Chapter 10
Control Systems Security

Jake Brodsky
Washington Suburban Sanitary Commission, USA

Robert Radvanovsky
Infracritical, Inc., USA

ABSTRACT

With recent news media discussions highlighting the safety and integrity of the U.S. national power grid, questions have been raised by both political and executive-level management, specifically, as to the risks associated with our critical infrastructures. More specifically, the issue of concern is dealing with and addressing cyber vulnerability issues, threats and risks associated with an extremely complex and inter-twining series of dependencies arising from legacy industries established almost 100 years ago. Equally as important are the growing threats and risks to these environments resulting from their exposure to outside networks (such as the Internet), exposing critically vital and important cyber systems to just about everyone and anyone globally. This chapter highlights the importance of preventing hack attacks against SCADA systems, or Industrial Control Systems (abbreviated as ICS), as a means of protecting our critical infrastructures.

INTRODUCTION

This chapter highlights an important but seemingly under-represented area of attack for Black Hat hackers or terrorists' intending to cause harm to an industry's networks and/or to a nation's citizens. It provides an overview of a critical aspect of security that impacts end users and security personnel, alike. It also gives a review and discussion of the weaknesses of SCADA systems and the various ways they may be compromised. Suggested remedies for securing these systems are presented at the end of this chapter.

DOI: 10.4018/978-1-61692-805-6.ch010

What are Control Systems?

Generally speaking, most control systems are computer-based. Control systems are used by many infrastructures and industries to monitor and control sensitive processes and physical functions. Typically, control systems collect sensor measurements and operational data from the field, process and display this information, and relay control commands to local or remote equipment. In the electric power industry, they can manage and control the transmission and delivery of electric power, for example, by opening and closing circuit breakers and setting thresholds for preventive shutdowns. By employing integrated control systems, the oil and gas industry can control the refining operations on a plant site, remotely monitor the pressure and flow of gas pipelines, and control the flow and pathways of gas transmission. With water utilities, control systems can remotely monitor well levels, control pumps, monitor water flows, tank levels, and so on.

Control system functions vary from simple to complex, and many may be used to simply monitor processes running. For example, environmental conditions within a small office building would represent the simplest form of site monitoring, whereas managing most (or in most cases, all) activities for a municipal water system or a nuclear power plant would represent the complex form of site monitoring. Within certain industries, such as chemical and power generation, safety systems are typically implemented to mitigate a disastrous event if control and other systems fail.

It is important to note that control systems were not always computer-based. In fact, there are still many pneumatic control systems; some are analog systems (based upon operational amplifier circuits), some are mechanical feedback systems, and others are hydraulic systems. The motivation for migrating controls toward digital computing platforms was primarily driven by increasingly complex systems and a need for embedded diagnostics. For example, the set-point for many pressure-reducing valves is made by setting the position of a hydraulic pilot valve configuration.

Besides guarding against both physical attack and system failure, organizations may establish backup control centers that include uninterruptible power supplies and backup generators (Shea, 2003, 2004).

Types of Control Systems

There are two primary types of control systems: Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. Distributed Control Systems, typically used within single processes, a generating plant, or over a smaller geographic area or single-site location, usually work in a strictly real-time environment. The term "real-time" in this context means that the time it takes to transmit data, process it, and command a device is fast enough to be negligible. A DCS usually polls data regularly and deterministically.

Supervisory Control and Data Acquisition systems are typically used for larger-scaled environments that may be geographically dispersed in an enterprise-wide distribution operation. A SCADA system may be a real-time computing environment, or it may have "near real-time" features. A SCADA system tends to have a more irregular and less-deterministic polling strategy than the DCS. To illustrate, a utility company may use a DCS to generate power, but would utilize a SCADA system to distribute it (Shea, 2003, 2004).

Operators tend to see "open control loops" (meaning control systems with a human in charge) in a SCADA system; conversely, operators tend to see "closed control loops" (with automation in charge) in DCS systems. Moreover, the SCADA system communications infrastructure tends to be lower bandwidth and longer range, so the RTU (Remote Terminal Unit) in a SCADA system has local control schemes to handle that eventuality. In a DCS, networks tend to be highly reliable, high bandwidth campus LANs (Local Area Networks). The remote sites in a DCS can not only afford to send more data but they can afford to centralize the processing of that data.