White Paper **WP031001EN** Effective April 2014

Securing access at the machine level

Kerry Sparks
Eaton

Abstract

When a machine is not functioning properly, it is important to diagnose the problem quickly and take corrective action. Often, local maintenance personnel look to the original equipment manufacturer (OEM) to solve the problem. In order for the OEM to do so, remote accessibility is crucial. Without remote access to the machine, it can be difficult to determine and address the issue in a timely manner, resulting in costly and time-consuming trips. On average, field service visits cost more than $1,000, according to data from the Technology Services Industry Association (TSIA).

At the same time, it is important to recognize that there are risks with remote connectivity. There is regular news coverage surrounding cyber security issues and breaches. For example, the Stuxnet virus was a wakeup call for automation suppliers who assumed that their systems would not be targeted for attack. Further, as the use of smartphones, tablets, and other bring your own devices (BYOD) continues to increase in the manufacturing sector, those devices become targets for cyber attacks as well.

Consequently, cyber security is a core focus of IT departments. Understanding how to mitigate risks while also providing secure remote access can prevent production disruption and reduce support costs.

Key remote capabilities

Remote access encompasses a broad range of technologies that can be useful in determining the cause of a machine-level concern. These technologies include:

- **Thin client connectivity over the Web**
  The ability to use standard Web browsers to log in remotely to the machine's control system and view the same screens that the operator uses without disrupting the operator's ability to monitor and control the machine.
- **Remote annunciation via email and text messaging**
  The ability to configure alarms and events to automatically generate text messages and emails can prevent production disruption and minimize downtime.
- **Smartphone applications**
  The ability to provide key process graphic and alarm information and control capability to mobile devices expands support to a growing suite of ubiquitous mobile tools.
- **Remote desktop**
  The ability to manage the machine/process remotely, as if standing in front of the HMI, is often required to fix problems quickly.
- **File transfer protocol (FTP)**
  The ability to send and receive files, such as historical alarms and archived data, can help the remote experts troubleshoot the machine.
- **Development software interface**
  The ability of the HMI/SCADA developer to connect to the remote system and make changes to the application on-the-fly over the Web can facilitate enhancements to the application that can prevent problems in the future and improve the user interface without forcing a shutdown of the running application.

Powering Business Worldwide

Security technologies

There are also many ways to secure remote access, enabling OEMs to provide support in a secure environment even if they are located hundreds of miles from the machine. Firewalls, virtual private networks, and other methods can help reduce cyber security risks, while enabling the connectivity required to support and service equipment.

For example, a firewall can be used to help keep a network secure. It can either be software-based or hardware-based, and its primary objective is to control the incoming and outgoing network traffic. Firewalls are designed to analyze the data packets and determine whether they should be allowed to pass or not, based on a predetermined rule set. Most routers that pass data between networks contain firewalls and/or firewall components.

Secure socket layer (SSL) encryption is important to help prevent unwanted access to information about the machine. This addresses security between outgoing email and incoming (HTTPS) network access.

A virtual private network (VPN) uses the Internet to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides security so that traffic sent through the VPN connection stays isolated from other computers on the network. Some routers can create one or more VPNs that allow secure connections from the Internet to computers within a plant network.

Deep Packet Inspection (DPI) is a form of network packet filtering that examines the data portion of a packet as it passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or other defined criteria. It can then decide whether the packet may pass, be blocked, or be routed to a different destination. Certain routers and passive network devices that are commercially available incorporate this technology to filter messages at the application protocol layer (e.g., Modbus® TCP or EtherNet/IP).

Segmenting the network into functional areas using intelligent routers provides additional layers of security. The more layers of security, the more difficult it is for cyber criminals to compromise the security of the manufacturing line and its control system. In addition, network segmentation provides a mechanism to isolate the control system from a plant or office network by providing an "air gap" in the event that other segments of the network are under attack. Unplugging the router's uplink to the rest of the network kills remote connectivity, but it allows the manufacturing line to continue to run in this worst-case scenario.

Some Windows®-based HMI/SCADA systems offer a protected, non-corruptible operating system. In the event that the machines do contract a virus or other malware, the problem can be cleared with a simple reboot. Despite all of the network security measures, an engineer or operator can still introduce a virus into the network by simply plugging an infected USB memory stick into a PC behind the firewall. A reboot will get the machine running much more quickly than a backup to a restore point, assuming a good restore point is even available.

Web conferencing tools provide on-demand collaboration and Web conferencing applications. Because these on-demand tools and their security mechanisms are familiar to company IT groups and because they require both ends of the conference to initiate a connection, they can be secure ways of granting remote access without the risk of exposing the network to unwanted users.

Security threat vectors

From the perspective of the engineer designing the methods that support remote access, the control network for a typical mid- to large-sized plant information and control network may look like **Figure 1**.

That same network likely looks vastly different to the corporate IT manager who is working to secure the network. The IT manager may see the same network that is shown in **Figure 2**.

The IT department may seem like the "preventers of information services," but recent history shows that they are not paranoid. They are keenly aware of the dangers that remote access can cause.

Security threat vectors are those paths that malware may use to infect the plant network. In **Figure 2**, those paths include:

- External users accessing the network through the Internet
- Misconfigured firewalls
- Unsecure wireless routers and wired modems
- Laptops infected elsewhere that can plug into the network behind the firewall
- Infected USB keys and PLC Logic programs
- Unsecure RS-232 serial links

Conclusions and recommendations

Remote connectivity can help end users and OEMs address machine issues more efficiently and quickly. Providing that access in a secure environment is crucial. To achieve both connectivity and reasonably secure access, it is important to evaluate those capabilities in your HMI/SCADA supplier, and see how they can help protect the operating system from malware attack. Further, it is important to engage the end user and their IT organization early in the planning stages to design the network interfaces and firewalls. Working closely with the IT team, manufacturers, and OEMs can help to minimize internal and external risks and develop a remote support plan that can be both secure and effective.

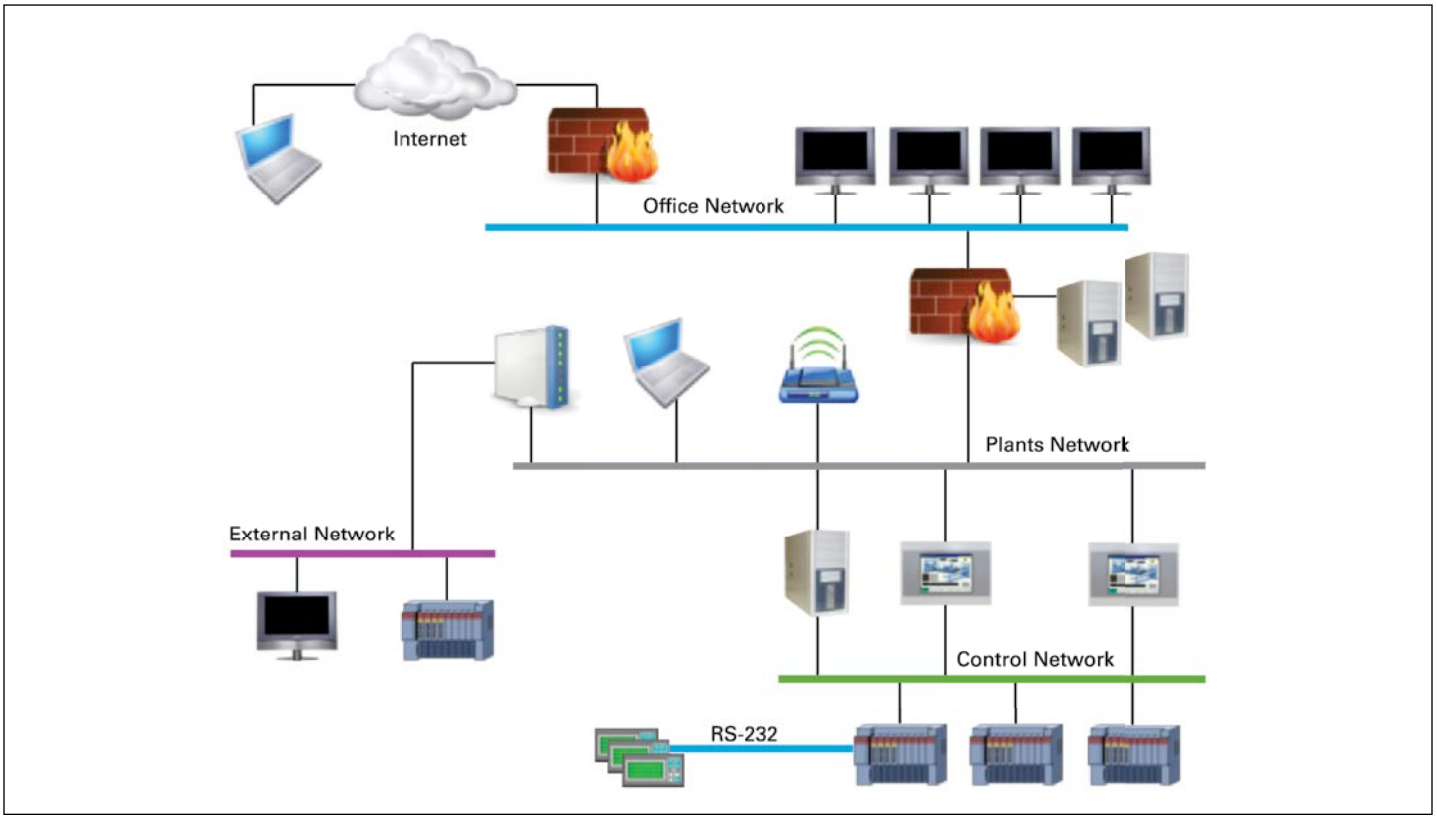

Figure 1. Paths to the Control Network from an Engineer's Perspective

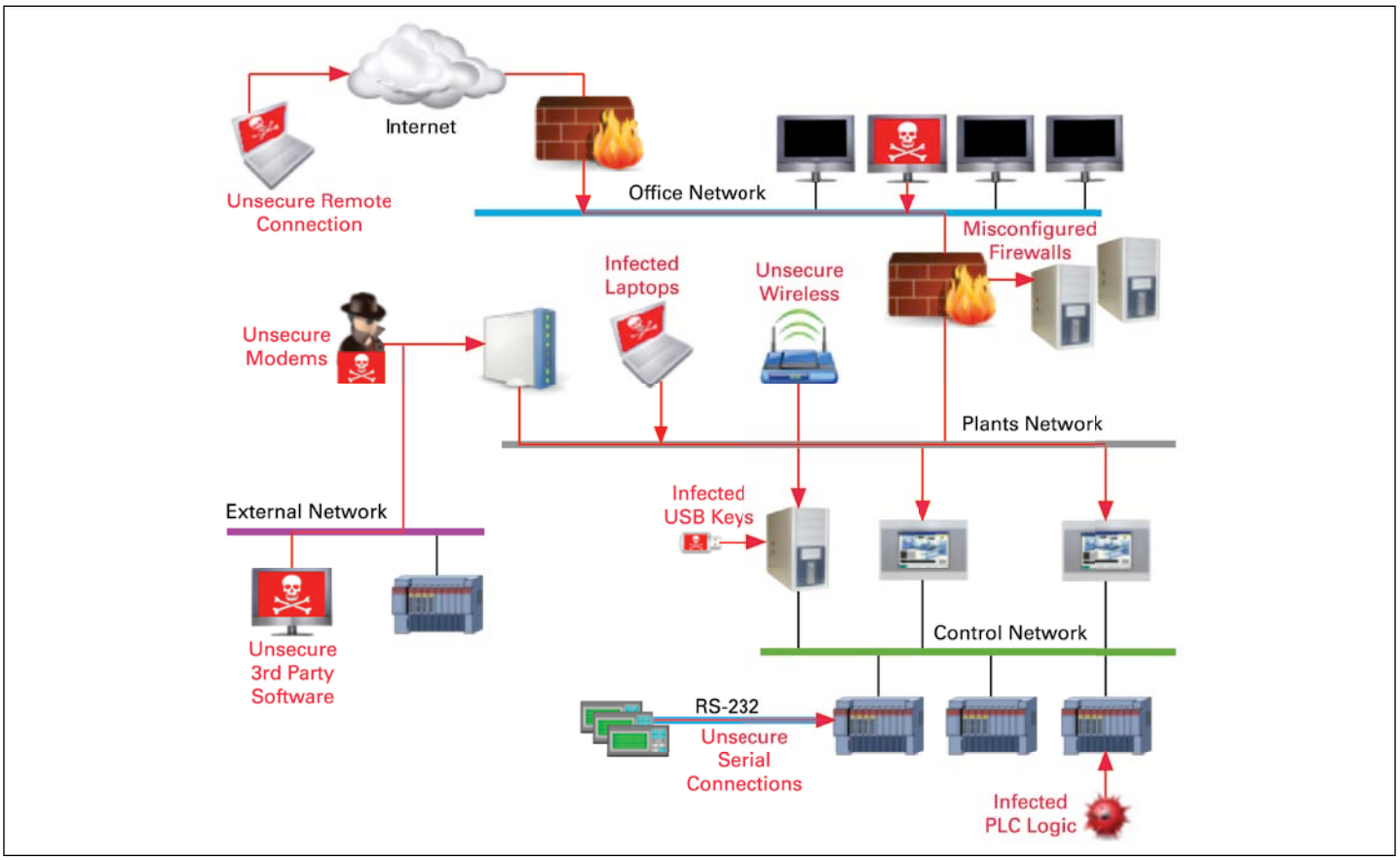

Figure 2. Paths to the Control Network from a Corporate IT Manager's Perspective

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP031001EN / Z15037
April 2014

Powering Business Worldwide