# Risk Assessment of a Power Plant: Evaluating the Security of a Supervisory Control and Data Acquisition System

**Scott D. Lathrop** **Christopher L. Gates**

**Darrell D. Massie, PhD, PE**
*Member ASHRAE*

**John M.D. Hill, Ph.D.**

## ABSTRACT

*With the increased potential of a bona fide cyber terrorist attack and the possibility of a future "war in the wires," we must continue to sterilize the networks connected to critical infrastructures. This paper provides a risk assessment of an existing operational computer network used to control a boiler system generating power and heat for an installation. The methodology used in evaluating the security of the system is described along with specific recommendations for minimizing the risk associated with connecting the network to the Internet for the purposes of remote data collection and administration. Our assessment and proposed recommendations may be applied to any critical infrastructure with a requirement for remote administration and/or data collection.*

## INTRODUCTION

As an aftermath of the terrorist events that occurred on September 11, 2001, the President of the United States created the Office of Homeland Security to analyze, plan, and coordinate the interior defense of the country. One of the critical components of this new organization was the creation of the President's Critical Infrastructure Protection Board (CIPB), tasked "to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems" (US 2003a). Within a year, the organization, in conjunction with computer security experts from academia, industry, and government, produced a draft of a national strategy to secure cyberspace that outlines some of the critical steps required for the United States to secure its information systems from deliberate cyber attacks. The key sectors addressed in this document were critical infrastructures such as banking and finance, transportation, and electrical power. This document was recently finalized and endorsed by the President of the United States (US 2003b).

The forensics analysis of al Qaeda computers seized from the caves of Afghanistan in the spring of 2002 suggests an extremely high level of interest from this terrorist group in how to remotely control, through the Internet, electrical substations, pipelines, dams, and communication grids (Gellman 2002). The devices used to control such systems remotely are called *supervisory control and data acquisition* (SCADA) systems. They use their own application protocol but employ the standard transmission control protocol/Internet protocol (TCP/IP) used by computers to communicate across the Internet and local intranets. The computer devices used to control critical systems and the protocols they use to communicate are often not well understood except by the vendors who develop them. Because they are not as common as the familiar Internet application protocols, they are not subject to the constant scrutiny of the Information Assurance (IA) community. However, the threat against such systems is real. One utility reported 100,000 scans a month in 2001 (Dagle et al. 2002).

The problem with such a situation is that assuming information systems are secure because the nodes on the network and the protocols used to communicate are obscure is a fatal mistake. Obscurity only slows the development of attacks on the system. Given enough time and money to replicate the devices used in the system, a motivated cyber agent or cyber warrior will develop tools to attack the system. The proliferation of such tools to the computer underground is then trivial (Welch 2002).

In this paper we describe a risk assessment of a power plant's information system. The power plant is real and oper-

**Scott D. Lathrop** and **John M.D. Hill** are senior research scientists at and **Christopher L. Gates** is with Information Technology and Operations Center, United States Military Academy, West Point, NY. **Darrell D. Massie** is with Intelligent Power & Energy Research Corporation, Fort Montgomery, NY.

ational with a network of control devices and computers controlling the plant's central boilers. The plant is capable of producing over 5 MW of electricity as well as central heating. Ultimately, the goal of the project is to reduce the cost of operating the plant by remotely administering the system and enabling a software application to dynamically control the mechanical equipment. The software makes decisions based on several attributes, such as electrical and fuel tariffs, ambient air temperature, and the number of personnel on site. The purpose of the assessment is to identify specific threats and vulnerabilities of the system and then take the necessary steps to minimize the risk associated with connecting the network to the Internet. In order to fully evaluate the network, we conducted a penetration test using open-source software tools that both cyber attackers (i.e., computer hackers) and computer security professionals use to evaluate network security. We emphasize open-source tools because these tools are freely available for download on the World Wide Web and, thus, could be obtained by anyone. An organization with more resources could purchase more advanced tools or modify the open-source software tools to fit their needs.

## Facilities and Motivation

The central plant was originally built in 1903 as a heating facility. However, upgrades over time have changed it into a cogeneration facility that is capable of providing up to 5.2 MW of emergency power. The plant consists of two 1.25 MW steam turbines and one 1.65 MW steam turbine. High pressure (1.2 MPa) and low pressure (184 kPa) steam lines, acting as the condenser for the plant, provide heat to buildings. Due to steam pipe losses and process loads, only 40% of the steam condensate returns to the central plant. Makeup feed water, from a local reservoir, is mixed with the condensation that returns from the heating load. Once mixed, the water is pumped to any combination of the three boilers in the system. In 1993, a 1.2 MW diesel generator intended for peak shaving (demand reduction) was added to the plant.

The organization purchases grid electrical power under a fixed price of demand (kW) plus energy charges (kWh), which vary by time of year. Since electricity can usually be purchased for less than it costs to produce it on site, local power generation is only economical for peak shaving or when cogeneration is possible. Since the only condensing capability is from the heating and processing loads, the steam turbines can only be economically run during winter months. The diesel generator may be operated at any time of year; however, waste heat recovery is not possible with the current configuration.

The plant had traditionally been controlled by operators who set its operation based upon their experience. Unfortunately, they often did not operate the plant optimally because they lacked access to certain information. Such information included site population, hourly weather predictions, and electrical price signals. In some cases, the plant operators were not trained in all the subtleties of plant operation. This sub-optimal performance can be improved with a clear methodology of how plant equipment operates and interacts.

An artificial intelligence agent-based software application is being developed that takes input from equipment sensors, building thermal loads, and an electrical profile coupled with rates from a remote location and determines the combination of equipment that would offer the least-cost option for providing power and heat. This information is used to produce accurate models, which increase the ability to operate the plant efficiently. While this information could be collected manually, operator error would be minimized if the program were fully automated.

The SCADA system uses component off-the-shelf (COTS) technology. The operating systems and the applications they run, along with the communication protocols used to exchange information between devices, are subject to the same sort of attacks that are used everyday on the Internet. The weakest link—the human element—is subject to attack through social engineering, weak or absent passwords, poor policy, and improper configurations.

The security of the system and assurance of its information are paramount. In order to provide the functionality desired, the system must be connected to the Internet. Preventing cyber attacks against the plant requires a risk assessment of the current infrastructure and hardening of the final implementation.

## Related Work

Published work in this area is very sparse. This may be because results of such assessments are not releasable to the public or, worse, tests such as described in this paper are not being conducted. Government and private agencies are continuing to investigate protection and security of critical infrastructure. Their recommendations consist of making industry aware of the threat and potential vulnerabilities associated with their SCADA systems, providing assistance in the form of a training and penetration tests similar to the one described in this paper, and establishing partnerships between the national laboratories and industry in order to leverage each organization's expertise. As in this paper, their presentation describes the typical vulnerabilities observed in SCADA systems (Dagle et al. 2002). The difference between this paper and their presentation is that we present a more thorough risk assessment, including results from a vulnerability assessment.

# RISK ASSESSMENT

We use the Information Assurance (IA) model (Figure 1) presented by Maconachy et al. (2001) as a framework for assessing an information system. The model describes four dimensions: (1) information states, (2) information services, (3) information security measures and countermeasures, and (4) time.

The power plant uses information that can be in any one of three states at any given point in time: (1) processing, (2) transmission, or (3) storage. When assessing the security of

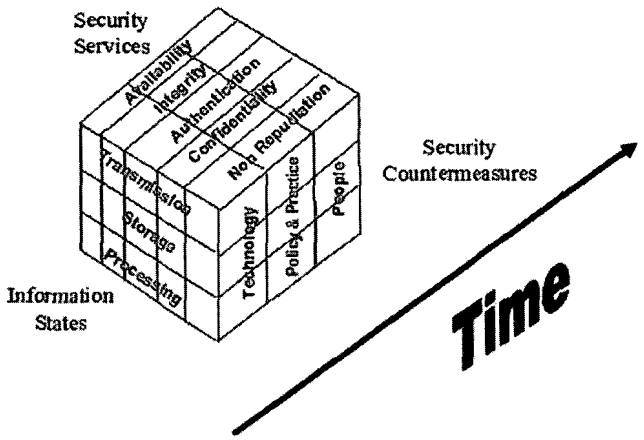


***Figure 1*** *Information assurance model.*

that information, one must consider all three states. The types of security services a system can provide include confidentiality, integrity, availability, authentication, and nonrepudiation. We focused our evaluation on the first three services. When considering where one may accept risk, confidentiality may be the least important attribute, as the power plant still operates even if an outsider is able to view the information. On the contrary, the integrity of the data is very significant. Any modification of the data may cause damage or loss. For example, a data packet with incorrect values may be sent to a boiler computer that in turn directs the combustion subsystem to overcompensate the air-to-fuel ratio. Or, incorrect information could be fed to the software application, leading to incorrect predictions. In every case, availability is important, as loss of data to the system degrades or possibly disables power and heat generation. Availability and integrity over time are particularly important factors for control systems, as updates to the controllers happen in real time. Any disruption to the flow of information can result in the system becoming desynchronized.

As with any risk assessment process, the ultimate goal is to reduce risk to an acceptable level without giving up the functionality and performance required by the organization. In the context of the IA model, risk is the probability that a particular threat is manifested against a specific vulnerability in the system that undermines availability, integrity, or confidentiality. One cannot eliminate risk in the information system without physically disconnecting the computers from the network and burying them in a hole. Obviously such a solution defeats the purpose of deploying and using the technology in the first place.

The model's security countermeasures enable one to reduce risk. These countermeasures include technology; policy, procedures, and practices; and the people within the organization administering and using the system. Most people will immediately associate security countermeasures with computer security applications such as firewalls, anti-virus software, and patches. In most cases, however, the people, policy, and procedures play the most important role in determining the overall security of an information system. Throughout the remainder of the paper we will use the IA model as a roadmap for our discussion. First we will look at the threat and potential attacks against the three security services we studied (confidentiality, integrity, and availability), then we will look at the vulnerabilities we found as they relate to each of the information states and provide recommendations in terms of the security countermeasures.

## The Threat

Based on our penetration test and an analysis of the protocols and platforms used in the power plant, we conclude that there are three major forms of attack against the power plant's infrastructure, each with an increasing degree of severity.

**Integrity Attack on the Information**. This type of attack involves modifying the information stored in databases and transmitted across the communication networks. Such an attack's visible end state is an unknown amount of decrease in the efficiency of the power plant's generation of power or heat, resulting in a higher cost of operating the plant. Such a scenario involves an attacker modifying the current cost of electrical power, number of personnel, ambient air temperature, or data returned from the boiler's sensors that is either stored in the databases or in transit. Modification to the data causes the software relying on the information to incorrectly adjust boilers and either over- or underproduce steam, resulting in an inefficient process, lack of confidence in the design capacity during critical loads, and any competitive edge that the control software was supposed to provide. This is exactly the opposite result desired by the designers of the agent-based control software.

**Availability Attack on Power Generation.** The second attack is an availability attack (also known as a *denial of service* attack). The attack causes degradation in the facility's ability to generate power. There are two possible ways an attacker could perform a denial of service attack against the power plant and effectively prevent it from producing power or heat. The first is a very overt, noisy attack where the attacker sends several thousand packets, or "pings of death" in hacker terminology, to control computers running on the power plant's internal network. The victimized computers become overwhelmed with packets and are unable to perform their primary function as they are busy attending to the large number of incoming packets. Another possibility for such an overt attack is for the attacker to execute an exploit that effectively shuts down a device on the network responsible for maintaining network connectivity. A network router is an example of such a device, and an exploit in this context is a computer program that takes advantage of a particular vulnerability in software. Once the router can no longer perform its connectivity function, communication ceases between computer nodes on the network, and information cannot be transferred to the boilers' controllers. This action results in degradation to default operations.