确保工业网络的安全

文/美国红狮控制 Diane Davis

由于工业网络已从生产现场设备间的互联扩展到覆盖管理供应链的公司办公室和设备，因此需要提高安全性以确保数据在各网络设备间安全而有效地传输。

通过使用工业路由器可轻松将网络扩展到生产现场，并提供安全、可靠和高速的网络通信。但在采购工业路由器时，首先要考虑以下几个关键因素。

伴随网络规模扩展而产生的挑战之一是网络更容易受到远程和病毒等网络攻击。这也是决策者在购买网络设备前需要进行安全评估的重要原因。

在部署有线路由器，对工业资产进行监控和管理时，数据安全是首要考虑因素。通常需要采取最佳防护措施，以跟踪网络中的通信、确定通信的数据类型及有权限访问相关数据和硬件的用户。

某些有线路由器通过虚拟专用网络 (VPN)将专用(公司)网络安全的扩展到远端，例如生产工厂。公司决策人员应选择购买支持IPSEC和OpenVPN软件的设备，这两个软件都可以针对不同的网络应用提供独特的VPN功能。其中，IPSEC通过可靠的加密和共享参数来保证前端到远端网络设备间数据通信的安全性；OpenVPN则通过共享证书来确保数据的安全，同时在路由器间提供安全的数据传输。

下一层防护是使用SPI防火墙(全状态数据包检测型防火墙)。SPI可以对每个数据包进行扫描，并根据当前运行的服务判断允许数据包通过或丢弃。例如，某个远程端可能只被允许发送Modbus数据包，以限制数据的使用。这种情况下，路由器内的防火墙将拒绝任何非Modbus数据通过。

类似于防火墙的数据包控制功能，路由器和远程终端设备 (RTU) 也应该具备相应的访问控制表 (ACL) 。该表用于对访问网络设备的用户凭证进行控制。通过将ACL和用户身份验证结合使用，可以确保只有特定的用户才可以访问特定的服务，以提高安全性。

设备同时也应该具备适应环境变化的能力，例如可适应广泛的工作温度范围、输入电压的波动和空气中混有可能导致设备中运动部件故障的颗粒物。不管是用作基本的WAN连接还是现有网络连接的备用，只有能适应严苛工业环境的有线路由器才最为可靠，尤其是在油气、能源和水/污水处理等首重安全和可靠性的应用中。

增加生产现场工业网络的连接是提高办公室、工厂和设备间通信的可靠投资方式，但决策者在考虑网络性能的同时应进行必要的安全评估以保护基础设施的安全性。