



documented incidents of process disruption than any other source. A few of its dubious achievements include interrupting power distribution SCADA systems, infecting the safety parameter display system (SPDS) in a nuclear plant and curtailing oil production operations in the Gulf of Mexico.

What is particularly interesting is that the Slammer Worm has used at least five different pathways to get to its control-system victims. In one case it got into a petroleum control system via a maintenance laptop that was used at home (and infected) and then brought into the plant. In another case it infected a paper machine human machine interface (HMI) via a dial-up modem that was used for remote support. In the third case it passed right through a poorly configured firewall. In all these examples there were firewalls in place, but the worm either bypassed them by using a secondary pathway, or it took advantage of some flaw in the firewall's deployment.

Slammer is just one example. An analysis of 75 security incidents against control systems between 2002 and 2006 shows that more than half the external attacks come through secondary pathways such as dial-up connections, wireless systems and mobile devices. In these cases, the firewall did its job, but the security strategy failed.

### The Leaky Data Pipeline

The third cause of SCADA insecurity is a flaw in SCADA network design. For many years, just keeping systems communicating was a primary challenge for the SCADA engineer. Communications technology was expensive and rather unreliable, so any network that promised to solve these issues was welcome. The emergence of Ethernet, TCP/IP and Web technologies radically changed this equation.

The result was the creation of "control networks" that acted as common pathways for all industrial control communications. When a new control application needed a network to transport its data on, too often the answer was "we'll connect it to the control network." Within a few years, any clear understanding of exactly what devices were attached to most corporate "control networks" or what traffic was traveling over the network, was impossible. For example, after one U.S. refinery conducted an analysis of its control systems traffic as part of security review, the systems manager commented:

"We discovered misconfigured computers and devices generating traffic that never should have been on our control system."

Like an unattended pipeline in a third-world country, well-intentioned staff had been "tapping" into the control system network for years to add or access network traffic. Over time the result was an unreliable and insecure SCADA system.

### Getting SCADA Security Under Control

How does a company ensure its SCADA system is secure? The answer is spelled out in a new standard called "ISA-99.02.01, Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and

Control Systems Security Program," approved and published recently by the American National Standards Institute (ANSI). This readable standard lays out seven key steps for creating a Cyber Security Management System (CSMS) for use on SCADA and control systems.

The steps in ISA-99.02.01 are divided into three fundamental categories: Risk Analysis, Addressing Risk with the CSMS, and Monitoring and Improving the CSMS. The first category lays out the stages a company needs to follow to both assess its current security situation and determine what security goals it wants to achieve.

The second category outlines the processes to define security policy, security organization and security awareness in the company and provides recommendations for security countermeasures to improve SCADA security. The core idea in this section is a concept known as Defense-in-Depth, where security solutions are carefully layered to provide multiple hurdles to attackers and viruses.

The final category describes methods to make sure a SCADA system not only stays in compliance with the CSMS but follows a continuous improvement program.

### More Than Just Improved Security

The benefits for oil and gas companies that have followed the ISA-99.02.01 program (or a similar program) extend far beyond just reducing the possibility of attack from a hacker or virus. By cleaning up both the corporate processes concerning SCADA systems and better managing the actual traffic on the control system networks, many companies have realized significant improvements in overall system reliability.

One senior manager of a European oil company recently noted that each time they put a refinery through a SCADA security-improvement program, the increase in production reliability justifies the cost of the security program alone. The increased security ends up being just an extra benefit.

On the other hand, failure to adapt corporate SCADA systems to the changing threats and vulnerabilities of the cyber world will leave companies exposed to increasing numbers of security incidents. The consequences unfortunately could include a marred reputation, environmental releases, production and financial loss, and perhaps even human injury or death. *PE&GJ*

*Author: Eric Byres, P.Eng., is chief technology officer of Byres Security Inc., Lantzville, BC, Canada. He can be reached [eric@ByresSecurity.com](mailto:eric@ByresSecurity.com).*

## Defense In Depth

Sound strategy, regardless of whether it is for military, physical or cyber security, relies on the concept of "defense in depth." Effective security is created by layering multiple security solutions so that if one is bypassed another will provide the defense. This means not over-relying on any single technology such as a firewall. Firewalls aren't bad technology. In fact, they are a fantastic tool in the security toolbox. But, industry has misused them by believing they will solve all security ills.

Defense in depth begins by creating a proper electronic perimeter around the SCADA or control system and then hardening the devices within. The security perimeter for the control system is defined both by policy and technology. First, policy sets out what truly belongs on the control system network and what is outside. Next, a primary control-system firewall acts as the choke point for all traffic between the outside world and the control system devices.

Once the electronic perimeter of the control system is secured, it is necessary to build the secondary layers of defense on the control system itself. Control components like HMIs and data historians that are based on traditional IT-operating systems such as Windows and Linux should take advantage of the proven IT strategies of patch and anti-virus management. However, this requires prior testing and care.

For devices like PLCs and SCADA controllers — where patching or anti-virus solutions are not readily available — most security experts recommend the use of industrial security appliances. This rapidly evolving security solution deploys low-cost security modules directly in front of each group of control devices needing protection. The security modules then provide tailored security services like "personal firewalling" and message encryption to the otherwise unprotected control devices. ■

Low-cost industrial security appliances are designed to protect SCADA and control devices by providing defense-in-depth protection. (Source: Honeywell)

