



卡罗来纳精密制造公司在 Mooresville 的机床监测系统可以与每个工作站的输入板和大屏幕显示器进行无线连接

网络安全

保持工厂网络安全

对网络安全的担忧不应阻止工厂安装机床监测系统。

文 | Mark Albert



许多机械加工公司和工厂对机床监测系统感兴趣。这些系统将机床和其他制造设备连接到网络，从而收集机床产生的数据，并由检测软件进行分析。机床监测系统帮助工厂记录生产统计数据、工作状态、正常运行时间和配置。

多数监测系统使用互联网技术，这一点受到了现有和潜在用户的关注，因为网络安全已经成为了新型工业物联网讨论的一个紧急话题。黑客、病毒、恶意软件、数据窃取和其他威胁案例增加了人们的担忧。

位于 Massachusetts 的 MachineMetrics 公司是一家机床监测系统和制造分析装置供应商。从 2014 年以

来已经在很多机械工厂内安装了机床监测系统，目前正在监测超过一千台机床。MachineMetrics 公司的 CEO 和创始人 Bill Bither 在工厂网络和网络安全方面的经验让他看到了连接机床和监测网络存在的风险和好处。

首先，Bither 解释道，多数威胁来自黑客，他们专门攻击公司和公司的数据。幸运的是，这类攻击在机械工厂很少见。破解机床数据可以提高生产率并带来很大收益，这显然比风险要高。

Bither 提到，人们普遍持有一种错误观念，就是网络机床的意思是机床可以通过公共互联网直接访问。实际上，即便是最基本的网络，连接到互联网之

前也要设置一个路由器，任何外来黑客无法直接访问机床。

机床受到监测时共有八个步骤可以保护机床。Bither 表示：“这些步骤只是理解网络安全的开始。需要特别注意的是，这些步骤都是可以管理的。有了它们，考虑机床监测系统的工厂就可以自信地开展网络工作，尤其是与系统供应商解决网络安全问题时。”

修改路由器和交换机默认密码

不要让任何人（黑客或员工）能够通过你的网络修改你的路由器设置。一个未知员工或供应商可能会通过修改设置开放一个安全漏洞。试图访问网络的黑客可能会使用默认密码进行各种破坏。

工厂安装网络后，通常需要在初次配置路由器和交换机时设置密码。网络供应商通常会提供一个默认密码，这是为了方便配置。安装技术员或网络管理员可以使用默认密码进行路由器和交换机设置，网络需要通过这些设置连接到互联网或独立网络，以便进行数据交换。

一旦网络配置和试验完毕，应修改默认密码。同时，工厂需要确定哪些人有权知道用于修改网络路由器设置或连接到交换机的新密码，路由器设置和交换机连接控制设备如何与网络或互联网上的设备进行通信。正常情况下，必须为网络指定一个网络管理员。管理员通常具有 IT 背景，尽可能是参与网络安装的人员。然而，在较小的工厂，这个角色可能要由工厂管理者来担任。一旦网络投入使用，这些人可能意识不到修改密码的重要性。

很多小型工厂使用 IT 供应商的外包网络维护，供应商应该意识到密码保护的重要性，并提出维护建议。任何情况下保留默认密码都是有风险的，因为黑客掌握

了制造商设置的常见默认密码列表，所以这些密码的保护作用很小甚至可以忽略。

可用无线加密方法

不要使用未加密的无线网络。加密仅意味着网络协议对传输和接收的加密和非加密消息进行区别对待。然而，旧的加密方法，如 WEP（无线加密协议）很容易破解。新的加密方法 WPA（Wi-Fi 保护访问）则很难破解。最新一代协议 WPA2 对黑客的抵抗能力更强。即便如此，如果具备正确的工具和足够的时间，WPA 和 WPA2 加密也是可以破解的。这就是工厂最敏感的信息不应该通过无线连接访问的原因。

当然，多数工厂配备了基本的 Wi-Fi。这种网络适合于查看电子邮件、浏览网页等。然而，Wi-Fi 用于机床监测通常不能满足要求。实时机床监测要求与每台机床可靠连接。工厂的环境通常很嘈杂。工厂的机床和设备会随机发出各种频率的电能和无线电波。噪声可能会干扰采用无线方式发送的数据。即便工厂配备了使用工业 Wi-Fi 接入点和中继器的网络，仍有可能遭遇数据丢失的情况。由于这个原因，硬线连接的网络更可靠。对于硬线连接的网络，加密保护几乎不会增加系统的复杂程度。

通过互联网与工厂网络进行远程通信，加密的等级往往更高。例如，系统与 MachineMetrics 进行通信时，所有数据通过安全网页协议 HTTPS 进行加密。即便远程用户采用非加密的 Wi-Fi 或蜂窝连接，并且攻击方能够拦截每个数据包，仍然不能破译敏感数据。

个人计算机和服务器为最新产品

用于机床监测的工厂网络有可能包括与各种 PC 的连接。这其中包括设计、编程和管理办公室使用的桌面以及组成数控机床控制系统，用作操作人员界面的 PC（通常称为 PC 前端）。任何 PC，如果软件没有进行安全更新，在打开未知的电子邮件附件或运行可疑的下载应



图 1 MachineMetrics 的 CEO Bill Bither 支持使用带两个网卡的网关设备将机床网络与公共互联网分开

用时更容易受到钓鱼邮件和病毒的攻击。

黑客经常使用窃取的大规模电子邮件列表发送带有隐藏病毒或有吸引力的下载应用邀请，病毒或邀请可以秘密控制 PC。通过这些方法对网络上的 PC 进行未授权使用时不会发出警告（通常称为“零日攻击”，因为安全软件供应商采取反制措施的时间为零天）。除非这是一次针对性攻击，否则被攻击的 PC 会被用作一台垃圾邮件服务器，用于寻找银行账号详细信息或窃取信用卡号码。如果这是一次针对性攻击，则黑客可以窃取或修改被攻击的 PC 有权访问的敏感公司数据。

网络管理员处于最佳位置，可以确保工厂内连网的 PC 和服务器已经为操作系统安装了安全更新。更新工作应按照规定定期进行。然而，很多带 PC 前端的机床控制系统使用旧版本的 Windows 操作系统，导致无法再进行安全更新。这些 PC 常常被忽视，或即便

受到关注也无法更新。因此，建议将工厂网络与公司网络分开。

软件供应商，包括机床监测软件的供应商经常会通过更新或升级产品引入一些新特性，提高软件性能或修复 bug（不能实现预期功能的代码）。这些升级可能包括改进的安全措施，所以必须确定这些更新是否为强烈推荐内容。云系统可以一次对所有具有需要的注册用户实施这些软件更新和修复，这也是云系统应用的优势之一。

购买硬件防火墙并保持更新

使用防火墙是一种控制数据流入网络或网络设备的方法。防火墙的功能是通过检查数据包（包括使用代码告诉软件要发送哪种数据）或数据包中的数据来控制数据流动。然后，防火墙有选择地阻止数据到达预期目标位置。根本上讲，防火墙是一个规则检查单。例如，

如果为网络数据（TCP 80 和 443），允许通过；如果是电子邮件数据（TCP 25），允许通过；如果是从办公室服务器转移的文件数据，允许通过；任何其他数据都将被阻拦。

对于每个进来的数据包，防火墙都会读取规则列表，直到找出匹配的规则，然后才会采取行动。防火墙遵循的规则目的在于保护计算机免受黑客攻击和其他互联网威胁的侵害。

市场上有很多廉价的硬件防火墙（例如 SonicWall、Linksys、思科）。硬件防火墙的设计用于保护整个网络，而多数计算机运行自己的软件防火墙，使用特定规则来实现同样的保护功能。一个网络只需要一个硬件防火墙。硬件防火墙通常安装在连接公共互联网的交换机前面。

网络管理员应该确保防火墙正确配置，以便接收日常安全更新，获取这些更新通常需要缴纳在线服务年费。例如，服务可能包括保存着危险 IP 地址的范围或可以阻拦的垃圾邮件发送人的数据库。

使用强度较高的密码

要求员工为所有独立帐号设置高强度密码。确保任何云服务均通过 HTTPS 协议互联网基本操作系统的安全版本，设置高强度密码。使用孩子的姓名、自己的生日或其他个人数据作为密码较容易破解，尤其是内部员工进行网络攻击时可能知道这些信息。

高强度密码会增加猜测或破解密码的难度。黑客使用的复杂算法非常擅长破解看似复杂的密码，因为密码设置人只是使用外观相似的符号代替了字母，或使用其他策略让密码更难记忆。八位或更多位的随机字母、数字、符号组成的字符串强度足够大，但四个或五个单词串起来也可以提供相似的安全水平，即便这种密码违反了最常用的密码复杂性要求规则。新型密码生成器考虑使用 16 位或更多位随机字符作为密码，这样安全性更高。

另外，关于密码的其他两个问题值

得一提。密码应定期修改。如果用户名和密码已经被破解，并且包括在了黑客的密码列表中，使用新的密码可以恢复保护功能。更重要的是，每个站点或帐号应使用不同的密码。这样可以限制黑客使用相同的窃取代码访问多个数据源并进行破坏。

最后，双重身份“验证”如今越来越流行，也应该引起关注。这种验证方法要求增加一个入口，即使用物理设备，如 USB 记忆棒或一款应用生成新的代码，并且每 30 s 重置一次，必须在代码失效之前使用。即便某个人知道你的密码，也不能访问你的数据，因为增加一重身份验证就增加了一层安全保护。

确保工厂的物理安全

在工厂内的黑客更容易发起网络攻击。将门锁住，安装一个安全报警系统或采取其他措施阻止入侵者访问你的物理网络。当然，除了保护计算机外，使用需要钥匙卡或入口码的入口通道限制访问也是一种安全措施。然而，很多工厂忽视了装载平台、材料输送口和屋顶开口，也很少使用侧门作为入口。

将数控或其他敏感机床加入到 VLAN

VLAN（虚拟局域网）是一个由交换机管理的独立网络。在网络软件中设置交换机，用于确定可以使用哪些机床或设备进行通信。一旦交换机设置完毕，网络访问就会受到限制。由于交换机在软件上运行，不必改变物理线缆就可以重新配置 VLAN。可以采取与主网络分离的方式锁定 VLAN 上的设备。网络分离的关键优势是阻止外人访问运行多个机床子系统的可编程逻辑控制器。

这些控制器常被 IT 人员忽视，所以软件更新也不频繁。许多 PLC 运行的专用操作系统相对简单、高效，因为系统是模仿机电电路接线使用的基本梯形逻辑语言开发的。这种软件不容易被病毒攻击。然而，很多机床制造商使用自己

的操作系统和 PLC。操作系统可能是某个版本的 Windows 或嵌入式 Windows 系统。软件，尤其是运行旧版本 Windows 系统的软件更容易被病毒攻击，所以不应允许互联网进行开放访问。

PLC 不太可能成为黑客的攻击目标，因为多数黑客团队一般对 PLC 不熟悉。然而可以想象，如果 PLC 受到针对性攻击，很可能对关键应用领域，如国防或航空方面使用的机床造成运行故障。PLC 可能成为一个弱点，受到攻击后会引起机床故障或导致机床生产出不符合规定的零件，且难以进行检测。工厂的 VLAN 应该可以访问公共互联网。受控交换机将为工厂提供非常安全的 VLAN。

使用网关管理机床连接

如果机床网络与员工网络分开，机床监测服务如何能够实时访问机床数据呢？这是通过带两个网络接口的网关实现的，其功能与受控交换机类似。一个网络接口与锁定机床所在的 VLAN 进行通信。另一个网络接口只与机床监测系统通信。这样做可以防止机床与监测系统之外的任何系统进行直接或间接通信。

例如，MachineMetrics 提供的一项客户服务是使用工业 PC 作为网关。工业 PC 由两个网络接口，一个连接机床或机床网络，另一个连接公共互联网或内部 IT 网络。产品使用本地部署的网关软件通过 MTConnect 标准从所有机床收集数据、给数据加密和将数据传输到云端。

安装工业 PC 时，每处要使用一个网关。网关后的交换机实现网关与所有被监测机床的连接。如果一个工厂要将每台机床分隔开，则网关应连接到受控制的交换机，交换机每个数据端口代表自己的 VLAN 或子网络。否则，建议使用一个简单的受控交换机，既能满足需求，又方便使用且成本低廉。

Bither 关于机床连接监测系统的最终建议是恰当的网络连接源于良好的设计。需要让一部分人深入理解这些概念，并确保在设计中正确落实。MM