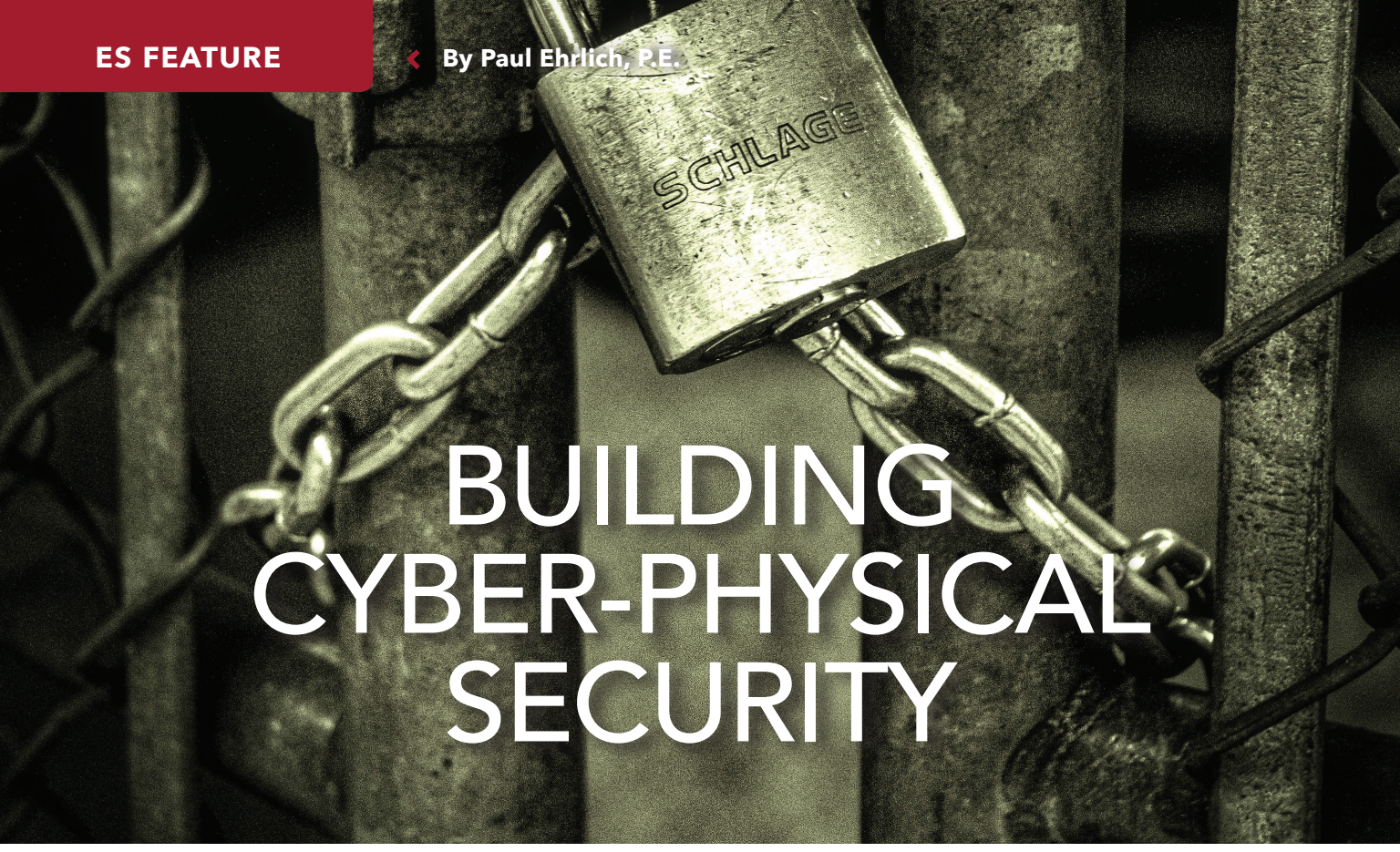
By Paul Ehrlich, P.E.



BUILDING CYBER-PHYSICAL SECURITY

The rewards may not be flashy, but the risks cannot be ignored. Survey the range of issues, from basic physical access to updated standards.

Cyber attacks are becoming more common and brazen. You may already have been a victim of one of these attacks and only find out when your credit card company calls to asks about suspicious activity. Many of the attacks that are in the news are focused on obtaining "personal identifiable information" such as credit card numbers, bank accounts, and social security numbers. But there is a whole other target for these cyber criminals, and that is the area of cyber-physical systems including industrial control systems, infrastructure controls such as the electrical grid, and even controls for building systems. While not as well publicized as financial and personal information attacks, both are a very real risk and a clear and present danger.

Historically, there was little risk of someone attempting to take over a building control system. Systems were largely mechanical (i.e., pneumatic), and when they moved toward digital technology tended to be islands of proprietary systems. But today it is much more common for a control system to be highly integrated, follow open standards, and be connected to networks and the internet. There are numerous benefits to these new systems, including the ability to do much better control, monitoring, operations, and even analytics and optimization. But the downside is that as these systems become a more compelling target for cyber attacks, potentially endangering the reliability and resilience of building systems and other critical infrastructure systems.

ATTACK SCENARIOS

In order to evaluate the potential risk of a cyber-physical attack on a building, you need to put yourself in the place of a cyber attacker. What motivates these folks? Why do they do what they do? The answer to this is varied and complicated. Attackers range from those who are merely curious and are pushing to see what they can find, to those who are looking to create havoc, to criminal or state-sponsored cyber attacks intended to cause financial or physical damage. An even bigger challenge is that with the availability of information online an attacker does not necessarily even need to be technically astute. Attacks can be perpetrated by "Script Kiddies," who may be able to download existing tools from the web and, with very little programming expertise, gain access to a system.

There are several potential approaches that a cyber attack on a building could take. One approach is to access the system and use it as a way to get into or attack other systems. Such an attack occurred last year and involved placing a program (called a Bot) on thousands of internet connected video cameras and DVRs. These were all triggered to send messages to a site at one time (called a denial of service attack) that caused major havoc to numerous websites. This same approach could be used to exploit a weakness in a control system and then attempt to use that entry point to get into a connected business system. There was broad speculation that this was the approach used to gain entry into the credit card system for a major retailer, although it turned out that the attackers had used a contractor's access for a work order system to gain entry.

A second approach is to attempt to get into the control system and disable, or override, normal controls operation. You can readily imagine potential scenarios for how this could cause problems in a building. Many of these potential changes could result in being no more than minor nuisances that could easily be dealt with by facility operations. For example, changes to zone setpoints or schedules would probably result in calls to building management, who could easily override the system and return it to proper operation. But others could have the potential to be very destructive — especially if they resulted in damage to mechanical equipment. Imagine an attack that cycled equipment on and off continuously or one that set equipment to values outside of where it should be operating. The potential risk of impact from this type of attack will vary proportionally with the criticality of the building. For example, changing the building static pressure setting for a low-rise office building might keep the lobby doors from closing fully, while that same change in a hospital operating room could have a devastating impact.

A third potential attack would be to get into a control system and make changes that would either erase existing programming or perhaps just remove access for operations. That type of attack could be used potentially for financial gains by an attacker who then would ransom access to the system.

There are likely many other potential scenarios and attack vectors that could be used by cyber attackers. The most worrisome is likely some form of coordinated attack that might go after a large group of resources at one time. The risk of potential attack is very real, and it is prudent to be designing and operating buildings with the need for cyber-physical protection in mind.

UNLIKELY (BUT NOT IMPOSSIBLE) BUILDING RISKS

Many movies and TV shows portray a hacker (or law enforcement) who is able to readily gain access into a building's systems and override the security system, elevators, sprinklers, and fire alarm. While none of this is impossible, it may be improbable. Many of the controls used for these systems remain largely thermal or mechanical such as fire sprinklers. Others are very proprietary and are not integrated to either other systems or the internet.

Finally, many systems still have mechanical safeties. For example, most boiler controls still have hardwired high temperature and pressure safeties that will shut off systems even in the event of a software override. Systems should be designed with security in mind, employing good design practices such as the use of distributed controllers and hardwired protection.

But keep in mind that protecting a building's systems is a matter of both cyber as well as physical protection. Control systems can be properly protected, but that may not prevent an attacker from entering a mechanical room and manually overriding or disabling systems. Proper access protection and monitoring of mechanical and electrical equipment rooms is a key part of providing cyber-physical security.

BEST PRACTICES TO PROTECT BUILDING SYSTEMS AND CONTROLS

There are a series of best practices that have evolved over the years to help building owners and designers protect systems against a cyber attack. Some of the basics include:

- Physical access. Just like locking your car or your house, the first deterrent to any sort of cyber-physical attack is blocking physical access. For buildings, this means protecting access to both physical assets as well as access to cyber assets. Physical assets include making sure that electrical and mechanical rooms are protected. It also means that the BAS console on the operator's desk is only logged on to the system when they are at their desk and using that system. Cyber access includes limiting access to data rooms, switch closets, etc. Best practice is to both limit access to these areas and also to make sure that the switches and other devices are in locked cabinets within these rooms.
- Password control and protection. One of the greatest security holes in any system is through the "front door" by simply entering in a default user name and password (or perhaps the one written on a post it note on your monitor?). Make sure that you set up unique user names and passwords and that these are regularly updated especially when there is a change of personnel. Ideally, the control of user credentials is done through the IT system so that it can be properly maintained. Many control systems are able to support industry standard password management systems such as LDAP and Active Directory that make the management of these credentials easier to do and more secure. Proper setup and configuration are one of the key tenants for security.
- Use of VLANs. One of the most important things to do for any control system is to provide protection when it is connected to the network. There are two approaches that are broadly used for network support. One is to use a dedicated facility network, and the second is to use an existing Enterprise Network that is already in place. There are pros and cons to both of these approaches, but both approaches require careful attention to providing the proper attention to security.

For a dedicated network, care is needed for monitoring the network and managing how it is connected to the internet through an ISP. For an enterprise network, the best practice is to utilize a "Virtual Local Area Network" or VLAN. The VLAN is configured and managed by the network switches and limits which switch ports can see and communicate with others. Most VLANS will only allow a recognized device (such as a controller or PC) to even connect to the network. Setting up and managing a VLAN generally requires an IT professional, and while a VLAN does not provide perfect protection, it does significantly help protect a control system from access from potential cyber attackers.

- Firewalls and network protection. Connecting building control systems to the internet provides numerous benefits in being able to remotely access systems, as well as collecting data for analysis and improved operations and efficiency. But connecting to the internet provides a potential portal for cyber attack. When systems connect to the internet, they can and should be protected using a firewall. There are many commercial firewall products available today that range from what comes built into a residential-grade router to enterprise class solutions. There are also several products specific to building automation available that manage the connection to the internet and also allow for secure remote connections. The use of a firewall is essential for any internet connected system.
- Identifying and reacting to an attack. The final best practice is to be aware of when an attack is occurring and have a plan for how to react. The key to being aware is to be actively managing the network, looking at traffic, and being able to identify when something out of normal is occurring. Perhaps the easiest and most effective way to accomplish this monitoring is to utilize an enterprise network and request that your organization's IT professionals monitor and manage the network. It is also possible to monitor traffic on a dedicated facility network, but it does require having the expertise to look at network activities and dedicating the time necessary to do so.

FUTURE EFFORTS

Even with today's best practices in place, there is no question that the control systems in commercial buildings are at risk for a cyberattack and need to be better protected. This is a key topic that is related to research and development efforts currently under way and starting over the next few years. Here are some of the key efforts underway or needed in this area.

UPDATES TO OPEN COMMUNICATIONS STANDARDS

One of the goals of open control protocols is to make it easy for controllers to share information with each other. Many control protocols such as

BACnet, Modbus, and LonWorks were developed with the assumption that they would be used on a closed controls network and included little if any form of encryption or network security. But over the years, control networks have evolved to utilize both dedicated and shared enterprise and public networks. This introduces the potential for a cyber attacker to get access to the network and potentially view communications and even issue valid commands to read and write information.

One solution to this issue is to update standards to include network security which includes encrypting data as it travels across the network and establishing a method where only "trusted" commands are followed. Methods to achieve secure network communications have already been well defined by other industries. For example, when you do an online financial transaction with your bank, the data is encrypted (look for the little lock in your browser window). There are also well established methods to generate and validate digital identity. In 2010, the BACnet standard was updated to include an optional method for network security. This included a method of authentication as well as data confidentiality. Unfortunately, few, if any, BACnet products are currently supporting this option. The BACnet committee is continuing to work on updating options for security using the latest technology and is preparing to release an improved security option for public review called BACnet Secure Connection. Vendors seem optimistic about delivering products that may use this new standard, but requests for improved security from owners, operators, and design engineers will influence if and when these new options are available in control systems.

RESEARCH ON CYBER SECURITY

The topic of cyber-physical security is very dynamic and evolves with new technology and a continued effort to circumvent it. There is a large-scale research agenda required to support these efforts. This work is being conducted globally across government labs, universities, and industry. Some examples of research efforts that are ongoing in this area include:

- Security frameworks. Work to develop agreed-upon frameworks for evaluating and protecting systems are one of the first steps in providing improved cyber-physical protection. These frameworks are architectures that can be used across industries and applications to assess the level of protection available.
- Tools for evaluation and detection. With continued and ongoing threats against all forms of systems and networks, it is necessary to not only have a form of protection but also of detection. If you think of your home, the lock on your front door is good protection against a burglar, but a security system is used to detect and notify when there is an intrusion. New tools will be able to evaluate networks for possible issues and analyze network traffic to determine if an attack may be imminent.
- New methods of security. Just as networks and the devices connected to them continue to evolve, so do the methods to provide protection. One interesting new tool being used for security is "blockchain." Distributed blockchain was first developed for use as the accounting system for the crypto currency bitcoin. Blockchain serves as the distributed ledger used for accounting for bitcoin transactions. Since the blocks are linked using cryptography, they can be used as distributed ledgers for numerous purposes including improvements in cyber-physical security.
- Managed security services. There are already a number of suppliers offering a managed service for accessing and protecting control networks. Look for this to be an area of increasing interest and development as new solutions and standards evolve.

CONCLUSION

Here are a few key items to keep in mind regarding the topic of cyber-physical security of building systems.

- The risk is very real. There are bad folks out there who are trying to cause problems, and once into your system, they can cause havoc.
- Protection needs to be balanced. Making a building control system robust and reliable is critical. But these protections need to be balanced against the purpose of the system which is to provide a tool for improved building operations and efficiency. Providing protection in a way that reduces functionality may be shortsighted.
- Follow best practices. Make sure you provide physical security to mechanical spaces. Log out of your system when you aren't using it. Manage user names and passwords. Work closely with your IT staff to implement tools including VLAN, VPN, and firewalls.
- Support standards and research efforts. There is a lot of work going on in this area. But what helps bring the work that is done in research and standards organizations into reality is customer demand. The more owners, operators, and designers demand solutions which are both open and secure, the sooner industry will work to help bring these solutions from the research labs onto the market. **ES**

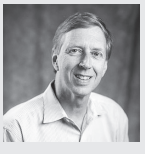
DEPARTMENT OF ENERGY (DOE) RESEARCH ON CYBER-PHYSICAL SECURITY

The DOE is actively involved in researching new tools to help in evaluating the risks of cyber-physical attack and in improving control systems for more reliable operations. Work on this topic at the Pacific Northwest National Laboratory (PNNL) has included both a security framework and tools to assess an organizations control systems. These tools are easy to use online surveys that provide instant feedback.

See https://bc2m2.pnnl.gov/ for the online assessment tool.

IS MY BAS EXPOSED TO THE INTERNET?

Good question — but also one that is easily answered. There is an online search engine that goes out and searches for all types of control systems that are on the internet. This site called Shodan (www.Shodan.IO) "crawls" the web looking for control systems and allows users to readily search for systems. For example, searching on "BACnet" shows 7,500 sites that have been found by Shodan. Running a Shodan search for your building or system is a good first step in evaluating the security of your system. Note that just being identified by the search engine does not necessarily indicate a vulnerability, but it does indicate that your site is visible on the web.



PAUL EHRLICH, P.E.

Paul Ehrlich, P.E. is a program manager for the Pacific Northwest National Laboratory with a focus on projects related to building energy efficiency, advanced controls, and building to grid integration. Prior to joining the lab he was the president of Building Intelligence Group LLC, an independent consultancy whose primary purpose was to support and promote the delivery of high-performance buildings. Services included systems assessment, master planning, training, and design for intelligent and sustainable building systems with a focus in the areas of integrated systems, facility operations, and enterprise management. Paul has a bachelor's degree in mechanical engineering from the University of Wisconsin and a master's of business administration from the University of St. Thomas.