

## 技术讨论

Sinumerik 内嵌式的 Linux 系统不同于分布式桌面 Linux 系统，如 Suse 或 Redhat。系统经过 MC 特殊设计的。此系统只能用于 MC 产品。只有 Siemens 才了解系统详细结构。通常，病毒入侵桌面 PC 和服务器系统，不能在内嵌式 Linux 上运行。

所有的病毒可归为以下几类：

- ELF
- 脚本病毒：Perl, Shell, python...等脚本。
- 宏病毒

宏病毒需要主机支持宏语言运行的应用（例：MS-Word, OpenOffice, ...）。这类程序不能在 NCU 上运行，可以阻止病毒的传播。

Perl 病毒不能运行，因为 SINUMERIK LINUX 没有安装 Perl。

Python 脚本病毒不能运行，因为 SINUMERIK LINUX 不支持 Python script。

### Shell 脚本病毒

NCU 执行的脚本（启动过程中使用的）已经写保护，不能被病毒修改；所以病毒不能侵入，更不能通过此渠道传播。

关于"ELF"类型的病毒（LINUX 二进制格式）

NCU 执行的程序都已被写保护了，不能被病毒修改。同样，病毒不能侵入，更不能通过此渠道传播。

有害的代码经常通过缓冲区溢出的方法执行。SINUMERIK 与其他系统（桌面 PC 和服务器系统）有很大的不同，所以这种代码不能执行。

通常 Linux 系统不能被 Windows 病毒感染，也就是 Windows 的蠕虫、特洛伊等病毒不能在 LINUX 系统传播。

|

此外 SINUMERIK 840D sl NCUs / LINUX 操作系统采用更加严密保密措施。

Linux 内核含有多种过滤软件包（防火墙），防火墙用于工厂网络信息过滤。集成的防火墙已经优化输入输出通讯的设定。自动化网络隐藏于 NCU 集成的路由后端。

若客户希望提供其他方法，必须使用被此版本源码编译的特殊病毒扫描程序，如 Clamav。用户需使用“Open Architecture package”软件包在 NCU 上运行此软件。

同样的原因，Windows 上运行的病毒扫描软件(Sophos, Trend Micro, ...) 不能在系统上运行，同病毒不能运行一样。