



Cyber Security

Power Industry Locks Down

Authors: Ernest Rakaczky, Director of Process Control Network Security, Invensys
Thomas Szudajski, Director of Global Power Marketing, Invensys

What's Inside:

1. Introduction
2. Open Exposure
3. Not Just an Engineering Problem
4. A Prevention-Based Cyber Security Architecture
5. Securing the Business Network
6. Securing the Plant Control Networks
7. Planned-in Prevention

1. Introduction

Like it or not, the power industry is susceptible to a variety of cyber threats, which can wreak havoc on control systems. Management, engineering and IT must commit to a comprehensive approach that encompasses threat prevention, detection and elimination.

Consider a couple of plausible threat scenarios:

CYBER- ATTACK SCENARIO 1

Using “war dialers,” simple personal computer programs that dial consecutive phone numbers looking for modems, a hacker finds modems connected to the programmable circuit breakers of the electric power control system, cracks passwords that control access to the circuit breakers, and changes the control settings to cause local power outages and damage equipment. He lowers the settings from, for example, 500 A to 200 A on some circuit breakers, taking those lines out of service and diverting power to neighboring lines. At the same time, he raises the settings on neighboring lines to 900 A, preventing the circuit breakers from tripping and overloading the lines. This causes significant damage to transformers and other critical equipment, resulting in lengthy repair outages.

CYBER-ATTACK SCENARIO 2

A power plant serving a large metropolitan district has successfully isolated the control system from the business network of the plant, installed state-of-the-art firewalls, and implemented intrusion detection and prevention technology. An engineer innocently downloads information on a continuing education seminar at a local college, inadvertently introducing a virus into the control network. Just before the morning peak, the operator screens go blank and the system is shut down.

Although the above scenarios are hypothetical, they represent the kinds of real threats facing cyber security experts around the world. Cyber security has become as much a part of doing business in the 21st century as traditional building security was in the last. While power engineers have always taken measures to maximize the security and safety of their operations, heightened global terrorism and increased hacker activity have added a new level of urgency and concern.

Many plants are convinced their networks are isolated and consequently secure, but without ongoing audits and intrusion detection, that security could be just a mirage. Moreover, the growing demand for open information sharing between business and production networks increases the need to secure transactions and data. For power generating companies, where consequences of an attack could have widespread impact, the need for cyber security is even more pressing.

A recent U.S. General Accounting Office report, titled Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems, offered the following examples of actions that might be taken against a control system:

- Disruption of operation by delaying or blocking information flow through control networks, thereby denying network availability to control system operators
- Making unauthorized changes to programmed instructions in programmable logic controllers (PLCs), remote terminal units (RTUs) or distributed control system (DCS) controllers, changing alarm thresholds or issuing unauthorized commands to control equipment. This could potentially result in damage to equipment, premature shutdown, or disabling of control equipment.
- Sending false information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators
- Modifying control system software, producing unpredictable results
- Interfering with operation of safety systems

Historically, control system vendors have dealt with such threats by focusing on meeting customer specifications within guidelines and metrics set by industry standards groups such as the Institute of Electrical and Electronics Engineers (IEEE) and Instrument Society of America (ISA). Indeed, much of this compliance was designed into proprietary equipment and applications, which were beyond the skills of all but the most determined cyber attacker. Increasingly, however, process control networks are better equipped for gathering information about generation and distribution and sharing it with business networks using standard communications protocols such as Ethernet or IP. These open protocols are being used to communicate between dispatch, marketing, corporate headquarters and plant control rooms as well. While such sharing enables more strategic management of enterprise assets, it does increase security requirements.

2. Open Exposure

The open and interoperable nature of today's industrial automation systems - many of which use the same computing and networking technologies as general purpose IT systems - requires engineers to pay close attention to network and cyber security issues. Not doing so can potentially lead to injury or loss of life; environmental damage; corporate liability; loss of corporate license to operate; loss of production, damage to equipment; and reduced quality of service.

Such threats can come from many sources, external and internal, ranging from terrorists and disgruntled employees to environmental groups and common criminals. Making matters worse, the technical knowledge, skills and tools required for penetrating IT and plant systems are becoming more widely available. Figure 1 shows that as the incidence of threats increases, the level of sophistication necessary to implement an attack is decreasing, making it all the easier for intruders.

Many companies are bracing for the worst. Major power producers, for example, have begun paying greater attention to security, as manifested by active participation in industry standards groups, including the Department of Energy, the Federal Energy Regulatory Commission, and the North American Electric Reliability Council.

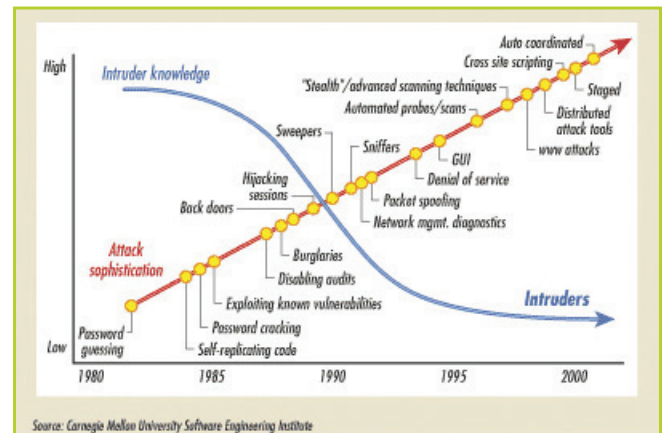


Figure 1: Attack Sophistication versus Intruder Knowledge.

Power producers have also been putting more pressure on automation suppliers and their partners to accelerate development of technologies that will support compliance with emerging standards. The power industry is looking to non-traditional suppliers to improve control room design and access, operator training, and procedures affecting control system security that lie outside the domain of control system vendors.

3. Not Just an Engineering Problem

While power engineers will play a critical role in hardening power operations against intruders, collaboration and support of both corporate management and the IT department is essential. A company-wide vulnerability audit of a large U.S. utility revealed some areas of technical vulnerability in the control system, but most of the findings had to do with organizational issues:

- Lack of plant-wide awareness of cyber security issues in general
- Inconsistent administration of systems (managed by different business units)
- Lack of a cyber security incident response plan
- Poor physical access to some critical assets
- Lack of a management protocol for accessing cyber resources
- Lack of a change management process
- Undocumented perimeter access points
- Lack of a disaster recovery plan
- Inability to measure known vulnerabilities

Corporate management must first acknowledge the need for secure operations. Then, because few companies will have the resources to harden all processes against all possible threats, management must guide development of a security policy that will set organizational security priorities and goals. Finally, companies must foster collaboration among all layers of management, IT and project and plant engineering. Project engineers need to understand the security risks and possible mitigation strategies. IT, which brings much of the security expertise, must understand the need for real-time availability to keep units online.

Cyber Security

Power Industry Locks Down

With priorities in place, engineering and IT can work together to create a plan that should, at a minimum, address the following issues:

- An approach to convergence of IT and plant networks
- A process for managing secure and insecure protocols on the same network
- Methods for monitoring, alerting and diagnosing plant network control systems and their integration with the corporate network
- A method for retaining forensic information to support investigation/legal litigation
- A means of securing connectivity to wireless devices

Management must also recognize that investment in prevention will have a far greater payback than investment in detection and removal. Although investment in the latter areas may be necessary to ward off immediate threats, focusing on activities that prevent attacks in the first place will reduce the need for future detection and removal expenditures.

Embracing open standards in the age of cyber-terrorism is another pressing management issue. While sticking with proprietary technologies may seem much less vulnerable to intrusion, doing so will limit reliability, availability and efficiency improvements that could be available from integration of digital technologies and advanced applications. In fact, proprietary technology could become even more expensive as vendors seek to recover the cost of additional hardening that may still be needed, since these systems are secure owing only to their obscurity, not to some inherent capability. Management support at the highest levels will help ensure that any technical hardening is implemented most strategically and cost-effectively.

4. A Prevention-Based Cyber Security Architecture

One of the most effective ways to implement a prevention-based, standards-driven cyber security architecture is to segment the network into several zones, each of which would have a different set of connectivity requirements and traffic patterns. Firewalls placed at strategic locations provide the segmentation. Intrusion detection and prevention systems are also deployed at key locations and alerts are reported to a monitoring center. Figure 2 illustrates a multi-zone cyber security architecture, consisting of five segments:

- The **Internet Zone**, which is the unprotected public Internet
- The **Data Center Zone**, which may be a single zone or multiple zones that exist at the corporate data center, dispatch and corporate engineering
- The **Plant Network Zone**, which carries the general business network traffic (messaging, ERP, file and print sharing, and Internet browsing). This zone may span multiple locations across a wide area network. Traffic from this zone may not directly access the Control Network Zone
- The **Control Network Zone**, which has the highest level of security, carries the process control device and application communications. Traffic on this network segment must be limited to only the process control network traffic as it is very sensitive to the volume of traffic and protocols used
- The **Field I/O Zone**, where communications are typically direct hard wired between the I/O devices and their controllers. Security is accomplished by physical security means.

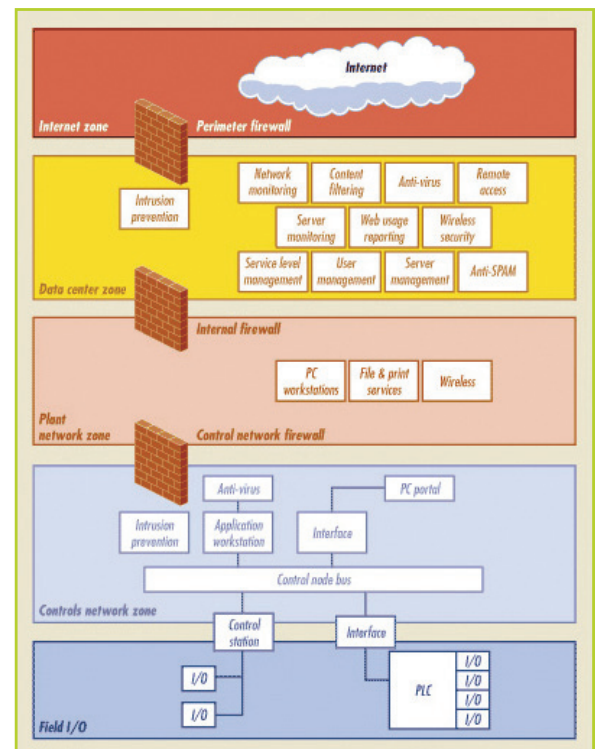


Figure 2: Multi-Zone Cyber Security Architecture.

An extra level of control - commonly implemented as DMZs on the firewall - is often added for supplemental security. These supplemental zones are typically used for data acquisition, service and support, a public zone and an extranet sub-zone.

The Data Acquisition and Interface Sub-Zone is the demarcation point and interface for all communications into or out of the process control network. This sub-zone contains servers or workstations that gather data from the controls network devices and make it available to the plant network.

The Service and Support Sub-Zone is typically used by outsourcing agencies, equipment vendors or other external support providers that may be servicing the controls network. This connection point should be treated no differently than any other connection to the outside world and should therefore utilize strong authentication, encryption or secure VPN access. Modems should incorporate encryption and dial-back capability. Devices introduced to the network should use updated anti-virus software. This last item is particularly important for service providers, who will often bring a PC into the plant for analysis. An example is turbine monitoring. What's more, power companies should audit outsourcing providers for adequate security measures.

The Public Sub-Zone is where public facing services exist. Web servers, SMTP messaging gateways and FTP sites are examples of services found in this sub-zone.

The Extranet Sub-Zone is commonly used to connect to the company's trading partners. Partners connect to these by various methods including dialup, private lines, frame-relay and VPN. VPN connections are becoming more common due to the proliferation of the Internet and the economy of leveraging shared services. Firewall rules are used to further control where the partners are allowed access as well as address translation.

5. Securing the Business Network

The two most critical components of data center security are a perimeter firewall and an internal firewall. The perimeter firewall controls the types of traffic to and from the public Internet while the internal firewall controls the types of internal site-to-site traffic and site-to-data center traffic. The internal firewall is essential for controlling or containing the spread of network-born viruses. It also restricts types of traffic allowed between sites and provides and protects the data center from internal intruders.

6. Securing the Plant Control Networks

At the plant control network level are the firewall, intrusion detection and prevention technology, modems, and wireless access points - all of which are integrated with a communications infrastructure involving equipment such as routers, bridges and switches.

Firewalls restrict the types of traffic allowed into and out of the control network zone, and can be configured with rules that permit only traffic designated as essential, triggering alarms for noncompliant traffic. Alarms should be monitored 24/7, either by an internal or third party group. In addition, each unit's network should be isolated, in particular from remote sites. This is extremely important for recovery.

The firewall should use a logging server to capture all firewall events either locally or in a central location. One can, for example, configure the firewall to allow remote telnet access to the control network, but while the firewall can monitor access to connections, it cannot provide information about what someone might be attempting to do with those connections. A hacker could be accessing the control system through telnet and the firewall would have no way of knowing whether the activity is from friend or foe. That is the job of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), which can detect usage patterns.

An IDS monitors packets on a network wire and determines if the seen activity is potentially harmful. A typical example is a system that watches for a large number of TCP connection requests to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan. An IDS may run either on the target machine, which watches its own traffic, or on an independent machine such as an IDS appliance (also referred to as Host IDS).

An IPS complements the IDS by blocking the traffic that exhibits dangerous behavior patterns. It prevents attacks from harming the network or control system by sitting in between the connection and the network and the devices being protected. Like an IDS, an IPS can run in host mode directly on the control system station, and the closer to the control system it is, the better the protection.

Modems connect devices asynchronously for out-of-band access to devices. Because modems can connect outside directly through public carriers, they are unaffected by security measures and represent a significant point of vulnerability. At the very least, any modem with links to the main control network should be a dial-back modem, which will not transmit data until it receives dial-back authentication from the receiving system. For sensitive data, encryption is also recommended.

Wireless access points are radio-based stations that connect to the hard-wired network. Wireless communications can be supported if implemented securely. Solutions provided must be capable of both preventing unauthorized access and ensuring that data transmitted is encrypted to prevent "eavesdropping." For maximum flexibility, devices must be capable of data encryption with dynamic or rotating keys; filtering or blocking Media Access Control (MAC) addresses that uniquely identify each network node; disabling broadcasting of Service Set Identifiers (SSID), passwords that authorize wireless LAN connections; and compliance with 802.11 & 802.1x standards. Consumer grade equipment is not recommended and VPN connection with software clients is preferable to WEP or proprietary data encryption. This allows support for multi-vendor wireless hardware with a common solution.

VPN concentrators are devices that encrypt the data transferred between the concentrator and another concentrator or client based on a mutually agreed upon key. This technology is most widely used today to allow remote users to securely access corporate data across the public Internet. The same technology can be used to add additional security accessing data across wireless and existing corporate WANs. In lieu of a separate VPN concentrator, it is possible to utilize VPN services that are integrated with the firewall.

While the firewalls, IDS, IDP and encryption, add the greatest hardening, they must work in tandem with the existing communications infrastructure. The job of the routers, hubs, bridges, switches, media converters and access units is to keep network information packets flowing at the desired speed without collision. The more network traffic is routed, segmented and managed, the more easily any intrusion can be contained and eliminated.

Although some of these systems do have certain levels of security functionality built in, it is not wise to rely on that to protect mission-critical data. Routers, for example, can be configured to mimic basic firewall functionality by screening traffic based on an approved access list, but they lack a hardened operating system and other robust capabilities of a true firewall.

7. Planned-in Prevention

Developing a prevention approach to plant control systems will require a new approach to network security between the plant network layer and business/external systems. It is an ongoing process that begins with awareness and assessment, continues through the creation of policy and procedures and the development of the security solution, and includes ongoing security performance management.

Some of the key activities for the awareness and assessment phase include defining security objectives, identifying system vulnerabilities, establishing the security plan and identifying the key players on the security team. In this phase, one is determining which networks are involved and how isolated they are from each other. Is there a DCS for common systems, coal handling, service water, for example? How vulnerable are remote facilities, such as landfill and water treatment?

At the policy and procedures phase, one would review safety and security aspects of established industry standards such as ISO 17799, ISA-SP99, META, and CERT along with regulatory drivers, such as those offered by FERC, NERC, and DOE. Local regulatory requirements related to site security and safety must also be considered.

The security solution phase is where one would focus on technologies and processes for system access control, perimeter security and isolation, identity and encryption, intrusion detection and system management. In the security program performance and management phase, one would address continual monitoring and alerting, yearly audits, periodic testing and evaluation, and continual updating of system requirements.

Following the procedures defined above will not guarantee immunity from cyber attack, but will ensure that the risk has been managed as strategically and cost-effectively as possible.