01 Jan 2005

Trends in Process Control Systems Security

Ann K. Miller
Missouri University of Science and Technology

Editor: O. Sami Saydjari, ssaydjari@cyberdefenseagency.com

Trends in Process Control Systems Security

Ann Miller
University of Missouri–Rolla

The protection of critical infrastructure systems is a hotly debated topic. The very label "critical infrastructure" implies that these systems are important, and they are: they support our everyday lives, from the water and food in our homes to our physical and financial welfare. They also support industry and government operation. Within the US alone, critical infrastructures include approximately 28,600 networked Federal Deposit Insurance Corporation (FDIC) institutions, 2 million miles of pipeline, 2,800 power plants (with 300,000 production sites), 104 nuclear power plants, 80,000 dams, 60,000 chemical plants, 87,000 food-processing plants, and 1,600 water-treatment plants.

In an effort to scope the issue, the US National Strategy for Homeland Security has identified 14 areas for critical infrastructure protection, most of which are privately owned: agriculture, information and telecommunications, food energy, water, transportation, public health, finance and banking, emergency services, chemical industry and hazardous materials, government, postal and shipping, defense industrial base, and national monuments and icons. At the heart and soul of nearly every one of these critical infrastructures is a *process control system*. PCSs have existed for millennia: float regulator mechanisms for controlling water levels, for example, date back to Greece circa 300 BC. In the 1800s and early 1900s, most control systems used relay and sequencer technologies; the most significant recent development was the introduction of programmable logic controllers (PLCs) in the late 1960s.

This article explores the recent evolution of PCSs and their environments, explains the need for improved security in these systems, and describes some of the emerging research areas that offer promise in PCS security.

The importance of PCS availability

A PCS frequently used in critical infrastructures and factory automation is a supervisory, control, and data acquisition (SCADA) system, which monitors switches and valves, controls temperature and pressure conditions, and collects and logs field data. A SCADA system can continuously record and report pressure data polled from an oil pipeline, for example; if an alarm is registered, the control-room operator can respond to the alarm and use the system to investigate other parts of the pipeline. SCADA systems also monitor pipelines for total volumetric rate, to provide yield data. Additionally, these systems can sample the produced fluids for specific gravity, gas composition, and other physical parameters as required. SCADA systems typically monitor and report these values to control-room operators.

SCADA systems specifically, and PCSs in general, have tiers of computing capability—from powerful workstations to PLCs to wired and wireless sensors—with all the components networked together to provide the desired process control. Such systems' operational requirements vary by industry and application, but most requirements typically include 24/7 availability, real-time or near-real-time response, and, increasingly, remote control. In terms of security primitives, security professionals typically prioritize by confidentiality, integrity, and availability. For a PCS, though, it's availability, availability, and availability: when you flip a light switch, you expect the light to turn on, and when you pick up a telephone, you expect a dial tone. In some sectors, estimates of the cost of downtime range from US$1 million to $4 million per hour or US$25 million to $100 million per day.

Designers typically build PCSs with fault-tolerant techniques such as redundancy and minimal mean time to repair, paying special attention to disaster recovery. For most systems, harsh environments (such as the North Sea and the Gulf of Mexico for deep-sea wells) and natural disasters (such as hurricanes and earthquakes) pose the biggest threats. The 1988 Piper Alpha explosion of an oil production platform in the North Sea, for example, resulted in 167 deaths and substantial financial losses. Since then, many oil pipelines have been fitted with emergency shutdown valves designed to close the pipeline at two or more places in the event of major breaks in the line or severe pressure

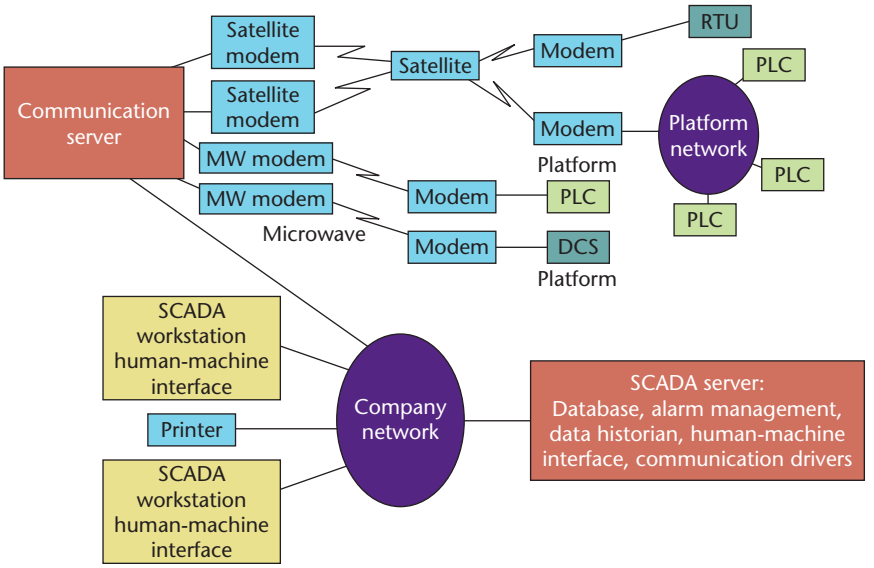

Figure 1. Supervisory, control, and data acquisition (SCADA) system for an oil platform with increasing use of remote control and connectivity to the rest of the enterprise. Programmable logic controllers (PLCs) and remote terminal units (RTUs) monitor and control offshore elements.

loss at one end. Many countries also mandate regulatory oversight and institute certification requirements for new oil and gas wells. But why isn't the threat of computer attack addressed equally?

To answer this question, we must first look at the evolution of PCSs and the environment in which they operate. Initially, PCS data communication relied on proprietary protocols and operating systems, but over time, standard Ethernet-based protocols offered several additional advantages: less training, increased overall productivity, and reduced costs. However, the flipside of this standardization is an increased vulnerability to Ethernet-based attacks. Furthermore, many PCS products now include commercial off-the-shelf software—for example, commercial operating systems and database packages. This computing environment promotes ease of use, but it also renders PCSs susceptible to myriad buffer-overflow vulnerabilities and other attack opportunities inherent in products such as Microsoft Windows. Connectivity has also significantly increased. Whereas human operators initially worked within the PCS's "blast zone" with its stand-alone network, safety considerations have encouraged the use of remote control and management, and a growing number of companies now control their SCADA systems from offsite. Oil production companies use remotely controlled pipeline-isolation plugs, for example, to seal pipelines for planned shutdowns (routine repairs), rerouting, adding valves, and so on. Figure 1 illustrates a typical example, with PLCs and remote terminal units (RTUs) monitoring and controlling specific offshore infrastructure elements.[1]

SCADA systems, with various communication links for redundancy and control-center management software, perform the system monitoring between field and control centers. Communication links can traverse the public Internet, thus the threat space is literally the world.

Even in less hostile environments, such as manufacturing lines, the PCS is frequently on its own subnetwork with connectivity to the rest of the enterprise (see Figure 2).[2] The advantage is that the organization has access to production-line output in real time, but the disadvantage is the potential for access by disgruntled employees within the organization and malicious outsiders via the Internet.

System security

Many studies have analyzed individual SCADA systems for reliability and security,[1,3,4] but it's still an important research area simply because its assets are so critical. Several specific areas are still ripe for further research.

Vulnerability assessments and decision support

The number, speed, and sophistication of network attacks continue to grow; naturally, this dynamic, yet escalating, threat environment requires a comprehensive approach to security that also includes vulnerability and risk analyses. Many vulnerability assessments are just results of a checklist's completion; they offer no assurance that the list is comprehensive or that the PCS, once it "passes the checklist," is now secure. We need a systematic methodology that can apply to a variety of SCADA systems. Some initial work in this area has begun,[5] but much more is needed. Moreover, these critical systems are large and complex, which makes changes and upgrades costly. Once we can identify and assess the vulnerabilities, we'll need a decision support system to prioritize various strategies for protection, mitigation, or recovery.

Network mapping and interdependency identification

A PCS's networked nature is one of its greatest strengths because it provides the opportunity for robustness, while also allowing the possibility of cascading failures. One of a critical infrastructure's most vulnerable layers is network access to its SCADA

systems. To understand a dynamic network architecture, we need tools that facilitate network mapping—tools that not only visualize node topology and connectivity but also provide information on types of reachability as well as path dependence. In hardware, reachability can be as simple as a link at the physical layer and (in system terms) whether a route allows a path to the system or network. In software, reachability can include the operating system or program's ability to make the necessary connections to the hardware or network to "reach" the system. Whether done directly through routing or via a series of handoffs, reachability opens vulnerabilities. The research needed in this area is more than a ping utility; automated network analyses that can run in background mode and provide warnings if a security policy is violated would greatly assist SCADA operations. Tool support through an analysis of information flow between SCADA systems is also needed—system security personnel might want to restrict certain types of packets in support of the organization's security policy and not permit any "backdoor" mechanism for those packets through indirect routing. Tools such as the prototype Cayenne Network Analyzer are a step in this direction.[6]

Infrastructures and their collective PCSs are often interdependent—the power grid, for example, depends on oil and gas pipelines, and oil and gas pipelines depend on the power grid. Yet such systems' vulnerabilities aren't obvious; an attack on one infrastructure can cause a failure in a seemingly unrelated infrastructure. Moreover, each infrastructure is composed of multiple layers, from cyber to physical system control; thus, a cyberattack in one infrastructure could cause a physical failure in another. Visualization tools could help operators manage and monitor this complex connectivity.

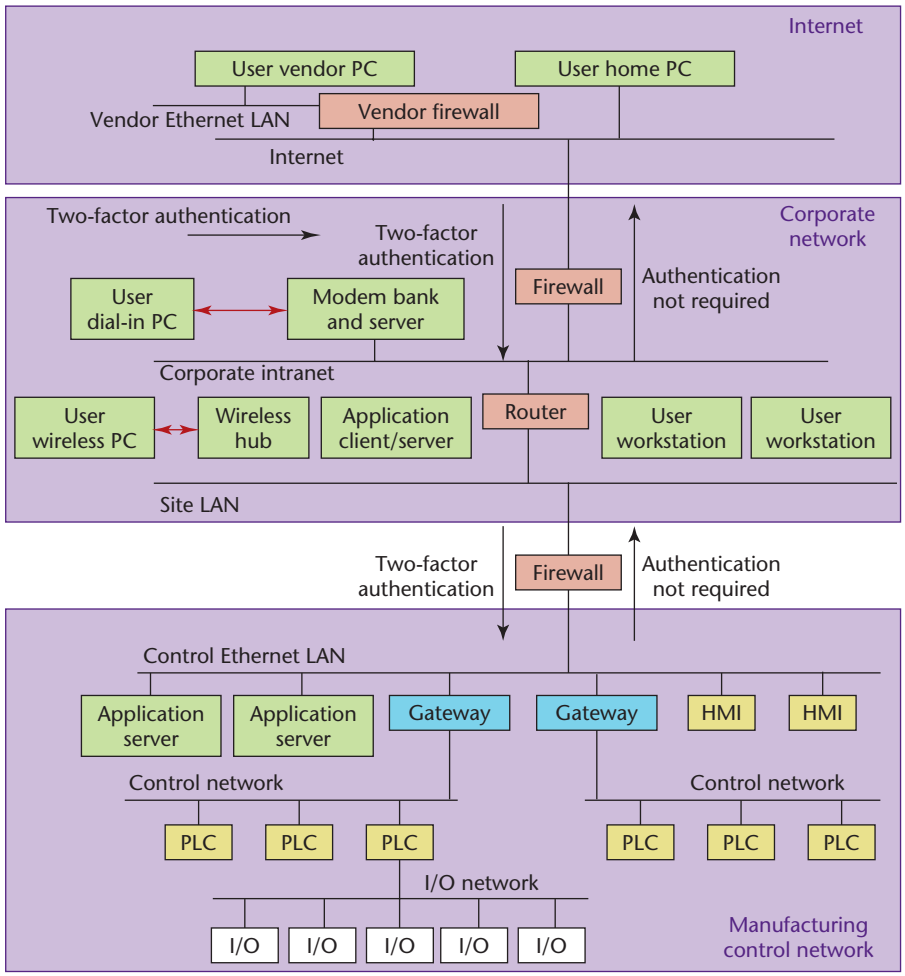

Figure 2. Process control system (PCS) network for a manufacturing line. Frequently, networks are located in isolated facilities with connectivity to the enterprise and, ultimately, to the Internet through one or more firewalls.[3] (HMI stands for human-machine interface, and PLC stands for programmable logic controller.)

Modeling, simulation, and experimentation

A PCS's tiered structure requires a multilayered model that can capture identified vulnerabilities. Furthermore, to link the vulnerabilities between interdependent systems, the modeler requires some notion of causality. Once developed, the modeler could link the resulting multilayered SCADA models to determine system interactions, and then test, refine, and validate these models and data through increasingly sophisticated experiments to discover and record additional dependencies and system interactions. Network congestion control also has room for improvement. Promising work is under way at the US National Infrastructure for Simulation and Analysis Center (NISAC; www.lanl.gov/orgs/d/nisac/) in its development of the Interdependent Energy Infrastructure Simulation System (IEISS) tool and the Water Infrastructure Simulation Environment (WISE).

Distributed control

PCSs are naturally distributed, but monitoring and control are often centralized, and controllability is limited to operations centers. With the advent of intelligent distributed

controllers, the rise in distributed decision-making via network communication has broadened the available responses to infrastructure changes due to natural failures or attack. However, controllers' actions must be cooperative so that they don't introduce negative network effects on the system. Distributed algorithms govern these actions, so they must also be fault-tolerant and secure. Many PCSs are, in reality, transportation networks; thus, flow models and flow-balance algorithms dominate the controllers. These algorithms can be made fault-tolerant via executable runtime assertion-checking. The distributed coordination algorithms for a specific type of controller for power systems, the Flexible AC Transmission System (FACTS), appear elsewhere.[7]

Full-spectrum attack planning

A recent survey analyzed cyberattack incident reports collected from various infrastructure control systems.[8] The study showed a fivefold increase from 1994 to 2004 in the annual control system incident rate. Another significant finding was a change in the type of incident. For the period between 1982 and 2001, 29 percent of the incidents were labeled as external, 50 percent as accidental, and 21 percent as internal. However, from 2002 to 2004, 66 percent were classified as external, 22 percent were accidental, and only 3 percent were internal; the remaining were categorized as unknown. We need improved techniques for dealing with network attacks across the entire spectrum, from real-time indications and pre-attack warnings to trans-attack methods for survivability, denial, and consequence management to post-attack means for attribution through digital forensics.

With so many PCSs in private hands, there is a very real reluctance to discuss vulnerabilities, but the sharing of information is essential. One group aims to ease this fear: the Process Control Systems Forum, www.pcsforum.org. Although the forum is a US Department of Homeland Security initiative launched in May 2005, it recognizes that PCS security is a global issue that requires a global solution, and international membership is invited and encouraged. This open forum has several subgroups, called interest groups; one particular such group focuses on research. The Research Interest Group will maintain an open, shared, and well-publicized Web site (www.pcsf.org) to serve as a repository for control systems research (with links to references and related sites), raise awareness of control systems issues where further research is needed, and encourage dialogue and collaboration between industry, academia, and government. ▢

References

1. K.T. Erickson et al., "Reliability of SCADA Systems in Offshore Oil and Gas Platforms," *Stability and Control of Dynamical Systems with Applications*, Birkhauser Press, 2003, chapter 20.
2. K.T. Erickson, *Programmable Logic Controllers: An Emphasis on Design and Application*, Dogwood Valley Press, 2005.
3. A. Miller and K.T. Erickson, "Network Vulnerability Assessment: A Multi-Layer Approach to Adaptivity," *Int'l Workshop Research and Education in Control and Signal Processing*, NATO Symp. Adaptive Defence in Unclassified Networks, 2004, pp. 13-1–13.8.
4. H.M. Paula, "Failure Rates for Programmable Logic Controllers," *Reliability Eng. and System Safety*, vol. 39, 1993, pp. 325–328.
5. A.B. Baker et al., *A Scalable Systems Approach for Critical Infrastructure Security*, tech. report SAND2002-0877, Sandia Nat'l Labs., Apr. 2002; www.sandia.gov/scada/documents/020877.pdf.
6. D. Craigen et al., "Multi-Layer Vulnerability Assessments of SCADA Networks," *Proc. Ottawa CyberSecurity Workshop*, 2005; www.ora.on.ca/.
7. A. Armbruster et al., "The Maximum Flow Algorithm Applied to the Placement and Steady State Control of FACTS Devices," to be published in *Proc. North Am. Power Symp.*, 2005.
8. US Computer Emergency Readiness Team, "Control Systems Cyber Security Awareness," US-CERT, 7 July 2005; www.us-cert.gov/reading_room/Control_System_Security.pdf.

Ann Miller *is the Cynthia Tang Missouri Professor of Computer Engineering at the University of Missouri–Rolla. Her research interests include systems and software engineering, with an emphasis on trustworthy systems, including system survivability, reliability, and security, and on the design and test of large-scale networked systems. Miller has a BS, an MS, and a PhD in mathematics from Saint Louis University. She is a senior member of the IEEE and a member of the IEEE Computer, Communications, and Reliability Societies, serving on the administrative committee of the Reliability Society. Contact her at milleran@umr.edu.*