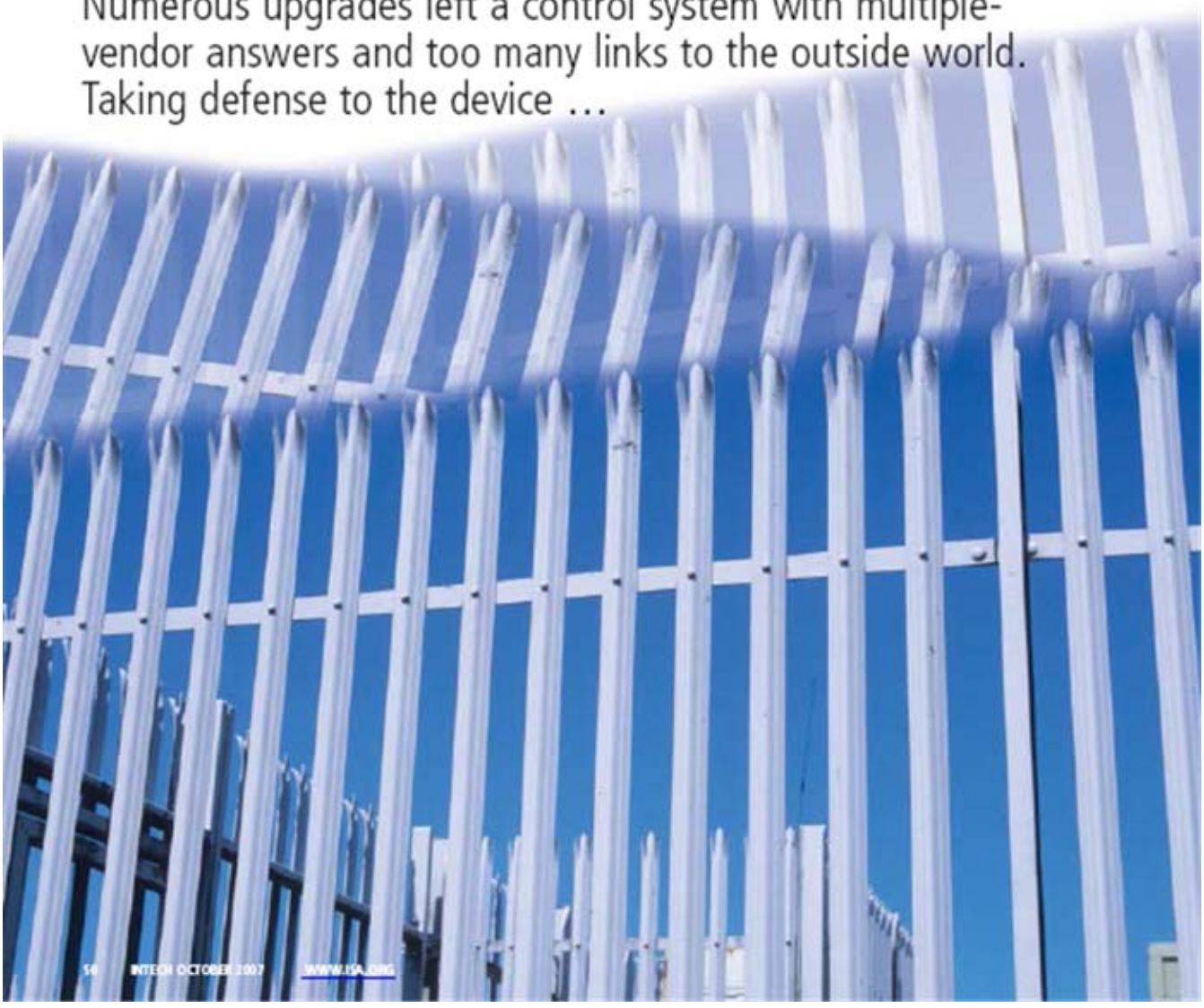
Making cyber security work in the refinery

By Eric Byres and Nicholas Sheble

Numerous upgrades left a control system with multiple-vendor answers and too many links to the outside world. Taking defense to the device …



FAST FORWARD

- A cyber defense strategy begins by creating an electronic perimeter around the control system.
- In the control-systems world, there are fewer security choices.
- For sure, the single, monolithic, popular firewall answer does not work.

Anyone reading *InTech* over the last five years will have seen many articles on the need to secure control systems from cyber attack. Nearly all include descriptions of actual security incidents that will concern even the most hardened controls specialist.

Along with these tales of cyber disaster come excellent articles concerning security theory, security standards, and security design for new plants.

Unfortunately, most of us cannot start with a blank slate where we can create the perfect security design. Instead, we must somehow shoehorn a security solution into an operating plant or factory filled with existing networks and equipment.

Furthermore, we must do this "shoehorning" without affecting production in any way—a tall order considering most security technologies' first responsibility is preventing communications, not letting them through. We need a clear path for designing and installing a cyber security solution into a real plant.

The control system team at a refinery in Texas faced this exact problem. The refinery is a decades-old facility owned by a now defunct oil company, and it originally handled 60,000 barrels of crude per day (bbl).

It has retrofitted and optimized over the years and is as state of the art as anything built in 1953 can be. By 2006, it was an award winning facility and had expanded processing to over 300,000 barrels of crude per day. Production included low-sulfur gasoline, diesel, and jet fuel, which pumped to Texas cities including San Antonio, Bastrop, Austin, Waco, and Dallas/Fort Worth via company pipelines.

The numerous upgrades, expansions, and mergers had left the team managing a complex collection of different control systems and networks, including products from Emerson (DeltaV and Provox), Invensys (Triconex, IA, and WonderWare), and Rockwell (PLC-5 and ControlLogix).

Dropping security into this mix, without influencing production, was certain to be a challenge.

Where are we, where are we going?

The old saying, "It is difficult to get to where you want to go if you don't know where you are starting from," applies to security as much as anything in life, so this refinery team began by carefully cataloging their control system.

In particular, they focused on the various communications pathways and networks that connected the various control systems and the corporate network. Although the plant's design philosophy has always been to minimize the number of connections between the business- and control-system networks, due to years of growth they found they had far more connections than they really wanted.

The ideal number from the control system team's perspective was zero. This of course is not practical, so the team went to work to reduce the number of connections to a bare minimum, while preserving the key business information needs.

Of course, if you do not know where you want to go, you will not get there, so the next step for the refinery control team was to determine security targets they would like to achieve.

Evolving standards such as ISA99 helped guide them, and over a number of months, the team created a collection of security policies and processes for the control systems, combining the requirements of production, safety, and security at the refinery. It was not an easy task but critical to the success of the program.

Creating defense-in-depth

Once the security roadmap was in place, it was time to make the changes to the control systems and networks that would move this Texas refinery toward a secure plant floor. To do this, the team needed a design philosophy.

One security philosophy that used to be popular in the IT world is the Bastion model. It depends on

hiding all key assets behind a single monolithic solution. For example, deploying a single firewall between the business and control system networks to protect all process devices is a Bastion design. Its supporters hope this firewall will be the ultimate security filter and prevent anything evil from ever getting to their critical systems.

Unfortunately, industry experience has shown Bastion designs present a single point of failure. With the help of Murphy's Law, eventually trouble bypasses all single-point solutions or some sort of malfunction compromises the single-point defense. When they do, the system is wide open to attack.

This refinery chose to skip the Bastion model and instead based their design on the concept of "defense-in-depth" security. Using this strategy, effective security transpires by layering multiple security solutions, so if one fails another will provide the defense.

For example, a (less expensive) firewall may still be located between the business and control system networks, but additional security solutions are also placed inside the control system that can protect key devices if the main firewall either fails or is bypassed.

Defense-in-depth begins by creating a proper electronic perimeter around the control system, and this is where our refinery started. Policy and technology defined the security perimeter for the control system.

The policy divided the overall system into zones and defined what belonged on the control system network and what did not. Critical systems that would have a serious impact on production or safety if attacked were together. For example, all DCS controllers and PLCs were mission critical, thus belonging on the lowest and most secure level.

Above the controller/PLC zone were the human machine interfaces (HMIs) and application/programming stations in a number of supervisory zones.

Finally, there were several zones (we call them demilitarized zones, or DMZ) where we place assets such as data historians and optimization systems. Systems are those we consider important overall, but without which the plant could still operate if they were to fail due to a cyber event.

Next, the many connections into the control system reduced to few. On each connection, a primary control system firewall acted as the choke point for all traffic between the outside world and the critical control system devices.

In this case, the decision was the IT department would manage the firewalls.

Wait until a plant shutdown? No

One major challenge for process control security is selecting second-layer security

Control systems security standard

The ISA99 committee addresses manufacturing and control systems whose compromise could result in any or all of the following situations:

- Endangerment of public or employee safety
- Loss of public confidence
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Economic loss
- Impact on a nation's security

The concept of manufacturing and control systems electronic security applies in the broadest possible sense, encompassing all types of plants, facilities, and systems in all industries.

Manufacturing and control systems include, but are not limited to:

- Hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes

The committee has completed work on its first standard, *Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models*. This standard will publish this month and establishes the context for all remaining standards in the ISA99 series by defining a common set of terminology, concepts, and models for electronic security.

In addition, the Part 2 standard in the ISA99 series, *Establishing an Industrial Automation and Control Systems Security Program*, is out for committee voting. This standard will provide guidance for developing a program for the security of industrial automation and control systems including detailed guidance on process activities and key elements for establishing a cyber security management system.

Beyond its work on the initial standards in the ISA99 series, the committee has also completed of an updated technical report, first published in 2004. This report focuses on identifying and evaluating currently available technologies for control systems security, covering areas including:

- Authentication and Authorization
- Filtering/Blocking/Access Control
- Encryption and Data Validation
- Audit, Measurement, Monitoring, and Detection Tools
- Operating Systems
- Physical Security

Guide to the ISA99 standards: **www.isa.org/link/Guidetoo99**

solutions that actually work in the industrial setting.

In the IT world, personal security software such as host-based firewalls (like firewall software like Zone Alarm running on the PC) can offer excellent second-layer defenses.

In the controls world, there are fewer choices since commercial security software typically cannot add onto devices such as PLCs or safety controllers. Even some PC-based devices, such as HMIs, may be unsuitable for add-on security software because of vendor restrictions or the age of the operating system.

To address this problem we decided to use a new security system. This scheme offers process control companies a layered security model by providing security appliances directly in front of groups of control devices needing protection. This way, even if a hacker or virus manages to get through the perimeter firewall, they still face and must breach an array of control system-focused security devices before doing any damage.

Starting in early August 2007, trial device installed to various locations at the refinery, starting with the control-system test lab and moving into more critical systems such as the boilers.

With traditional security devices, these installations would have needed to wait until a plant shutdown. These new apparatuses, however, have two special features that allow live installation: "zero-configuration" field installation and the device test mode.

The zero-configuration installation procedure means the technician who installs the piece, needs only to mount it on a DIN rail and connect the power and communication cables.

The units can hook up at any time and only affect the operating process for the few seconds it takes to attach the network cables. Once on the control network, the units remain in invisible pass-through mode until awakened by a special configuration computer, which can be at any convenient location on the plant network.

Once the devices were in place in the Texas refinery, the system automatically established a secure communications link to allow configuration.

The controls team then selects and uploads software security modules from the included library. In this case, those modules included firewalls and diagnostics.

Next, the team downloaded a series of device "security templates," each tailored for a control device to be protected. These templates defined the activities the firewall would eventually execute against incoming or outgoing traffic, as well as the appliances' actions in non-standard conditions, such as when the network is under attack.

In the IT world, personal security software such as host-based firewalls, like Zone Alarm running on the PC, can offer excellent second-layer defenses. In the controls world, there are fewer choices.

For example, we loaded one of the proprietary system templates that allows all the traffic that company's systems would typically require and block everything else. We performed all these chores without affecting the refinery's control system in the least.

When the configuration process is complete, the technology goes into test mode. This activates the firewall rules in the templates, but it does not actually drop any traffic. Instead, it reports the traffic that would be blocked once full operation mode is running. If the controls engineer notices packets he or she thinks should get through, he or she merely adjusts the firewall rules.

At this installation, we left the security in test mode for nearly one month to collect traffic and allow the team to be certain there were no rare control messages critical to operations but that someone had forgotten. Only when the logs showed there were no exceptions reporting, did we switch to operational mode and did actual traffic blocking begin.

The preliminary test mode proved to be valuable in ways no one expected at the refinery. The refinery control systems manager said, "Not only did the test mode allow us to deploy this new technology in a safe, gradual manner, but it gave us a microscopic view of control traffic that we had never seen before. We discovered miss-configured computers and devices generating traffic that never should have been on our control system, allowing us to clean them up right away."

As for the future, this refinery is only starting their security project. Over the next year, they will continue to install and tune more of these individual units throughout the plant, monitoring each to see what is really happening on their complex control system.

As well, they will continue to work closely with their IT department to improve the definition of their control system security perimeter. As one industry expert noted, "control system security is a journey, not a destination," and the team at this Texas refinery is on board with that.

ABOUT THE AUTHORS

Eric Byres (Eric@byressecurity.com) is the CEO of Byres Security, a registered P.E., and a senior member of ISA. He is a member of ISA99: Manufacturing and Control Systems Security. He founded the Critical Infrastructure Research Center at the British Columbia Institute of Technology. **Nicholas Sheble** (nsheble@isa.org) is the senior technical editor for *InTech*.

View the online version at www.isa.org/intech/20071005.

RESOURCES

The Line
http://www.isa.org/InTech/20070306

Uncovering Cyber Flaws
www.isa.org/link/Uncovercyber

SP99 counterattacks
www.isa.org/link/SP99counter

Who's the enemy? Don't look at IT
www.isa.org/link/enemywho