Security Considerations for Industrial Remote Access Solutions

By Keith Blodorn, Director of Product Management, and Vishal Prakash, Strategic Product Manager, ProSoft Technology

Abstract

For manufacturers, machine uptime is directly proportional to profitable operation. As machines and production processes become more complex, the need to provide expert technicians with remote access to industrial control equipment is more important than ever. This paper highlights several key points for enterprise network engineers and automation engineers when considering how to safely and securely provide remote access to industrial machines.

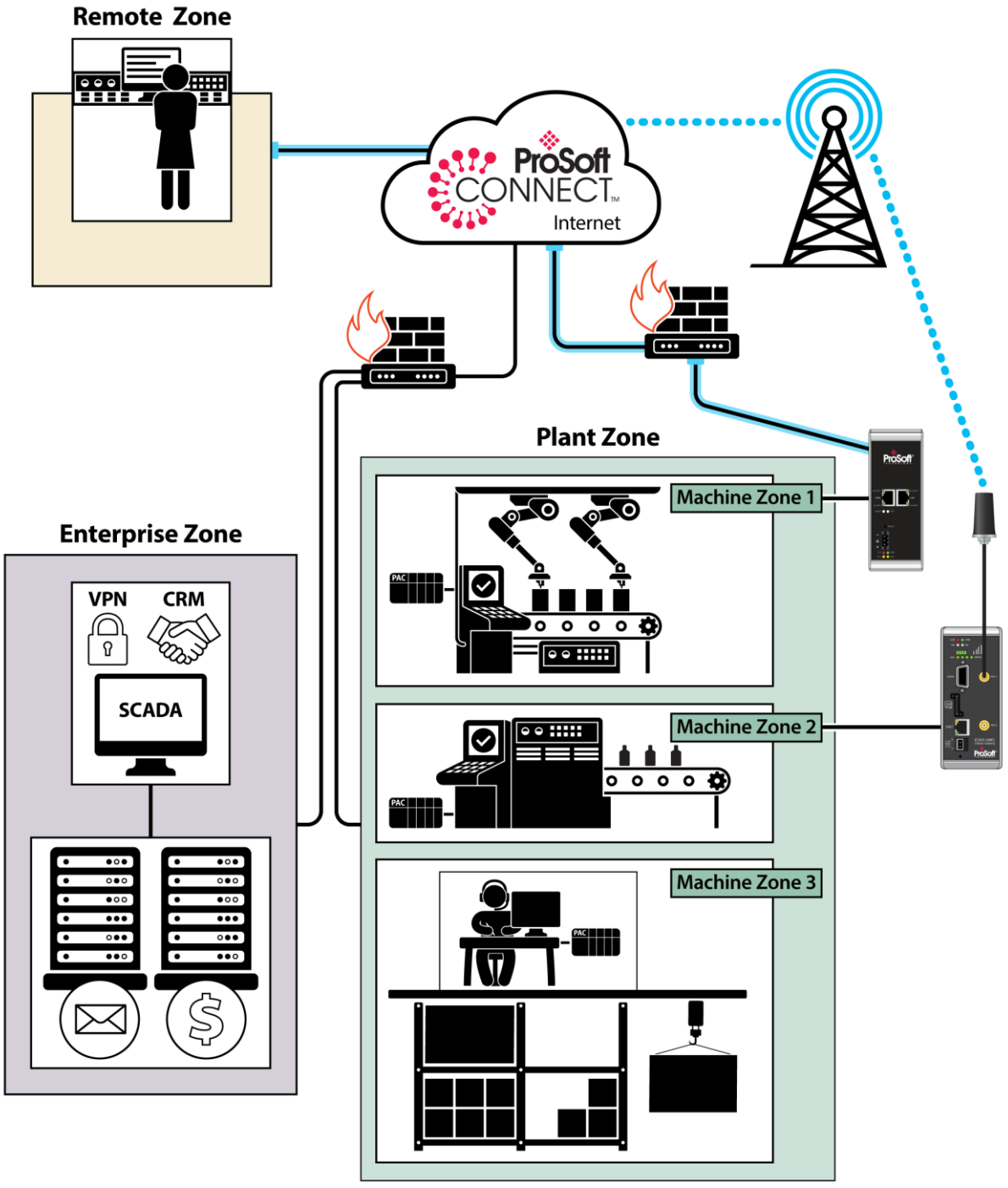
Introduction

It's 4PM on Friday, when the phone rings with news that the palletizer on your plant's main bottling line just went down. The plant technical team is stumped and the palletizer vendor's service engineer won't arrive until Monday. The plant manager is on the other end of the phone line, asking you to somehow let the vendor access the palletizer control equipment to resolve the problem remotely. Otherwise, he'll need to idle the plant through the weekend, costing your company tens of thousands of dollars in lost revenue and wages.

This scenario is a frequent occurrence in today's world of automated manufacturing. At the same time, horror stories of corporate data breaches – including breaches due to outside contractor access mechanisms – raise the stakes for enterprise security professionals. With production quotas and profitability targets to meet, simply saying "no" to outside access is not an option for most companies. But before handing out a guest account on your corporate VPN or setting up a remote desktop connection to a production line PC, let's consider the security and personnel safety factors associated with remote access to machine networks.

To begin with, consider these three key zones:

1. **Machine Zone** – this includes the machine control equipment, the network that interconnects that equipment, and possibly remote access modules. Multiple machine zones within a plant make up the plant zone.
2. **Enterprise Zone** – this includes the enterprise core network, business assets like servers and applications, Internet access, and firewalls.
3. **Outside Zone** – this includes the remote user, cloud connectivity service, and communications infrastructure like the Internet and cellular networks.



Each of these zones presents unique network security requirements and challenges. Understanding the challenges in each zone will help the enterprise network engineer determine the best solution that balances the production team's need for fast remote support, the safety manager's need to ensure personnel safety, and the enterprise network team's need to safeguard the company's data and information systems.

Another consideration for enterprise security professionals is industry standard cyber security guidelines. Now, an entire novel can be written about the various standards – NERC, NIST, IEC27001, IASME, and several others. Almost all of these are guidelines to good practices rather than strict adherence. So, for the purpose of this white paper we are going to focus on IEC62443.

What and why is IEC-62443?

IEC/ISA-62443, formerly known as ISA-99, is a series of standards and guidelines aimed for the implementation of electronically secure Industrial Automation and Control Systems. This reference guide may be used by end users, system integrators, security professionals, manufacturers, control system engineers, and architects.

Of all the security standards, IEC-62443 is the main guide for Industrial Automation and Controls systems as it deals with processes and guidelines from systems design to product development. As such, it is important for personnel involved with control systems to have an understanding of this standard and how it can help them solve security-related issues.

The good news is that ProSoft Technology uses these processes and guidelines to ensure our hardware and software products meet or exceed industry standards. Our products and solutions are audited internally and by an external independent organization regularly as part of our continuous security improvement process.

Now, let's look at each of the zones mentioned earlier in this document.

Machine Zone

Machines are the heart of the manufacturing enterprise, making the products that drive revenue and pay the bills. In today's manufacturing world, machines are more complex than ever. A machine like a palletizer or filling machine typically has one or more Programmable Automation Controllers (PAC), electronic operator interface screens, and scores of sensors, motors, and actuators. Often, these controllers and devices are connected via Ethernet. However, the machine Ethernet network should be segregated from the Enterprise Zone network and other machine networks through a DMZ[1], which allows the machine to carry out its critical high-speed control communications without having to share its network capacity with office applications or other machines. This segregation also provides an important layer of security, as only specific connections between machines and enterprise assets are allowed to communicate and transfer data with each other. This minimizes the risk of industrial devices infecting enterprise assets, and vice versa.

Before considering network security in the Machine Zone, however, it's critical to first understand machine safety. The equipment in the Machine Zone is responsible for running motors, energizing actuators, and running the machine. Anyone accessing the machine network has the ability to cause the machine to operate, and must fully understand the risks associated with any changes to the machine controls. Access to the machine network should be limited to only when the machine is in a "safe" state.

This brings us to the remote access device used in the Machine Zone. There are two common ways to provide remote access to the Machine Zone – a PC with a remote desktop connection and a dedicated remote access gateway. For enterprise network engineers, it's tempting to connect a PC to the machine network and set up a remote desktop connection as this is a common practice in the Enterprise Zone for troubleshooting user PCs. However, this is not the best path in the Machine Zone for several reasons.

First, a PC in the Machine Zone provides a highly capable platform for launching cyber-attacks against the machine and up into the Enterprise Zone. PCs typically have more advanced networking capabilities, so the user on the other end of the remote desktop connection now controls a device

[1] "Securely Traversing IACS Data Across the Industrial Demilitarized Zone", Rockwell Automation® and Cisco

that can do a lot more than simply connect to the machine control equipment. This setup can allow a remote user, intentionally or inadvertently, to bypass the DMZ and access parts of the enterprise that he shouldn't access.

Second, PCs typically have a full featured operating system, including many components that have nothing to do with the basic goal of providing remote access to the machine. Over time, vulnerabilities in these OS components come to light, creating the need to regularly update the PC or risk exposing both the machine and the enterprise to attack. Worse, the PC used for remote desktop access is often supplied by the machine builder or system integrator, and may not be under the plant IT department's standard update and virus protection routine.

Finally, programming and troubleshooting industrial control equipment requires specific software packages, which are often quite expensive to license. Installing a PC on the machine for remote access requires purchasing licenses for all the necessary software, and adds to the list of installed software that the enterprise network team must monitor and update.

The better solution for access to the machine network is to use a purpose-built remote access gateway, like the ProSoft Technology ICX35-HWC cellular LTE and PLX35-NB2 wired network gateways. These devices plug in to the local machine network on one side and an Internet accessible wired or cellular wide area network on the other side.

Because the gateway is designed specifically for secure remote machine access, it does not have all the capabilities of a PC and thus does not provide a platform for attacks against the enterprise zone. The ports on the PLX35-NB2 are logically separate and *do not allow routing of traffic* from the machine network port to the wide area network port[2]. Unlike with the remote desktop approach, the remote access user cannot route back through the PLX35-NB2 to reach assets on the enterprise network. Both gateways can integrate into the machine controller program, such that remote access is *inhibited by the machine controller* whenever the machine is in a state where remote access would be unsafe. Both gateways use *outbound-only connections* to the secure ProSoft Connect service and only after the gateway has been activated in the Connect service through a two-factor activation process. ProSoft Connect requires a second form of authentication for a remote user when attempting to access the machine.

Unlike the full operating system on a remote desktop PC, the firmware on the ProSoft remote access gateways is regularly subjected to *extensive penetration testing* and *regular ongoing vulnerability evaluations* by a third-party cyber security consulting firm. The gateways were tested using industry standard penetration testing software tools, Achilles and Codenomicon. In addition, ProSoft contracts a cyber security consultant, Independent Security Evaluators, to perform regular evaluation of both gateways and the ProSoft Connect service looking for vulnerabilities. The ProSoft gateways have been hardened to withstand would-be hackers; before using a PC for remote access, consider whether it has been and will be subjected to the same rigorous testing.

An often-overlooked aspect of security and protection is capturing historical information of events and changes. A skilled hacker will defeat the logging in a PC and cover his tracks to avoid detection. The ProSoft Connect service keeps an audit trail of events, which cannot be changed or deleted, to maintain clear visibility into access and changes.

[2] Network Address Translation and Port Forwarding functions can be configured in the PLX35-NB2. If configured, these functions do provide a fixed software-based means of mapping local ports to wide area network ports.

Enterprise Zone

The Enterprise Zone is often a large, complex network that connects the organization's PCs, servers, email system, customer databases, and financial software. This zone is often the focus of hackers, looking to steal consumer data such as credit card numbers, employee information, or corporate intellectual property. The enterprise network typically provides users with access to the Internet, but also includes firewalls and other technology to limit the kind of connections that enter the network from the outside. Many companies provide VPN access to the Enterprise Zone for authorized users who need to access enterprise network services remotely. Companies sometimes also provide vendor and customer portals for access to some parts of the enterprise network.

Faced with the need to establish a remote connection for the external machine builder, the corporate VPN or a dedicated vendor portal might seem like a quick and easy way to solve the problem. However, guest VPN access will give the remote user access to more of the enterprise than he needs. In addition, the enterprise network engineer will need to establish a new connection or route from the Enterprise Zone through the DMZ to the Machine Zone. Not only is this inconvenient, these ad hoc configurations may inadvertently leave access to confidential enterprise assets open. Since the encrypted VPN tunnel terminates within the Enterprise Zone, the remote user will necessarily gain some visibility to the enterprise network. Additionally, granting enterprise VPN guest access to a PC that does not fall under the company's update and virus protection routine potentially exposes the servers and PCs on the enterprise network to malicious software on the remote PC.

Conversely, remote access gateways installed on the machine network provide a more secure way for the remote user to traverse the Enterprise Zone. The ProSoft PLX35-NB2 uses the enterprise network's Internet access to allow the remote user access to only the machine network, while the ICX35-HWC uses the cellular LTE network instead. The remote user's VPN tunnel is terminated *only on the local port of the gateway*, so the user never "sees" any part of the Enterprise Zone. The traffic between the gateway and ProSoft Connect service is strictly over secure HTTPS connections, using AES 256-bit encryption. This way, one can connect the machine to the Internet using the enterprise Internet connection or the cellular network, while maintaining a clear separation of the machine and enterprise networks.

Outside Zone

The outside zone includes the remote user's PC, the cloud connectivity service, and communications infrastructure like the Internet and the cellular network. Several key elements of any remote access solution reside outside the enterprise and are therefore more difficult for the enterprise network engineer to control. Therefore, it's vital to understand the security features of the remote access solution's components in the Outside Zone to determine how well the solution protects the enterprise.

The first component is the remote user's PC – and the software needed to make the remote access solution work. Some remote access gateways only work in conjunction with software that must be installed on the remote PC. While this kind of product offers the remote user a slightly more convenient way to connect, it also introduces several critical security issues. First, the software itself has been targeted by malicious actors like the Dragonfly group. By replacing the real remote PC software with an infected version, Dragonfly attackers were able to gain access to industrial machine networks across several industries[3]. Second, the enterprise network engineer has no way to know if

[3] "Defending Against the Dragonfly Cyber Security Attacks", Joel Langill, Belden Inc.

the remote user is keeping this software up to date. As vulnerabilities in common software components are discovered, the remote access software often needs updating to address these issues. If the remote user is not patching this software, he may inadvertently compromise your enterprise.

ProSoft Connect *does not require user-installed software*. Instead, the service uses the industry standard, operating system native L2TP VPN client with 256-bit AES encryption. Remote connections use *single-use, randomly generated user names* which cannot be reused. Even if an attacker were to steal the connection information when a Connect user creates a VPN tunnel, that information cannot be used to create another tunnel. If a vulnerability is found in any component used in ProSoft Connect, all users are covered as soon as we update the service. As a result, ProSoft Connect reduces the potential for the remote user's PC to introduce vulnerabilities beyond the control of the enterprise network engineer.

The next Outside Zone consideration is the security of the VPN server technology or appliance which might reside in the Enterprise Zone or in a cloud connectivity service. It is common practice to try and save a few dollars by using freely available VPN tools like OpenVPN installed on a server with a static public IP address and add static or common passwords rather than using a hardened two-factor authentication scheme. Once the complicated VPN software setup has been meticulously configured for remote access, network engineers must understand and learn all of the potential threat vectors to adequately secure the VPN software to ensure hackers cannot gain access. Finally, network engineers must regularly check for vulnerability and security updates to the VPN server software and the PC software running the VPN server. Cloud service technology, including security, has advanced significantly in the last few years. In addition, the major cloud providers like Amazon, Microsoft, and Google offer a level of physical and cyber security on their platforms that is significantly greater than what most companies can build on their own. Security-centric services like ProSoft Connect use several key technologies to keep remote machine access secure. ProSoft doesn't stop at using these key technologies; as stated earlier, white-hat security experts are regularly targeting the ProSoft Connect service to identify and address potential vulnerabilities so the network engineer doesn't have to become a security expert.

ProSoft Connect is built with scaling, robustness and security in mind by leveraging a container and micro-service architecture.[4] Compared to earlier cloud services using Virtual Machines to run monolithic software applications, each function in ProSoft Connect is designed as a stand-alone micro-service. These stand-alone services run in containers, which are like very tiny virtual machines and can be scaled to handle more demand when needed. The key difference is that the container *only runs the application components needed by the micro-service.* This reduces the likelihood that a security flaw in one OS component will compromise the service. In addition, because the micro-services all run independently of one another, a vulnerability in one micro-service won't provide access to the entire cloud service. Finally, if an update is needed in any one component or micro-service of the entire cloud service, the update is performed often without impact to any other running services. Due to our flexible design, we can even upgrade services without affecting that service.

Conclusion

ProSoft Technology's secure ICX/PLX gateways and ProSoft Connect are subjected to extensive penetration testing against the Achilles and Codenomicon platforms as well as constant evaluations by an independent third-party cyber security consultant. We take care of the security and complexity

[4] "ProSoft Connect demonstrates the benefits of a Container and Microservices cloud architecture", Keith Blodorn, ProSoft Technology

of remote access so that you can access your machines and processes at any time and ensure a positive impact on the bottom line.