Cybersecuring Healthcare Building Control Systems

By Michael Chipley, PhD

Healthcare facilities are some of the most complex structures ever built; yet, they are a system of systems that are notoriously easy to hack. As the use of the Internet of Things (IoT), cloud/mobile computing, medical devices and personal sensors continues to grow exponentially, cybersecuring this multitude of converged healthcare systems presents challenges that will require novel solutions, innovation and organizational culture change.

While hacking these systems is notoriously easy, defending them and ensuring they operate and perform their functions are exceptionally difficult. Creating an organizational cybersecurity culture and employing basic cybersecurity practices are the first steps to cybersecuring a healthcare facility's technological systems.

Information Technology and Operational Technology Convergence

The 2013 Target data hack and other recent events have brought increased attention to the network connectivity of facilities operations and maintenance vendors, an organization's business information technology (IT) systems and its facility/building control systems. Building control systems are physical equipment-oriented technologies and systems that actually run plants and equipment. These include devices that ensure physical system integrity and meet technical constraints. They have event-driven and often real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout a healthcare infrastructure to meet numerous, and often conflicting, safety, performance, security, reliability and operational requirements. Building control systems' key components—including building automation systems (BASs), fire alarm systems (FASs), physical access control systems (PACs), closed-circuit television (CCTV), utility meters and more—have become digital- and Internet protocol- (IP) enabled.

Within the controls systems industry, building control systems often are referred to as operational technology (OT) systems. Historically, the majority of OT systems were proprietary, analog, vendor-supported—and not IP-enabled. OT systems use human machine interfaces (HMIs) to monitor the processes vs. graphical user interfaces (GUIs) for IT systems. Most current building control systems and their subsystems are a combination of OT and IT, and serve as an entry point into an organization's other IT systems.

IT is about data; OT is about controlling machines, and OT is becoming increasingly IP-based. Smart Grid, Smart Cities, Smart Buildings, Smart Cars and IoT are redefining the boundary between IT and OT. As OT systems and components become digital- and IP-enabled, the interconnections to an organization's network and business systems begin to expose that organization to significant vulnerabilities. IT and OT systems are converging; so are the risks and vulnerabilities of hacking and using OT systems as a point of entry to take control of other system assets. "Figure 1" *(see below)* compares IT and OT systems.

Cyber-Physical Systems

The National Institute of Standards and Technology (NIST)[1] is beginning to classify the hybrid IT and OT as cyber-physical systems (CPSs). CPSs are defined as integrated, hybrid networks of cyber and engineered physical elements, co-designed and co-engineered to create adaptive and predictive systems and respond in real-time to enhance performance. CPSs are enabling a new generation of "smart systems." Essential CPS characteristics include:

- Treating cyber, engineered and human elements as integral components of a total system to create synergy and enable desired, emergent properties.
- Integrating deep physics-based and digital-world models to provide learning and predictive capabilities for decision support (e.g., diagnostics, prognostics) and autonomous function.
- Providing systems engineering-based open architectures and standards for modularity and composability for customization, systems of products and complex or dynamic applications.
- Using reciprocal feedback loops between computational and distributed sensing/actuation and monitoring/control elements to enable adaptive multiobjective performance.
- Networking cyber components for scalability, complexity management and resilience.

The vast majority of devices have been designed with little to no built-in cybsecurity capability, and many of the current generation devices have hardcoded firmware and passwords.

	Information Technology (IT)	Operational Technology (OT)
Purpose	Process transactions, provides information	Controls or monitors physical processes and equipment
Architecture	Enterprise-wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (custom)
Interfaces	GUI, Web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
Ownership	CIO and end-users	Engineers, technicians, operators and managers
Connectivity	Corporate network, IP-based	Control networks, hard-wired, twisted-pair and IP-based
Role	Supports people	Controls machines

Figure 1: Comparing IT systems vs. OT systems.

Cyberattacking a Healthcare System

A cyberattacker can exploit a healthcare system through many attack surfaces and vectors, including the following:

- *Traditional healthcare IT (web services, accounting, email, electronic health records, etc.)*. Cyberattacking traditional IT systems happens by gaining access via a phishing, spear phishing or whaling campaign. Tools are used to penetrate the system, elevate privileges, maintain persistence, cover tracks and exfiltrate data. Organizations should conduct penetration testing of the IT and OT systems on an annual basis. The SANS Institute provides penetration testing guides, rules of engagement and scope worksheets and templates.[2]
- *Facility/building OT control systems (BASs, PACs, FASs, EMSs, etc.)*. While these control systems use a combination of traditional IT protocols, such as transmission control protocol (TCP) and user datagram protocol (UDP), they also use unique building control system protocols. Unique protocols include Modbus, BACnet, LonTalk and DNP 3 to communicate with sensors, devices and actuators. Unfortunately, many system integrators and owners have direct Internet-facing connections to building control systems and minimal cybersecurity organizational practices in place. One search engine has written exploits specifically for control systems.
- *Medical devices and equipment (imaging, pacemakers, infusion pumps, etc.)*. In the healthcare environment, the cybersecurity challenges become even more complex as the number and types of medical devices and equipment (MDE) become connected to the Internet with little or no cybersecurity capabilities. Many MDE, similar to building control systems, have embedded passwords in the hardware and firmware. A 2013 security alert from the U.S. Department of Homeland Security (DHS) illustrates the scope and magnitude of the problem: "The affected devices have hard-coded passwords, which can permit privileged access to device passwords. In some devices, this access allows critical settings or device firmware to be modified. … [The DHS Industrial Control Systems Cyber Emergency Response Team] ICS-CERT recommends device manufacturers, healthcare facilities and users of devices take proactive measures to minimize the risk of exploitation of this and other vulnerabilities."[3]
- *Personal sensors (watches, phones, fitness bands, etc.)*. Concerns noted for medical devices and equipment also apply to this category.

Protecting and Cybersecuring Healthcare Building Control Systems

Traditional IT systems have standards, such as the Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPPA). These standards help ensure cybersecurity and provide IT staff with tools and training to manage these systems.

NIST is a primary source of IT cyber standards and guides. The NIST SP 800-37 and NIST SP 800-53 R4 publications, SANS' top 20 security controls and the International Organization for Standardization (ISO) standards are used by both government and industry as IT best practices. On the OT side, ISA 99 from the International Society of Automation[4] and NIST SP 800-82 R2 provide the standards and guides for industrial control systems. NIST SP 800-82 Rev 2 also has new security controls for acquisition, life-cycle software development, penetration testing and continuous monitoring.

Physical security specialists, facility engineers and managers, IT staff, system integrators and property owners should cohesively develop system security plans, including an IT/OT systems baseline risk assessment in planning and design phases and the factory acceptance testing in the construction phase. Furthermore, full site acceptance testing should include penetration testing for system turnover.

Facility owners and operators also need to utilize penetration testing tools.

Continued on page 34

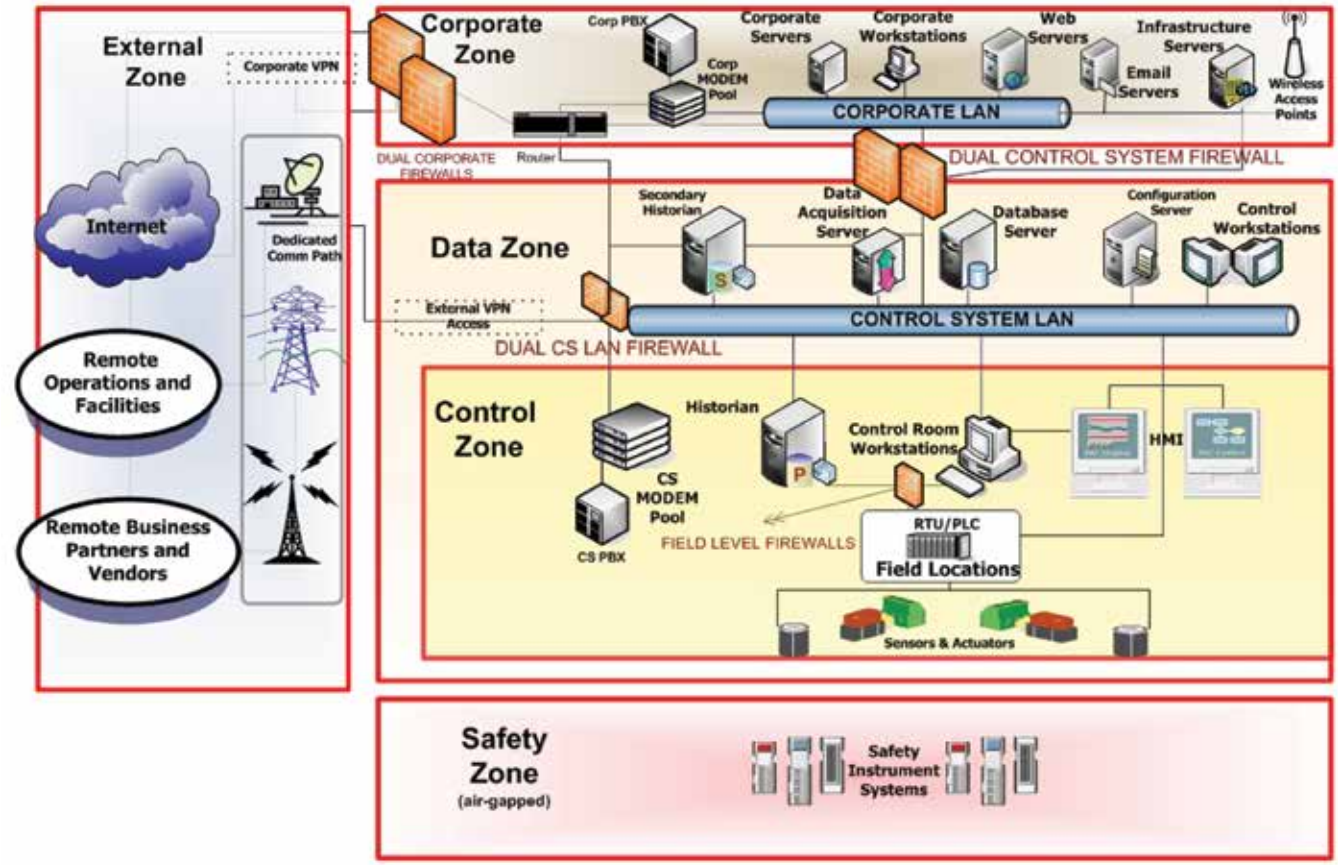

Figure 2: The U.S. Department of Homeland Security's Defense-in-Depth strategy outlines steps in cybersecuring control systems.

Traditional hacking tools now have add-on packages with OT exploits, while others expose any IP device and provide a wealth of information about the device, system and organization.

Continuous Monitoring

An organization needs to perform continuous monitoring (CM) of the IT and OT systems, as defined by NIST SP 800-137. Historically, performing CM on IT systems focused on anti-virus/malware detection and the use of a security information event manager (SIEM) for network and endpoint monitoring. CM for OT systems is a relatively new and emerging capability. An underlying fundamental concept of NIST SP 800-82 Rev 2 is the concept of "inbound protection and outbound detection." All control systems should be on a separate network from a corporate zone IT, with multiple levels of demilitarized zones (DMZs) and sub-networks; a virtual private network or other secure means to connect; and a SIEM as shown in the DHS Defense-in-Depth strategy[5] *(see "Figure 2," above)*.

New CM tools for control systems are able to evaluate and manage control system protocols, collect event logs and provide endpoint security.

Key Documents for Defending Building Control Systems

An organization that uses the risk management framework process from NIST generates and maintains several key documents and plans that cover both the IT and OT assets: a system security plan; a plan of action and milestones; an information technology contingency plan; incident communications procedures; and a security auditing plan.

Key personnel are appointed in writing. Templates for these documents are available on the U.S. General Services Administration (GSA) FedRAMP website.[6] Many cyber insurance policies now require these documents and are part of annual financial and IT audits.

Security Auditing

The security audit process documentation details the steps taken to verify an organization's software and hardware are functioning as intended; event and audit logs are reviewed; potential vulnerabilities are identified and addressed; patch management is current; continuous monitoring is functional; indicators of compromise or exploit are identified; and appropriate action is taken in a timely manner. NIST recommends system-level, application-level and user-level auditing.

The security audit process, which should be conducted monthly by the security team, compares previous and baseline configurations to identify any systemic changes. Documentation should be used in conjunction with the organization's IT policies and procedures, information technology contingency plan and documents associated with the organization's incident communications procedures.

WBDG Whole Building Design Guide® and Beyond

The Cybersecurity Resource page in the National Institute of Building Sciences WBDG Whole Building Design Guide®[7] is directed to the building community, but also offers links to other control systems, workshops and training. All facility/building owners and property

managers, as well as engineering and security staff, should understand the basic principles of NIST SP 800-82; know how to use the DHS CSET tool; understand how the open-source tools work for penetration testing; and prepare to adopt the new acquisition and procurement processes into their organizations. Whereas the IT community has had almost two decades to learn and implement cybersecurity, the OT community has an accelerated learning curve and needs to work closely with senior management, IT and other stakeholders to properly cybersecure an organization's assets.

Cybersecuring healthcare building controls systems and all other interconnected systems requires IT, facility and healthcare professionals (and even patients) to have basic cyber principles and security engrained in company and building management culture. Protecting these systems and information from damage or exploitation needs to become an automated process at the machine-to-machine level; in the transition, however, legacy systems still need to be protected and potential attacks and risks mitigated. The security team should ensure that all BCS are properly configured in a DMZ so that HMIs and building controllers cannot be found on search engines. They also must register with ICS-CERT to receive alerts and advisories; perform CM and security audits; and exercise them at least annually.

It is not a question of "will," but "when" outsiders could exploit building control systems. It's time to get prepared. JNIBS

References:

[1]National Institute of Standards and Technology (NIST), **www.nist.org**.

[2]SANS Institute. SANS Penetration Testing, **http://pen-testing.sans.org**.

[3]U.S. Department of Homeland Security. DHS ICS-CERT Alerts, **https://ics-cert.us-cert.gov/alerts**.

[4]International Society of Automation, **www.isa.org**.

[5]U.S. Department of Homeland Security. DHS ICS-CERT: "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," October 2009, **https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf**.

[6]U.S. General Services Administration. GSA FedRAMP Templates, **www.fedramp.gov/resources/templates-2016/**.

[7]National Institute of Building Sciences. WBDG Whole Building Design Guide, Cybersecurity Resource page, **www.wbdg.org/resources/cybersecurity.php**.

ABOUT THE AUTHOR: Michael Chipley PhD, *president of The PMC Group LLC, is the creator of the National Institute of Building Sciences' "Cybersecuring Building Controls Workshops." He can be reached at* **mchipley@pmcgroup.biz**.

"Cybersecuring Healthcare Building Control Systems," authored by Michael Chipley, PhD, was published in the August 2016 issue of theJournal of the *National Institute of Building Sciences* (JNIBS), a publication of the Washington, D.C.-based National Institute of Building Sciences. The article has been reproduced here with permission from the publisher. Learn more about JNIBS at **http://www.nibs.org/?page=journals**, and access your free issue(s) by subscribing at **http://www.wbdg.org/account/subscribe_jnibs.php**.