Cyber Security And The Pipeline Control System

By **Eric J. Byres, P.Eng.,** Lantzville, BC, Canada

In the winter of 2002-2003, Venezuela found itself in the grip of the largest and longest strike in Latin American history. Lasting from Dec. 2 until Feb. 2, the strike paralyzed the oil industry through work stoppages and acts of sabotage. According to a published report at the time, Ali Rodriguez, the head of Petróleos de Venezuela, S.A. (PDVSA), stated:

"[...] we have suffered many acts of sabotage at the terminals, the refineries, and even to some wellheads in Lake Maracaibo. There were even instances of computer hacking which did a lot of damage since much of the operation is centrally controlled by computer."

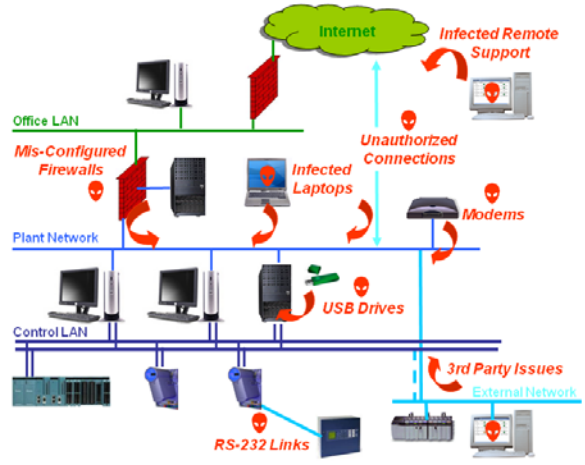
Details of the cyber attacks on PDVSA's systems were slow to emerge, but it seemed that hackers were able to penetrate the SCADA system responsible for tanker loading at a marine terminal in eastern Venezuela. Once inside, the hackers erased the programs in the programmable logic controllers (PLCs) operating the facility, preventing tanker loading for eight hours. Fortunately for PDVSA, the tactics of attackers were unsophisticated, making detection of the problem relatively easy, and backups of the PLC programs were unaffected, making recovery straightforward.

Two years later a book by Thomas Reed, senior U.S. national security official, made it clear that not all pipeline operators are so lucky. In his book, "At The Abyss," Reed reported how the U.S. allowed the USSR to steal pipeline control software from a Canadian company. Unknown to the Russians, this software included malicious code (known as a Trojan horse) that caused a major explosion of the Trans-Siberian gas pipeline in June 1982. The Trojan ran during a pressure test on the pipeline and massively increased the usual pressure, causing the explosion. Reed writes:

"In order to disrupt the Soviet gas supply, its hard currency earnings from the West, and the internal Russian economy, the pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds."

By creating an explosion with the power of a three-kiloton nuclear weapon, the U.S. managed to disrupt supplies of gas and consequential foreign currency earnings of the Soviet Union for over a year.

These instances of computer hacking were the first public examples of the susceptibility of oil and gas operations to deliberate external cyber attacks on control systems. For many companies it forced a complete re-evaluation of what cyber security meant when it came to oil and gas SCADA-control systems.



Attack routes taken. In 75 incidents from 2002 to 2006, attackers and viruses infiltrated SCADA systems via secondary pathways nearly 50% of the time. *(Source: Industrial Security Incident Database, June 2006)*

Misunderstanding The Risk

Internal surveys at several major oil companies indicated that managers often misunderstand the situation they face when it comes to SCADA security. First, many believe that the Information Technology (IT) group automatically looks after SCADA security as well. This is rarely the case.

While IT departments are very good at providing security for systems they understand, such as Windows® servers and accounting databases, the critical control systems that run the pipelines and refineries day in and day out are forbidding beasts to the IT professional. For example, instead of the typical IT operating systems and applications like Windows® and MS-Word®, many control systems have unusual operating systems and applications such as VxWorks or RSLogix™. This means that many of the proven IT security solutions will not function correctly or, if they do run, may interfere with the SCADA operations.

A good example of this was reported at an ISA Industrial Security Conference in Philadelphia a few years ago. When an emergency shutdown system on a boiler failed to operate correctly, investigators discovered that anti-virus software had been installed on the computer used to configure the safety system. This software blocked the proper operation of the safety system, putting the entire plant at risk. There was nothing wrong with the safety system or the anti-virus software on their own, but together they made a life-threatening combination.

The result is that many IT departments quietly wash their hands of a security responsibility once a piece of network or computer hardware is attached to the SCADA network. And if the SCADA operations/engineering team doesn't take up cyber security as its responsibility, this leaves a nice gap that the hacker or virus can silently slip though.

Wrong Assumptions

Many managers also assume that all cybersecurity problems arise from outside the company premises, generally from hackers. Next, they assume those problems that attempt to enter the company SCADA system come through obvious pathways that can be managed by a single Bastion Firewall between the business network and the SCADA network. Unfortunately, when problems originate from within the company, as they often do, the Bastion firewall does little to help, leaving the SCADA system an easy target for disruption.

To understand where the Bastion model fails, it is helpful to look at an Internet worm called the Slammer Worm and study how it has affected control systems since its creation in 2003. According to records in the Repository for Industrial Security Incidents (RISI), this one worm has been responsible for more

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 it 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. *P&GJ*

Author: Eric Byres, PEng., is chief technology officer of Byres Security Inc., Lantzville, BC, Canada. He can be reached 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)*