止非法入侵（图1）。

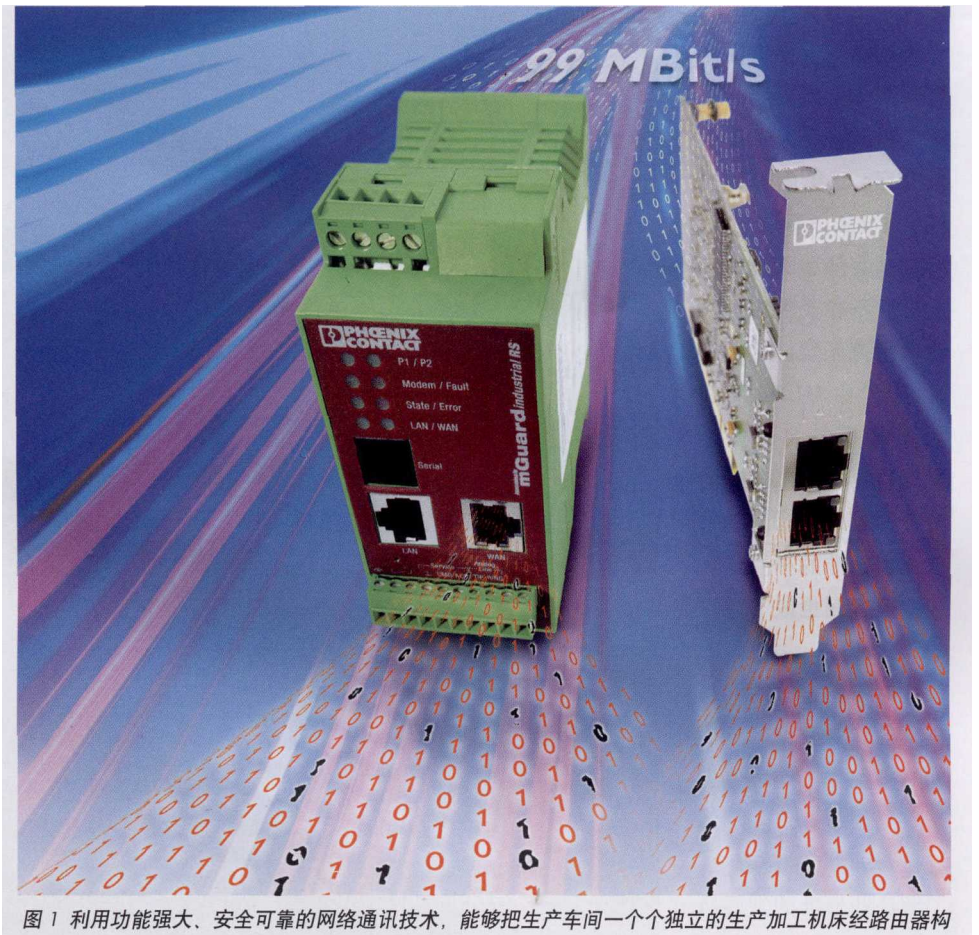

图1 利用功能强大、安全可靠的网络通讯技术，能够把生产车间一个个独立的生产加工机床经路由器构成一个网络，并利用其安全保护功能防止非法入侵

降低网络复杂性和费用成本

只有在有经济效益、能够直接提高附加值的情况下，在机械生产加工领域中使用以太网解决方案才是有意义的。若使用的是具有Layer3交换技术的以太网，则可以给生产车间带来下列好处：由于在自动化元器件中采用了通用化战略，因此网络系统的复杂性降低了；能够节约时间和资金，因为无需特殊的配置和专门的测试以及由此而产生的费用；故障排除更加简单，因为所用仪器设备可以在各个机床、设备之间交换；无需对机床、设备进行任何改动，因此也没有保修期方面的问题；所需的IP地址数

量也大大减少；有意识地采用了安全保护仪器和功能，以及登录检验功能。

在许多情况下，一台加工机床要驱动许多有着相同的、在同一 IP 地址范围内的部件。为了把这些相同的部件集成到统一的网络中，各个部件在上一级网络中要使用不同的 IP 地址，这就要求每一个被驱动部件进行单独的地址设置。按照这种方法为每一个机床部件配置 IP 地址时要做许多重复的工作，增加了辅助费用，也延缓了设备的调整试车。

网络中机床设备地址空间

Phoenix Contact 公司研发生产的 FL-Mguard 型带智能型防火墙的路由器，是按照所谓的 1:1 网址解析技术（1:1 NAT）来工作的，图 2 所示为 Factory Line 系列的工业用安全保护路由器；这样一来，有着同一 IP 地址的加工机床就可以受上一级网络的控制了，而这一路由器的结构却相当简单。例如，采用了这种 1:1 NAT 功能的印刷机就充分说明了这一技术的优点：在印刷机的不同工位上能够完成印刷图案不同颜色的印刷。印刷机的四个印刷工位内部联网并实现了自动化，四个印刷工位的功能相同，不同的只是其使用的颜料不同。若要用这一印刷机印刷色彩丰富的印刷品时，就要对机床的每一个部件及印刷工位单独设定地址。

驱动机床部件数据传输所需的带宽不是由通往控制点的路由器所决定的。这种带有性能强大微处理器的 FL-Mguard 型带智能型防火墙的路由器，有着与 Wirespeed 限速交换机相似的通讯速率，在 Vollduplex 模块中提供了足够的通讯能力。除此以外，这种路由器还提供了很高的登录访问安全性，不仅能够有效地保护机床设备的网络安全，而且也能够保护上一级网络系统登录访问的安全；所传递的数据包不是在网络元器件之间相互传递的，不会在它们中间被阻断。属于破坏行为的非法登录，利用 IP 欺骗——通过伪 IP 地址向计算机发送信息，并显示该信息来自真实主机等行为，都能够被这种带有智能型防火墙的路由器所识别和制止；另外，用户也可以利用网络安全软件（防火墙等）对其他访问方式进行保护。

利用电话服务的限制实现企业内部网络的安全保护

在销售服务工作的框架内，其他企业往往会不受限制地与销售服务部门的职工进行电话联系。这实际上也打开了企业通讯网络与外部通讯网络的大门，使得别有用心的人能够通过这一途径侵入到各个机床之中，能够在网络边缘绕过现有的安全保护屏障。技术人员可以利用其笔记本电脑对企业网络进行扫描，获取有关仪器设备数量、使用的操作系统、网络服务商以及安装使用的软件等许多信息。

在使用了 Mguard 智能型防火墙路由器之后，用户又多了一层安全保护，使得技术员的登录访问被限制在相关的单一机床上，从而保证了企业内部网络的安全，保证了企业的秘密不被窃取。

随着以太网元器件应用的推广，在许多网络中 IP 地址都成为了非常紧缺的资源。专门为

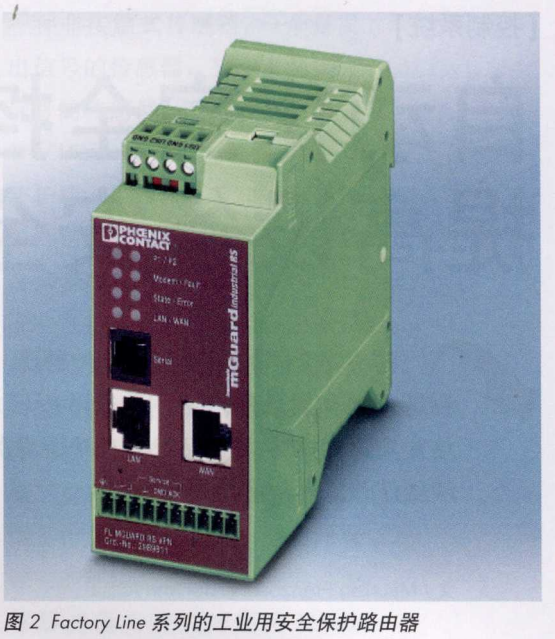

图 2 Factory Line 系列的工业用安全保护路由器

解决这一难题而研发设计的第 6 版互联网通讯技术协议（IPv6）、提供了 2^{128}（3.4 × 1038）个 IP 地址的通讯技术协议，在自动化技术解决方案中没有得到使用。为了能够更加经济地使用越来越多的 IP 地址，采用了虚拟地址的方法来解决问题：真实的 IP 地址与其他外部的 IP 地址结合起来使用。这种上一级网络与带有外部 IP 地址网络之间的连接也是由路由器来实现的：它只需要一个上一级网络的 IP 地址，就可以控制 100 个子网级的网络设备。

在这种虚拟地址技术中，1:1 NAT 技术同样有着重要的作用。每台机床的使用部件都可通过虚拟地址进行访问。因此，就可以在一个网络中使用任意多的 IP 地址了。每一个在虚拟地址和真实地址之间进行通讯联系的路由器都是网络系统中的一个瓶颈，是一个重要的“单点故障点”。Mguard 智能型防火墙路由器则有着足够的性能，保证通讯畅通无阻。MM