Securing a Control Systems Network

By Carl Neilson, Associate Member ASHRAE

With all of the recent news about security breaches in control systems, it is a wonder that anyone who is responsible for one gets any sleep at night. Those that do are either blissfully unaware of how open their control system might be, or they have done their due diligence and have secured their system properly. If you are in the position of being responsible for a control system network, and you have not performed a security evaluation, maybe you shouldn't be sleeping at night.

Some might think that there is no real risk if an HVAC control system is hacked. If a hacker gets into the system what is the worst they could do? Make the occupants complain about the temperature?

What if the building automation system is controlling the temperature in your corporate data center? Might the IT guys be a little angry if their critical computing infrastructure melts down because a hacker turned off the AC and turned on the heat instead? Lost business opportunities would definitely get you the wrong type of attention.

As seen with the Stuxnet[1] attack, hackers might attempt to damage the HVAC equipment. While your BAS might not be controlling a nuclear reactor, the cost of replacing damaged HVAC equipment could be significant.

But how does one go about securing a control system? And, what does it mean for a control system to be secure?

This article outlines a number of threats that should be considered and methods for mitigating those threats. The approaches outlined in this article are protocol agnostic; it does not matter if your control system is BACnet, LON, KNX, Modbus or Vendor A's proprietary network. These solutions will provide a level of security that is acceptable for most installations and will do this with standard IT technologies.

Threats to the System

The most obvious threat is the Internet. It is also the most probable source of attack that your control system will face. If you need to be able to access your control system from afar, odds are you connect to it through the Internet; gone are the days of dial-up connections (well mostly gone, anyway).

The Internet is the most obvious source, but is not the only source of attack. One needs to consider attacks originating from within the facility. In securing the system against unauthorized access from people in the facility, the control system is being protected not just against malicious attacks by people who have gained entry, but also from inadvertent attacks and indirect attacks from compromised computers located behind the facility's firewall, and poking around by curious users that are otherwise allowed to use the facility's computing resources.

About the Author

Carl Neilson is project manager with Delta Controls. He is chair of ASHRAE's BACnet committee (SSPC 135).

Depending on the level of control of entry to the facility, more or less security for the control system will be required inside the facility. For example, ultra-secure military installations might not expend too much effort ensuring security of the HVAC system, since physical access to the facility is tightly controlled and all people that enter are escorted or pre-vetted (assumed to be non-attackers). The opposite would be true for a university where there is no restriction on access, and some students would hack the system just because it's fun, and they learned about control systems in their morning engineering class.

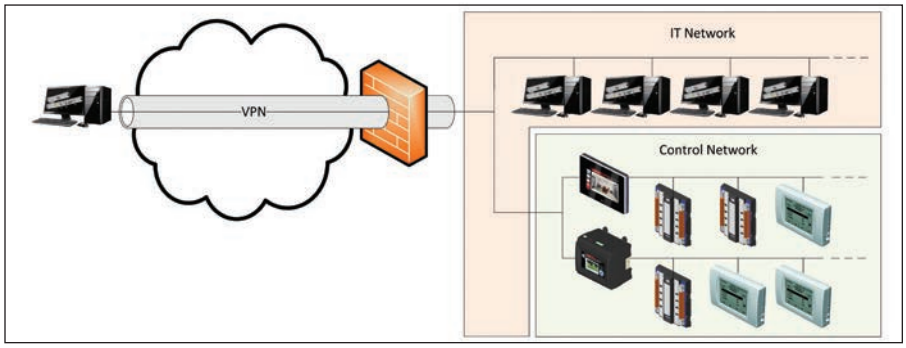

Figure 1: VPN connection.

Protection From the Internet

There are a couple of approaches that can be taken to secure the control network, in all of the cases discussed here, it is assumed that the control system is separated from the Internet via firewall and that there are no ports opened in the firewall that allow access to the control network. Starting from that position, the following approaches all provide good protection: virtual private network (VPN); remote desktop; and control system web server.

VPN

The VPN solution works by providing a secure tunnel from the user's computer through the control system's firewall to the control system network. Once the VPN tunnel is established, it appears to the user as if the computer is connected to the control system network directly. The user then runs any control system software and communicates with the control system through the VPN tunnel. All communications through the tunnel are encrypted, ensuring that no one monitoring the communications can see the data transferred between the user's computer and the control system.

VPN client products come in two main flavors: software clients and hardware clients. With a software client, the VPN software is installed on the user's remote computer, and usually requires that the user enters her user name and password each time she connects to the VPN. In addition, most VPN client software can be configured to require a shared secret, ensuring that only computers configured by the network administrator can connect the VPN.

In contrast, a VPN hardware client is a box that is installed in the remote site giving a full-time VPN connection between the remote site and the control system. This type of setup is common for central monitoring stations that connect to multiple remote control systems, or for connecting satellite offices into a network, or connecting multiple disparate control system networks through the Internet. Benefits of the hardware VPN solution include the ability for an always on connection and a VPN that supports multiple devices (the hardware VPN connects the complete network to the remote network versus the software VPN that only connects the local computer).

Many VPN products are available, including open source and commercial products.

Pros

- Simple to setup
- Inexpensive to deploy
- Secure/private connection
- Allows non-browser based applications access to the control system

Cons

- Vulnerable to attack from malware on computes that connect to the control system network
- Allows any software on enabled computers to interact with the control system

Remote Desktop

The most secure approach is to provide a remote desktop solution. A remote desktop solution restricts the access to the control system network to programs installed on a single computer that is directly connected to the control system. In restricting access to the single computer, control over which programs access the control system is easily restricted through management of the computer. If there is a central IT department that manages computers for the site, they should be able to provide management of the control system computer as well ensuring that security and software updates are applied as available.

In this scenario, a computer is installed onsite directly connected to the control system. The software required to interact with the control system is installed on the computer along with a remote desktop solution. Many commercial and open source desktop solutions exist. Depending on the particular remote desktop solution installed, different ports on the firewall will need to be opened so that the computer can be contacted from outside the firewall. Only those ports that are required for the remote desktop solution should be opened.

Pros

- Secure / private connection
- Better control over computers attached to control system network
- Allows non-browser based applications access to the control system

Cons

• Can be more expensive than other options (if multiple simultaneous connections are needed)

• Can be more complex to deploy

Control System Web Server

Almost all building automation system vendors provide web-based interfaces to their control systems. Providing a web server behind a firewall is better than connecting the control system directly to the Internet, and in most cases will provide a secure solution. Assuming that the control system web server provides a secure method of user authentication, such a product can be used to restrict access to a control system.

The problem with this solution though is that the customer is relying on the vendor's ability to develop a secure product. Experience shows that this is not always achieved.[2,3,4] It is my opinion that this occurs because a control system companies core competencies are not in the security domain, but in the control system domain. If companies that develop security related products have security issues in them,[5,6] companies that are focused on other aspects of their delivered products are more likely to have even more security-related defects.

Pros

• Simple to setup

• Inexpensive to deploy

Cons

• Relies on the control system vendor to develop secure product

• Less likely to be updated than commercially available security products

• Does not allow non-browser based applications access to the control system

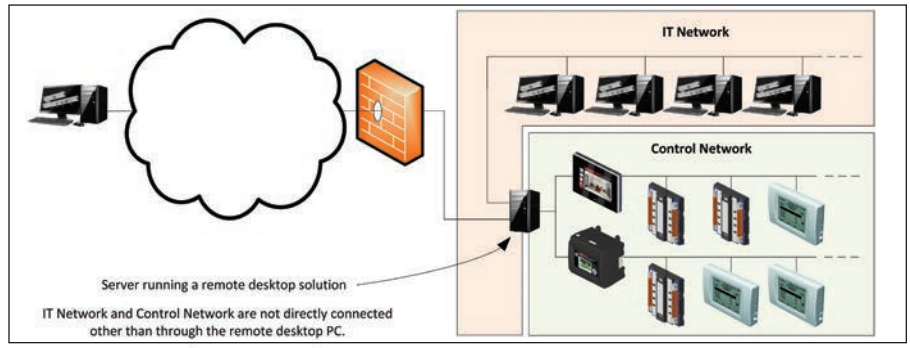

Figure 2: A PC with remote desktop is a useful tool for restricting access to a control network.

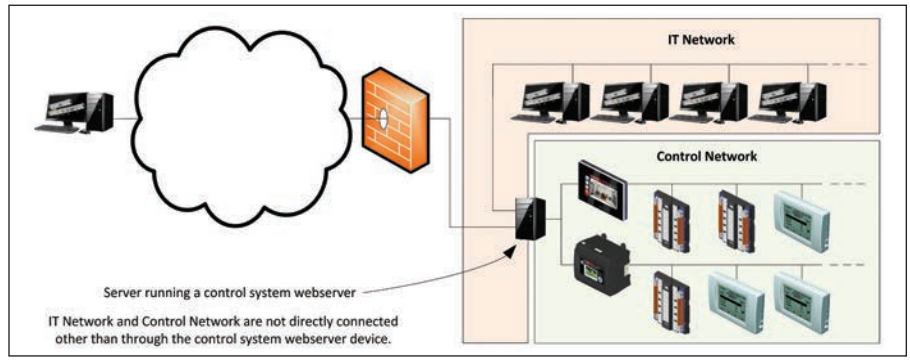

Figure 3: Access only allowed through the control system webserver.

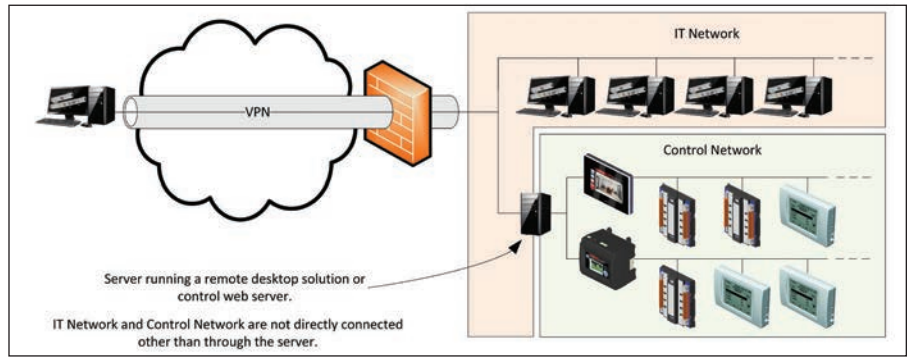

Figure 4: Mixed approach with VPN and control system webserver of remote desktop PC.

A Mixed Approach

Where the control system uses a web interface, that interface can be combined with either a VPN, or a remote desktop solution. The combination of either approach adds the protection of data hiding through encryption and robust security through a commercial security solution.

Combining a VPN with a web server interface provides the benefit of restricting the applications that can interact with the control system. The VPN provides a secure connection to the web server taking away the reliance on the web server's security implementation for user authentication. Having the web server installed on the only computer that has access to the control system network ensures that no other programs are using the VPN to access the control system. This reduces the risk that rogue programs on the user's computer can attack the control system.

Combining a remote desktop solution with a web server does not provide any more protection than using desktop solution with a non-web-based interface. In either case, the effort to secure the control system is reduced through the single computer being allowed access to the control system.

Pros

• More security than a VPN only solution by disallowing access to the control system for programs on the user's computer

Cons

• Does not allow non-browser based applications access to the control system

Protection from internal attacks. Unlike attacks from the Internet, there is no single point of entry within a facility. The result is that more work is required to ensure that the risks are mitigated, and one solution will not address all issues.

Within a facility, there are more people with logical and physical access to networks within the building. Depending on the type of facility the number and variety of individuals with access to the networks within the building will vary widely. In a school there can be thousands of people who are authorized to use the network, and there can be many people unauthorized to use the network but may have easy physical access to it (open network ports, unlocked computer labs, open wireless networks). In contrast many offices have severely restricted access policies making physical access to the network much more difficult for unauthorized users.

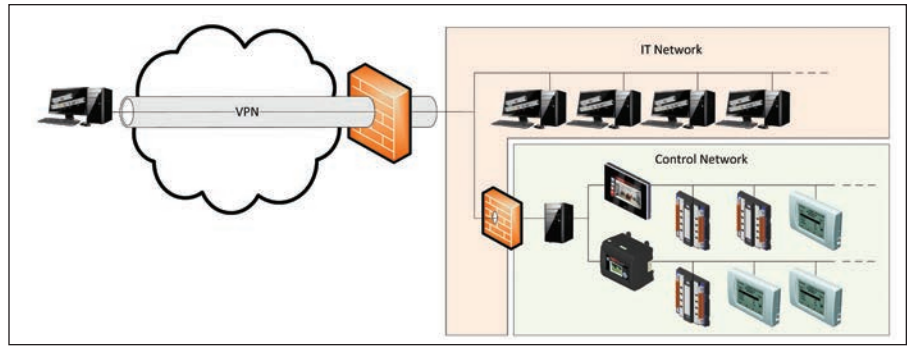

Figure 5: Protect the control network with its own firewall.

If your control network shares the IT computer network, are all of the controllers providing their own security? Is the IT network providing security? Or is the control network open to anyone who can get inside your building?

If your control network is segregated from the IT network, there are still threats. Are there any computers directly connected to the control network? Are there any networked controllers that are in the user space (networked thermostats, supervisory controllers in unlocked closets, etc.?)

Is there any equipment that is outside the building, such as rooftop units? Are there network controllers attached to the exposed equipment? If an attacker can get access to a controller, the attacker can probably take over the controller's connection to the network.

When deciding which of the mitigations to employ, one should evaluate the likelihood of the threat occurring, and the possible adverse impact. In some cases the likelihood and/or the impact is too low to warrant the effort.

Segregate the control network from the IT network. Segregation from the IT network reduces the attack points for a control network. To start, it means that users on the IT network do not have carte blanche access to the control network. It also ensures that slipups in security on the IT network have a reduced chance of impacting the control network.

Segregation can be achieved through IT technology (VLANs and managed switches) or through physical separation. While some costs can be reduced by using the same infrastructure, using a completely separate network also has advantages. The controls industry seems to be split when it comes to whether to share IT infrastructure or to provide a completely separate physical network. From a security perspective, providing completely separate infrastructure can be the better choice.

With seemingly constant changes to IT networks, each change is a source for the introduction of security holes. It is not uncommon for IT to forget that there is even a control network installed (until their equipment loses its AC) and that changes they make can cripple a control system network. Having a completely separate infrastructure reduces the probability that the day-to-day changes made to the IT network will negatively impact the control network.

That said, keeping separate infrastructure can mean that those operating the control system will need to supply their own network support, or convince IT to operate the network but to keep it separate. Being a building operator does not usually mean that one is skilled in maintaining a computer network. The IT department can provide support for an Ethernet/IP related network segment, but they most likely have no training when it comes to the other network technologies that control systems use (control system specific routers, other network media, etc.).

Once segregated, the connections between the corporate network and the control network can be limited and protected with firewalls.

Treat the IT network as hostile as the Internet. Once the control network is segregated from the IT network, treat the IT network as hostile. Protect the control network from the IT network using one of the solutions that would be used for protecting it from the Internet.

Turn off unused network ports. If there are connection points to the control network that are not used, or which are provided solely for service tools, ensure they are turned off when not in use. Do not make it easy for an attacker to connect into the control network by leaving a spot on the wall he can plug into.

Use simple sensor networks for controllers in the user space or apply network security on sensor networks. Any equipment that is in the user space (i.e., in the occupied portion of the building instead of in mechanical rooms or locked in cabinets), should be separated from the main control network. The most common controller found in the user space is a smart thermostat. An attacker can pull it off the wall, and plug in a computer to gain access to the control network.

The simplest method to protect against stealing a smart sensor's network connection is to use a simple sensor network instead of more powerful network, or use dumb sensors in the space and leverage the intelligence of supervisory controllers.

Or simply install secure products. There are some options available for secure user space smart sensors, but they are not the norm.

Provide users with individual usernames and passwords. A common approach to HVAC control user authorization is to share a single login credential. People will be less diligent with their login information if everyone has access to the same cre-

dential. And, if a security incident does occur, there will be less audit trail information to evaluate.

When users no longer require access to the control system, remove their login credentials.

Remove default usernames and passwords. Most control system products come with default usernames and passwords to allow for initial system configuration. These default login credentials should be removed.

Ensure the use of strong passwords. Since IT is not usually responsible for software on the control network, frequently IT password policies are not enforced on control network. While no users enjoy having the change their passwords, or having to remember yet another password, if a strict password policy is required to protect the IT network, why would it not also be in place to protect the control network?

Ensure that control system security patches are up to date. Any control system product reachable from the IT network should have security patches installed. Many control system products are based on common operating systems, web server applications, and protocol stacks. Security patches for these products should be field tested and then installed.

Install tamper alarms on all equipment cases. For the really paranoid who have to protect against malicious insiders with access to roam about the facility and into mechanical rooms, the installation of tamper alarms on all equipment cases can provide an indication not only when someone might be physically damaging equipment, the tamper alarms also provide a warning that someone might be attempting to take over the network connection of a device.

If your site has tamper alarms, don't ignore them. When one goes off, physically inspecting the unit is required.

Take the Time

Take the time to evaluate your needs, your budget and your level of risk tolerance then select the approach that best suits your situation. And remain vigilant; revisit the security of your control network regularly to ensure that it remains secure.

References

1. Wikipedia. 2013. "Stuxnet." http://tinyurl.com/mc3cypd.
2. Donohue, B. 2013. "Researchers Hack Google Office's Building Management System." 7 May. http://tinyurl.com/mk2s4ue.
3. FBI Cyber Alert Network Division. 2012. "Vulnerabilities in Tridium Niagara Framework Result in Unauthorized Access to a New Jersey Company's Industrial Control System." http://tinyurl.com/lr5rs84.
4. Menn, J. 2013. "Researchers warn of cyber flaws in Honeywell control systems." Reuters, 5 February 2013. http://tinyurl.com/lzwnugc.
5. Krebs, B. 2013. "Backdoors Found in Barracuda Networks Gear." Krebs on Security. 24 January. http://tinyurl.com/kqvtgs2.
6. United States Computer Emergency Readiness Team. 2013. "Cisco Releases Security Advisories." 25 April. http://tinyurl.com/cn6f3qq.
7. Krebs, B. 2010. "Experts Warn of New Windows Shortcut Flaw." Krebs on Security. 15 July. http://tinyurl.com/2668tfx. ■