Honeywell
THE POWER OF **CONNECTED**

产品信息

SMX 智能网关
USB 保护解决方案

虽然 USB 设备对于传输数据来说是极其方便的设备，但同时它们也会带来安全隐患。DCS 操作员及维护工程师需要使用 USB 可移动介质，比如用 U 盘和移动硬盘来将所需电子文件（例如补丁、备份及各种文档等）拷入 / 出工控系统。然而这些 USB 设备有可能将病毒及恶意软件带入工控网络，这将是一个很严重的安全隐患。

典型客户需求

- 客户既需要使用 USB 设备，又不希望引入恶意软件与病毒
- 保护 USB 设备的方法必须非常简单，可以作为一项网络管理政策加以执行
- 客户需要具备审核 USB 设备中文件的能力
- 客户需要一种数据防盗策略，可以有效对 USB 设备中的数据进行保护，防止数据失窃
- USB 设备保护最好使用密钥交换的解决方案

SMX 智能网关的主要功能

- 霍尼韦尔的 Secure Media Exchange（SMX）智能网关结合了硬件和 + 的优势，提供了一种主动性的防护方法，用以识别可移动介质上的恶意软件及病毒，并加以保护
- SMX 是一种介质扫描解决方案，可在 USB 驱动器连接到网络之前对驱动器的数据进行彻底的安全扫描
- SMX 由霍尼韦尔管理和维护，并且智能网关 SMX 软件会随着最新威胁的变化而自动更新，以便在有效期限范围内获得不间断的技术支持以及数据库的更新

SMX 智能网关的优势

- 与市场上流行的扫描杀毒软件不同，这些软件往往是控制系统被恶意软件和病毒传染之后才进行被动的扫描和查杀操作。SMX 智能网关在 USB 设备接入系统前就进行了扫描和认证，从而确保系统不会被感染。同时，USB 设备经过扫描认证之后转化为系统专用设备，即使丢失，系统之外的 PC 无法识别其中的数据，完全可以保证信息安全。

了解更多信息
请访问我们的网站：www.honeywellprocess.com
或联系您的霍尼韦尔客户经理

霍尼韦尔（中国）有限公司
特性材料和技术战略业务集团
过程控制业务部

北京办公室
地址：北京市朝阳区酒仙桥路14号兆维工业园甲1号
电话：010 – 5669 6000

上海办公室
地址：上海市浦东新区张江高科技园区环科路555号1号楼
电话：021 – 8038 6800

www.honeywellprocess.com

霍尼韦尔油气化工
微信公众号

霍尼韦尔油气化工
微博公众号

2017 年 9 月

Honeywell
THE POWER OF **CONNECTED**