

工业安全

高效的生产安全网络

网络化生产要针对未经授权访问、恶意软件、技术窃取以及网络破坏等建立防护，同时工业安全不得削弱网络化的 CNC 和运动控制系统的功效和可使用性。

文 | Sven Härtel 和 Klaus Merkl

顺畅的基于以太网的网络和由此连接的各个层面的网络信息传输，是很多工业企业生产工序的主要部分，是机床与生产设备使用透明、生产率高和可用性高的决定性因素。如通过网络连接进行自动化系统的远程维护和远程诊断，这样能够省去工作人员的远距离奔波，同时节省费用，减少自动化系统的停机时间和由此造成的停产。工业企业利用网络支持进行工业生产和软件维护，同时来自中央服务器上或是通过 USB 输入的 CNC 操作数据、数据归档、程序、技术方

案配方以及过程数据，这些均反映出该企业的技术水准。达到了这样的自动化生产技术水平，可在多层面上简化并加快企业的生产作业，这对提高生产力至关重要。

虽然实现这样的自动化生产机制可能性在不断提升，但是系统访问风险也在不断增加，这些风险往往容易被人们所忽略，而这些系统访问有时是不利的，为此，必须采取适当的应对措施。而长时间以来，采取网络风险应对措施已经成了装备企业工业安全的重要工作。

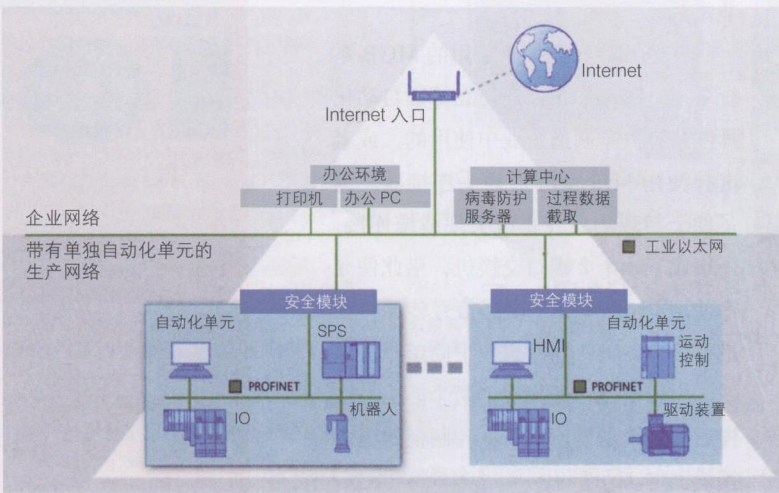
Siemens 公司作为世界上提供

领先自动化技术的企业，工业安全这个议题上也全心投入。工业企业使用 Siemens 公司的工业安全产品来控制机器、设备和系统，达到工业安全的目的。这样可通过一个整体化的途径，一个基于有形的设备保护、单元化的结构和各种网络访问，以及如开关、防火墙和在界面之上的 VNP 连接（虚拟专用网），这样的保护机制被称作“Defense-in-depth”战略（图 1）。

此外，使用 Siemens 的工业安全产品也使企业的自动化装置自身越来越“坚固”，且能够发挥辅助的安全功能（图 2）。Sinumerik 系统用于保护 CNC，Siemens Simotion 运动控制系统的作用为：针对非自主访问（局域 / 远程）的防护措施；针对有害软件（病毒和木马）的防护措施也属于工业安全范畴；针对技术窃取的防护措施（图 3）。

最新的 Sinumerik 840D sl 系统用于防护 CNC，该系统提供多种保护机制和功能，并与 NCK/PLC 和 HMI 部分相匹配。为了减少对自动化网络 Profinet 界面访问的可

图 1 企业自动化生产单元的结构分布图（如图），通过定义入口点（防火墙，VPN）来提供设备的可利用性并对设备进行保护



能性，Sinumerik 840D sl 系统将不必要的端口关闭。在专用的国际网络协议堆体系基础上，这些界面对 DoS 和 DDoS 有保护能力，这样即使负荷过大，也不会使系统崩溃。借助于网络服务器（在厂家提供时便已关闭）可在没有工程系统的情况下激活诊断系统，并通过一个使用者密码方案来确保诊断系统的安全。此时 PCU（PC 单元同 Windows 运行系统单位和 HMI）不通过重启系统便能简单的通过服务指令激活或关闭工作时间。

有效的工业安全方案的重要组成部分是使用者自始至终的管理和对控制访问权利的管理。在此，每个使用者在每次应用自动化系统时，只能得到其现实的任务所必需的权利（权利最小原则），这样便

能够减少错误操作和恶意操作（破坏），至少能够限制这些操作的发生。Sinumerik 840D sl 系统支持针对通过按键开关和软件对自动化系统访问的总体保护方案。

机器构造的基本议题是知识产权保护。为了防止截取和复制专门的控制功能，必须从技术层面就得保证可用一个密码进行保护，进而有锁住程序的可能性。而且，在锁住程序的状态下自动化程序的功能（系统的运行 / 反应时间）不受影响。因为影响程序的功能会对自动化生产质量产生影响。

Simatic Logon 软件包支持 Step 7 项目不受外来网络攻击。借助于 Windows 使用者管理功能，如支持使用者自动报告和使用密码自动运行功能。为了使企业的技术

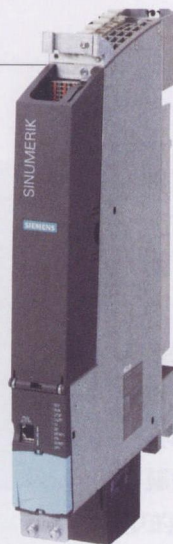
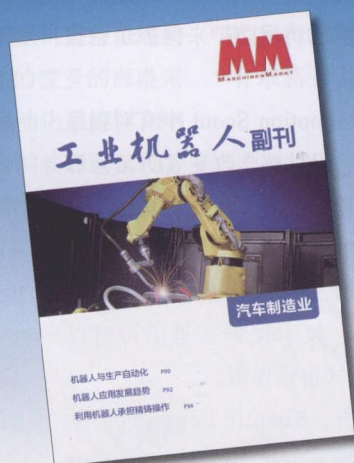


图2 通过可关闭的 Profinet 端口和所谓“硬化”的 Profinet 堆栈，Sinumerik 840D sl 系统避免企业工业网络受到外来攻击的可能性

不受外来攻击，现在固定组成部分包括集成有 Sinumerik 系统以及将 Siemens 的工业安全装置对 CNC 进行控制，且简单整合企业的信息交换、技术和生产程序的总集成软件包。为此所设计的“Lock-it”软件模块，通过加密 OEM 循环有效实施了有效实施了知识和系统的保护（Lock MyClock），并通过实践证明

工业机器人副刊

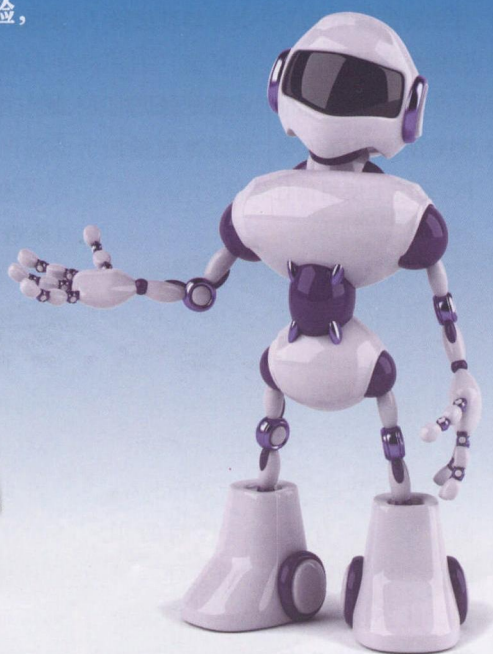
聚焦机器人，展望智能制造，解读行业案例，传播先进经验，推进中国制造业机器人应用水平。



精准定位

多渠道覆盖

资深编辑深度报道



纸媒



在线



会议



服务

联系方式：010-63326090 ext. 230/229
E-mail: mmsales@vogel.com.cn

MM 现代制造



Vogel 弗戈工业媒体

纸媒Print | 在线Digital | 会议Event | 服务Service

www.vogel.com.cn

Simatic Step 7 机制 (S7 Block Privacy (SBP), Lock MyPLC)) 对 PLC 程序的保护。为了保护工业企业生产运行及 PCU 文件系统不受恶意软件破坏, 建议使用病毒扫描装置。为此, 有以下三种装置已通过了测试, 可与 Sinumerik 系统配合使用: Trend Micro

Office Scan; Symantec Endpoint Protection; McAfee VireScan Enterprise。

Siemens 公司定期并及时检测后发布了 Microsoft Windows 安全补丁与自身系统的适用性, 并将测试结果于 Internet 上公布。

在向用户交付工业安全部件时考虑到必须符合高安全性标准, 包括激活防火墙、提供软件安装服务、借助于防破坏扫描仪对系统进行有规律的监控试验, 并提供静态代码分析小作用面。

一个进一步的工业安全保护机制是所谓的白名单, 借此可在一个 PC 系统上使用信任软件。

生产设备的工业安全

Simotion 运动控制系统可受到充分的工业安全保护, 在此 Windows 相应点只涉及基于 PC 硬件平台 (Simotion P3x0)。Simotion P 是一个基于 Windows 的系统, 带有一个高性能的实时核, 可实现最短的加工处理周期, 此外还具有工业安全扫描功能。Simotion P 在停机状态下通过一个 USB 实现与 Windows PE 的装配。此外 Windows XP 的防火墙可在 PC 系统上使用, Windows 保护补丁也是如此。在使用 Simotion

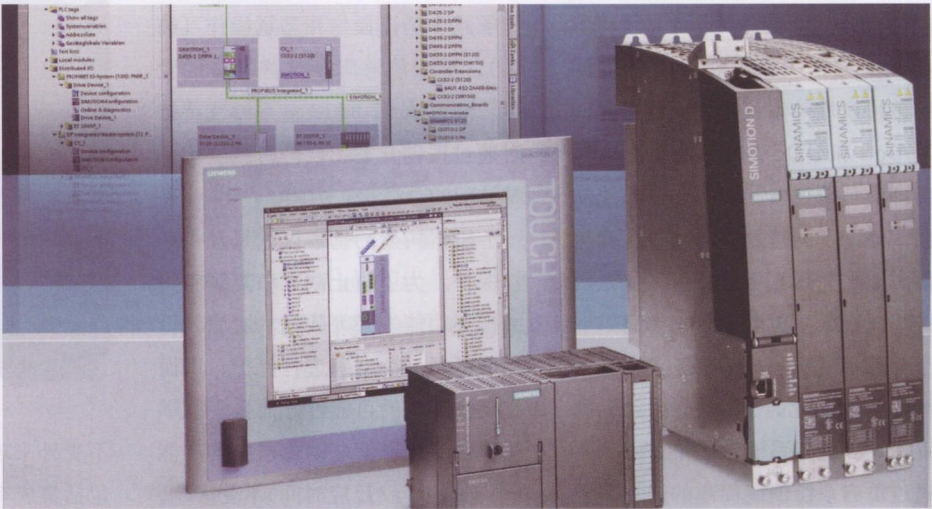


图3 随着生产领域越来越多的使用网络, 企业的工具和机器设备的工业安全变得意义重大, Simotion 便具备了所要求的工业安全保护机制和功能

系统时, Web 服务器是关闭且限制外来攻击, 此时该系统仅为各个使用系统的小组而设置的。不用输入密码便能够读取基本信息。要看表格、网页追踪和改动企业运行状态还要求进行一个总注册。在 Web 服务器中 (也包括在 Sinumerik 中) 的数据传输也可通过 https 连接实现 SSL 锁止 (Secure Socket Layer) 的发生。

在使用 Simotion 系统时也可通过可靠的访问防护来保护企业技术:

在 Simotion Scout 中有对程序 (原始)、设计感念改变 (DCC) 计划和文库的技术多级保护功能。由集成化的技术管理器锁住程序和文库, 在此有 4 级技术保护功能可供选择。技术保护在进出口时以 XML 格式继续保留。

此外, Simatic Logon 可借助 Simotion Scout 使用且对于项目和文库可通过以下的可能性来实现访问保护: 对使用者采取个性化授权分配和 / 或以使用者小组的形式进行授权, 将使用者分成小组 (如读结构件小组、书写输入小组、信息转移小组) 以及利用国际网络协议在线活动小组和在计算机上登录界

面小组, 以这样的小组形式实现项目访问和改动。使用者和使用者小组的授权有时间限制, 也有密码时效性对策以及其他可能性。

原则上 Simotion 能够提供技术保护, 其原因是每个 Simotion 程序在设置后便转变进一个专著文件, 并用于控制; 这在没有所属项目时, 不进行可逆向转换 (反向技术)。

此外, 对使用者而言还有不同应用形式的复制保护, 以阻止窃取项目的数据和将窃取来的项目数据传输给其他仿制的机器设备。一个 Simotion 程序是否改动了原始版本, 借助于技术系统的项目比较功能便可非常简单的进行确定。

工业安全远远广于单纯的生产 and 系统功能以及系统功能的具体实施, 必须始于在企业管理层直至企业员工层等所有层面, 所有层面均须建立一个广泛的工业安全的自觉性 (“工业安全意识”)。工业安全是一项与时俱进的任务, 人们不可能做到 100% 完成这个任务, 但是只要企业的经营者、系统集成商和供货商能够加强合作, 便可在很高程度上完成企业工业安全这个任务。MM