InTech®
A PUBLICATION OF THE INTERNATIONAL SOCIETY OF AUTOMATION

Six steps to control system cybersecurity

By Lee Neitzel

Securing your automation systems does not have to be a complex undertaking

FAST FORWARD

- The main goal of automation system security is maintaining safety and availability, primarily by preventing the intrusion of foreign software, such as malware and viruses.
- This goal can be attained by following the six steps derived from converging ISA/IEC/WIB standards and detailed in this article.
- End users can ease the hardening of their systems during implementation and on-going maintenance by partnering with certified hardware vendors, software suppliers, and service providers.

If you are like most process automation professionals, you are aware that your automation systems are not as secure as they should be, and you would like to make improvements. But you are somewhat confused by all the industry chatter regarding security and standards, and you are looking for a clear path toward improvement, minus the hype and scare tactics.

The main objective of control system security is to keep the plant safe and to keep production running. In contrast, IT security focuses on protecting data, such as credit card numbers, from being stolen. The primary threat to both of these goals is the infiltration of malicious software into the system.

Malicious software normally infects a system by 1) using file transfer mechanisms, such as file shares and the file transfer protocol (FTP), 2) exploiting vulnerabilities in network-facing software that allow code to be injected into the system, and 3) the automatic copying of files from portable media, such as USB sticks, CDs, DVDs, and cell phones to the system.

There are six steps that you need to address this threat. These steps are taken from emerging NIST, ISA, and industrial cybersecurity standards that are being integrated into a single international IEC standard [IEC 62443]. They define not only the security mechanisms needed in a control system, but also the supplier capabilities needed to harden the system at the site. In addition, certification programs are now in place to certify suppliers against these standards. Standards activities are summarized after the steps to security are described.

Before beginning these steps, you should make sure that you have security policies for the control system. IT departments all have security policies that you can review if you do not have one yet for your control system. Your security policies should support each of the steps below and be geared toward keeping unauthorized software off your system.

Six steps to security

The steps that follow reinforce the concept that security cannot be accomplished just by buying a control system with the right security features. They emphasize that security is just as much a process as it is technology. Following these steps not only addresses the malicious code threat, but also other attacks that threaten control systems.

These steps can be implemented in an evolutionary fashion so that security improves over time. The evolution of security is defined by a maturity model specified in the IEC standard. It should encourage you to start down the path to security, rather than thinking security is just too ominous and complicated to address. Adoption of these new security standards is going to be like the painful adoption of seatbelts that we all went through, from initial denial of the need to finally recognizing the benefits.

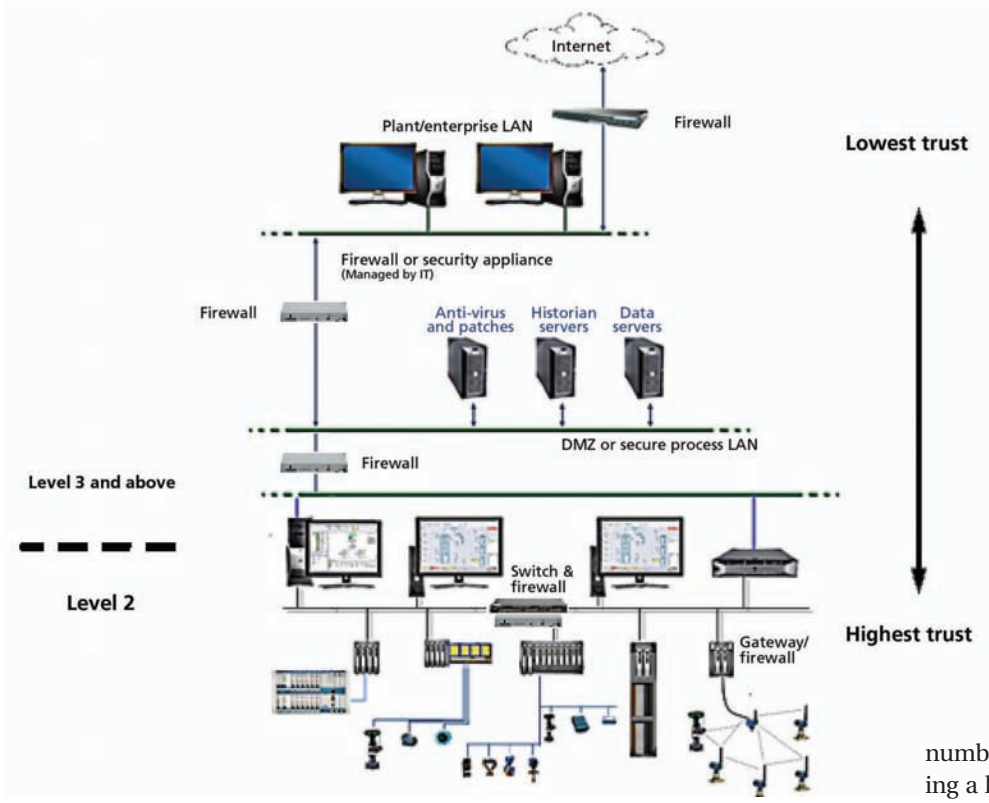
Step 1: Network security perimeters

Step 1 involves establishing network security perimeters to restrict access points where foreign software can enter the automation system. As shown on the following page, in a typical control system plant/enterprise networks are at Level 3 and above in the Purdue model, while the control system networks and buses are at Level 2 and below.

Firewalls are used to segment the control system internally and to isolate it from Level 3 and other external networks. You must ensure that all traffic to/from the control system is encrypted and passes through at least one firewall. Further, under no circumstances should any Level 2 workstation be granted direct access to the Internet, or have an IP address that allows it to be directly accessed from the Internet.

Within the control system, firewalls should be used to protect controllers, wireless device networks, and SIS networks from Level 2 workstations. In addition, switches with lockable ports should be used to prevent unauthorized devices from connecting to the control system. These firewalls and switches, in conjunction with the Level 3/Level 2 firewalls, create a layering of security perimeters with the lowest degree of trust attributed to Level 3 and the highest level granted to Level 1.

Components that are not as critical to safety and availability, such as historians and data servers, should be installed at an upper level in the hierarchy, with less protection, but correspondingly more access, so that plant personnel can view data and make changes as needed.



Once the firewalls and smart switches are installed, they must be maintained throughout the lifetime of the system to keep their effectiveness from degrading. Firewall rules must be kept current to reflect changes to IT and control systems and to protect against newly discovered threats. Unused switch ports must be regularly checked to make sure they are still locked.

Step 2: Workstation hardening

Step 2 involves hardening control system workstations to make it more difficult for malicious software to find a way into the system. Five primary hardening activities should be performed. First, the Center for Internet Security (CIS) hardening template should be applied to lock down the workstation's security policies.

Second, these workstations should be dedicated to operator and engineering functions, and, as such, all applications, services, and ports that are not needed to support these functions should be removed or disabled to prevent vulnerabilities they may have (known or unknown) from being exploited.

Third, anti-virus software should be installed to detect and delete known malware before it can infect the workstation. In addition, virus definition files should be kept up to date to keep up with new viruses that are circulating.

Fourth, the file system should be configured to permit only authorized users to access sensitive files. The default, unfortunately, is to allow users with administrator privileges to access all files on the workstation. These users should be carefully analyzed, and they should be granted access only to files/directories that they need.

Fifth, USB, CD, and DVD drives should be locked down when not used for authorized purposes. Additionally, users should be reminded that using portable media is a common way of infecting a system. It is not unheard of for an attacker to drop infected USB sticks in the parking lot and hope someone will pick one up and plug it into the workstation.

Finally, these hardening activities can be supplemented by one more: regular reboot of the workstation to protect against memory-only infections. Some of the more sophisticated attacks involve installing memory resident malware that is hard to detect. Workstations that are targets for this type of attack are those that run 24/7. Rebooting these workstations when time permits will remove this type of malware.

Step 3: User account management

Step 3 involves managing user accounts. Users should be given only the privileges that they need, and their passwords should be sufficiently long and require the use of a combination of three of the following four: upper and lower case letters, numbers, and special characters. Granting a limited set of privileges should reduce the ability of foreign software that has infected a user's program from using elevated privileges to perform some malicious act – a very common technique used by malware.

Using complex passwords makes it significantly harder for hackers to guess passwords or to reverse engineer password files should they gain access to them. In addition, password policies should be set to cause passwords to expire regularly and to prevent the reuse of previous passwords, generally the last three. Protecting passwords not only protects against malware gaining access to the system, but also protects against hackers logging onto the system.

Using complex passwords makes it significantly harder for hackers to guess passwords or to reverse engineer password files should they gain access to them.

If malware is running in a user's program and is able to acquire the password of an administrator, it may use that password to elevate privileges of that program or to start another program using administrator credentials. These techniques are commonly used by malware to elevate its privileges.

Step 4: Security updates

Step 4 is making sure that security updates (patches) for both operating system and control system software are kept up-to-date. These updates remove vulnerabilities that can be exploited to infect the software containing the vulnerability. Free tools can be found on the Internet that allow hackers to search a workstation for vulnerabilities and then automatically inject malicious software that provides cmd.exe shell access to the workstation or that allows custom hacker code to be downloaded to the workstation and run.

Of course, updates should be approved for the workstation so they do not disrupt workstation software. Certified suppliers are required to validate all security patches for operation on their systems.

Step 5: Backup and recovery

Step 5 involves implementing a backup and recovery plan. An effective backup and recovery plan allows an infected system to have its configuration data and software restored to an uninfected state. Certified suppliers are required to have a backup and recovery strategy that specifically recommends when and how to recover a system to a stable state even if there is no evidence of infection. This is important since sophisticated malware often hides itself from detection and can sit dormant until the right time.

Step 6: Security monitoring and risk assessment

Step 6 involves monitoring the system for suspicious activity and performing risk assessments. Security monitoring packages examine logs of workstations, firewalls, switches, and devices for evidence of foreign software. Some monitoring packages inspect network traffic, as well as processor and memory usage, looking for anomalies. In the absence of automated monitoring packages, manual review of event and network traffic logs should be performed to look for suspicious activity, such as an unexpected increase in network traffic, particularly at odd hours.

Risk assessments should be performed during initial design, prior to handover, and during the maintenance cycle of the system to ensure that changes to the system have not been introduced that weaken security. Actions taken after a risk assessment may include new firewall rules, new switch ports to lockdown, stronger password policies, removal of unused software programs, and better procedures for managing the connection of external devices like USB memory sticks.

The industry is converging on the IEC 62433 standard.

Converging standards simplify compliance

In the past, a number of different groups worked independently to formulate security standards, but these groups have come together to create one common standard, which will greatly simplify implementation and compliance. NIST is also participating in this effort, whose participation has been reinforced by the 12 February 2013 Executive Order entitled "Improving Critical Infrastructure Cybersecurity."

ISA created the ISA99 project, *Industrial Automation and Control System Security*, ten years ago to develop a comprehensive suite of security standards for the automation industry. Their work has been submitted for IEC standardization as IEC 62443.

In parallel, the International Instrument Users' Association, referred to as the WIB after its original Dutch name, created a security standard for best practices of control system suppliers. This standard complements the ISA-99 suite and has also been accepted for standardization within the ISA-99/IEC 62443 series.

Still in parallel, two device level security certification standards have been developed: ISA SecureDevice and Wurldtech's Achilles Communication Certification. These standards are also being integrated into the ISA-99 IEC 62443 series.

In summary, the industry is converging on the IEC 62433 standard. This standard will provide a very comprehensive set of standards for industrial cybersecurity that includes standards for organizations, control systems, components, and deployment/maintenance. Existing certification programs will continue, but these will reference the IEC 62443 standards rather than their own separate specifications.

Conclusion

Industrial security is more than just hardware and software. Project and support personnel have a responsibility to promote security awareness at the site and to ensure that they are capable of hardening a control system according to the security policies of the site.

Emerging standards, converging within IEC 62443, provide requirements for manufacturers of control systems/components and for suppliers of deployment and maintenance services. Within the context of IEC 62443, security programs go through an evolutionary process that allows them to mature.

Finally, a number of suppliers have achieved certifications that reflect their commitment to control system security. The use of certified suppliers and service providers can cut costs, reduce risk, and quicken compliance – both during implementation and over the entire life cycle of the automation system.

ABOUT THE AUTHOR

Lee Neitzel, senior engineer at Emerson Process Management in Austin, Texas, has been involved in security and network standards for more than 25 years, having worked on IEEE 802, FDDI, Fieldbus Foundation, and OPC standards. He is currently the IEC project leader for integrating the WIB "Process Control Domain – Security Requirements for Vendors" specification into the IEC 62443 and the ISA-99 security standards.

Resources

Defense in Depth
www.isa.org/link/DefenseinDepth

Control Network Secure Connectivity Simplified
www.isa.org/link/controlnetwork

ISA99 examines standards' strength against Stuxnet-like attacks
www.isa.org/link/ISA99