CRITICAL INFRASTRUCTURE PROTECTION – CHALLENGES AND EFFORTS TO SECURE CONTROL SYSTEMS –

BOARU GHEORGHE, BĂDIȚA GEORGE-IONUȚ

Universitatea Națională de Apărare „Carol I”

Abstract

The increase in the interconnectivity between computers, especially those connected to the Internet continues to revolutionize the manner the governments, nations, the economic and financial community communicates and does business. However, increasing the interconnectivity will expose the computers of a country or a government to great risks. A greater threat is the risk arising from the reliance on critical operations and infrastructures that support such activities to the control information systems. The main risks to the control system are not physical (as considered until recently), but the cyber attacks that can have very different origins: hostile governments, terrorist groups, dissatisfied employees etc.

Historically, security concerns about control systems were related primarily to protecting them against physical attack and preventing the misuse of refining and processing sites or distribution and holding facilities. However, more recently, there has been a growing recognition that control systems are now vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way governments, nations, and much of the world communicate and conduct business. The benefits have

been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day, and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with an unlimited number of individuals and groups.

However, this widespread interconnectivity poses significant risks to the government’s and nation’s computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution systems, water supplies, public health services, national defense (including the military’s warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. If not properly controlled, the speed and accessibility that create the enormous benefits of the computer age may allow individuals and organizations to eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

What are control systems?

Control systems are computer-based systems that are used within 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, control systems can manage and control the generation, transmission, and distribution of electric power - for example, by opening and closing circuit breakers and setting thresholds for preventive shutdowns.

Employing integrated control systems, the oil and gas industry can control the refining operations at a plant site, remotely monitor the pressure and flow of gas pipelines, and control the flow and pathways of gas transmission.

Water utilities can remotely monitor well levels and control the wells' pumps; monitor flows, tank levels, or pressure in storage tanks; monitor water quality characteristics - such as pH, turbidity, and chlorine residual; and control the addition of chemicals.

Control systems also are used in manufacturing and chemical processing. Control systems perform functions that vary from simple to complex; they can be used simply to monitor processes - for example, the environmental conditions in a small office building - or to manage most activities in a municipal water system or even a nuclear power plant.

In certain industries, such as chemical and power generation, safety systems are typically implemented in order to mitigate a potentially disastrous event if control and other systems should fail. In addition, to guard against both physical attack and system failure, organizations may establish backup control centers that include uninterruptible power supplies and backup generators.

There are two primary types of control systems. Distributed Control Systems (DCS) typically are used within a single processing or generating plant or over a small geographic area. Supervisory Control and Data Acquisition (SCADA) systems typically are used for large, geographically dispersed distribution operations. For example, a utility company may use a DCS to generate power and a SCADA system to distribute it. Figure 1 illustrates the typical components of a control system.

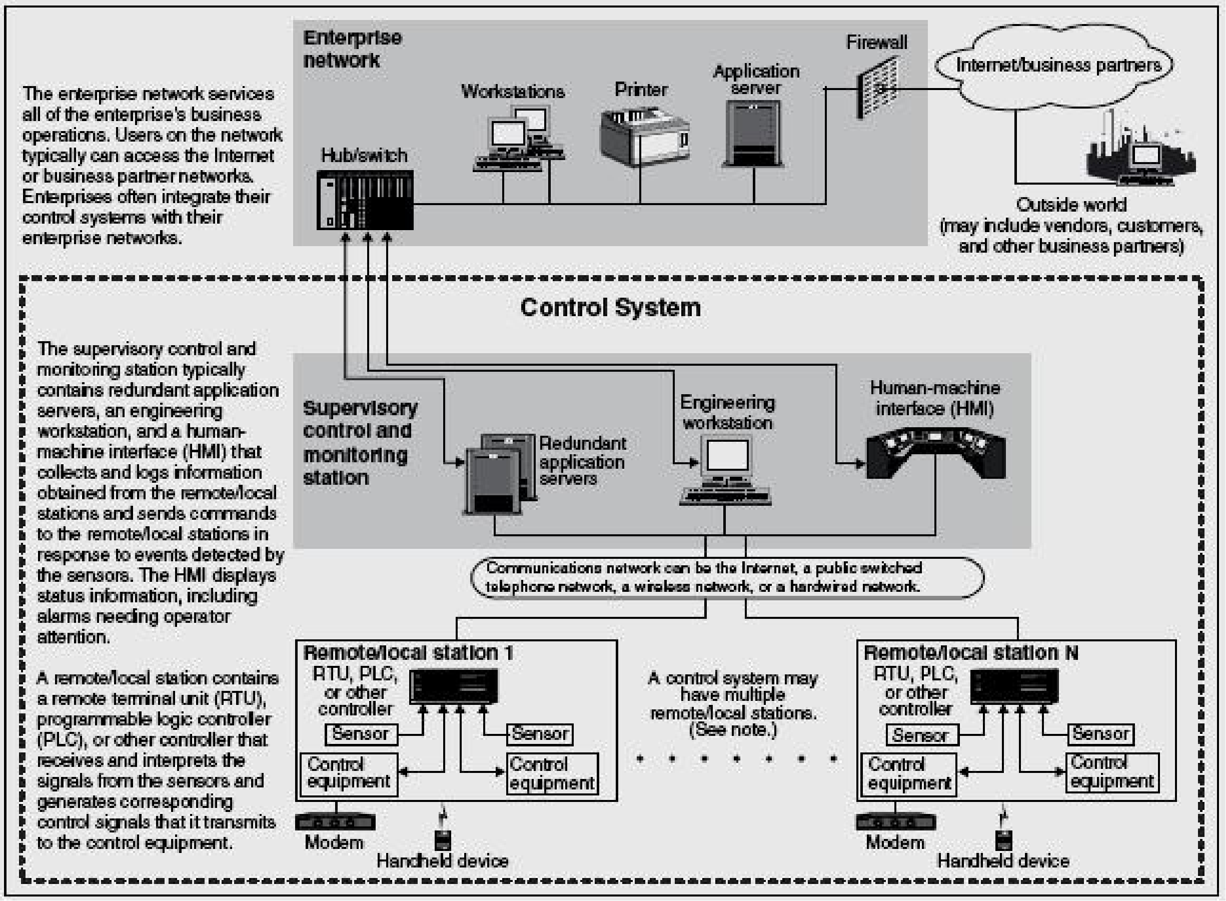
Enterprise network
The enterprise network services all of the enterprise's business operations. Users on the network typically can access the Internet or business partner networks. Enterprises often integrate their control systems with their enterprise networks.
Hub/switch
Workstations
Printer
Application server
Firewall
Internet/business partners
Outside world (may include vendors, customers, and other business partners)
Control System
The supervisory control and monitoring station typically contains redundant application servers, an engineering workstation, and a human-machine interface (HMI) that collects and logs information obtained from the remote/local stations and sends commands to the remote/local stations in response to events detected by the sensors. The HMI displays status information, including alarms needing operator attention.
Supervisory control and monitoring station
Redundant application servers
Engineering workstation
Human-machine interface (HMI)
Communications network can be the Internet, a public switched telephone network, a wireless network, or a hardwired network.
A remote/local station contains a remote terminal unit (RTU), programmable logic controller (PLC), or other controller that receives and interprets the signals from the sensors and generates corresponding control signals that it transmits to the control equipment.
Remote/local station 1
RTU, PLC, or other controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device
A control system may have multiple remote/local stations. (See note.)
Remote/local station N
RTU, PLC, or other controller
Sensor
Sensor
Control equipment
Control equipment
Modem
Handheld device

Fig. 1. Typical Components of a Control System

A control system typically is made up of a “master” or central supervisory control and monitoring station consisting of one or more human-machine interfaces where an operator can view status information about the remote/local sites and issue commands directly to the system. Typically, this station is located at a main site, along with application servers and an engineering workstation that is used to configure and troubleshoot the other components of the control system. The supervisory control and monitoring station typically is connected to local controller stations through a hard-wired network or to a remote controller station through a communications network—which could be the Internet, a public switched telephone network, or a cable or wireless (e.g., radio, microwave, or Wi-Fi7) network. Each controller station has a remote terminal unit (RTU), a programmable logic controller (PLC), or some other controller that communicates with the supervisory control and monitoring station.

The control system also includes sensors and control equipment that connect directly with the working components of the infrastructure - for example, pipelines, water towers, or power lines. The sensor takes readings from the infrastructure equipment - such as water or pressure levels, electrical voltage or current - and sends a message to the controller. The controller may be programmed to determine a course of action and send a message to the control equipment instructing it what to do - for example, to turn off a valve or dispense a chemical. If the controller is not programmed to determine a course of action, the controller communicates with the supervisory control and monitoring station and relays instructions back to the control equipment. The control system also can be programmed to issue alarms to the operator when certain conditions are detected. Handheld devices, such as personal digital assistants, can be used to locally monitor controller stations. Experts report that technologies in controller stations are becoming more intelligent and automated and are able to communicate with the supervisory central monitoring and control station less frequently, thus requiring less human intervention.

Control Systems' Risks

Historically, security concerns about control systems were related primarily to protecting them against physical attack and preventing the misuse of refining and processing sites or distribution and holding facilities. However, more recently, there has been a growing recognition that control systems are now vulnerable to cyber attacks from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and other malicious intruders.

Several factors have contributed to the escalation of risk to control systems, including (1) the adoption of standardized technologies with known vulnerabilities, (2) the connectivity of control systems to other networks, (3) insecure remote connections, and (4) the widespread availability of technical information about control systems.

Control Systems Are Adopting Standardized Technologies with Known Vulnerabilities

In the past, proprietary hardware, software, and network protocols made it difficult to understand how control systems operated - and therefore how to hack into them. Today, however, to reduce costs and improve performance, organizations have been transitioning from proprietary systems to less expensive, standardized technologies such as Microsoft's Windows, Unix-like operating systems, and the common networking protocols used by the Internet. These widely-used, standardized technologies have commonly known vulnerabilities, and sophisticated and effective exploitation tools are widely available and relatively easy to use. As a consequence, both the number of people with the knowledge to wage attacks and the number of systems subject to attack have increased. Also, common communication protocols and the emerging use of extensible markup language (commonly referred to as XML) can make it easier for a hacker to interpret the content of communications among the components of a control system.

Control Systems are Connected to Other Networks

Enterprises often integrate their control systems with their enterprise networks. This increased connectivity has significant advantages, including providing decision makers with access to real-time information and allowing engineers to monitor and control the process control system from different points on the enterprise network. In addition, the enterprise networks are often connected to the networks of strategic partners and to the Internet. Furthermore, control systems are increasingly using wide area networks and the Internet to transmit data to their remote or local stations and individual devices. This convergence of control networks with public and enterprise networks potentially creates further security vulnerabilities in control systems. Unless appropriate security controls are deployed in both the enterprise network and the control system network, breaches in enterprise security can affect the operation of control systems.

Insecure Connections Exacerbate Vulnerabilities

Vulnerabilities in control systems are exacerbated by insecure connections. Organizations often leave access links - such as dial-up modems to equipment and control information - open for remote diagnostics, maintenance, and examination of system status. If such links are not protected with authentication or encryption, the risk increases that hackers could use these insecure connections to break into remotely controlled systems. Also, control systems often use wireless communications systems, which are especially vulnerable to attack, or leased lines that pass through commercial telecommunications facilities. Without encryption to protect data as it flows through these insecure connections or authentication mechanisms to limit access, there is little to protect the integrity of the information being transmitted.

Information about Infrastructures and Control Systems Is Publicly Available

Public information about infrastructures and control systems is readily available to potential hackers and intruders. The availability of this infrastructure and vulnerability data was demonstrated last year by a George Mason University graduate student who, in his dissertation, reportedly mapped every business and industrial sector in the American economy to the fiber-optic network that connects them, using material that was available publicly on the Internet - and not classified. For example: in the electric power industry, open sources of information - such as product data and educational videotapes from engineering associations - can be used to understand the basics of the electrical grid.

Cyber Threats to Control Systems

There is a general consensus - and increasing concern - among government officials and experts on control systems about potential cyber threats to the control systems that govern critical infrastructures. As components of control systems increasingly make vital decisions that were once made by humans, the potential effect of a cyber attack becomes more devastating. Cyber threats could come from numerous sources ranging from hostile governments and terrorist groups to disgruntled employees and other malicious intruders. Based on interviews and discussions with representatives from throughout the American electric power industry, an organization with sufficient resources, such as a foreign intelligence service or a well-supported terrorist group, could conduct a structured attack on the electric power grid electronically, with a high degree of anonymity, and without having to set foot in the target nation.

According to the National Institute of Standards and Technology (NIST-USA), cyber attacks on energy production and distribution systems -including electric, oil, gas, and water treatment, as well as on chemical plants containing potentially hazardous substances - could endanger public health and safety, damage the environment, and have serious financial implications such as loss of production, generation, or distribution by public utilities; compromise of proprietary information; or liability issues. When backups for damaged components are not readily available (e.g., extra-high - voltage transformers for the electric power grid), such damage could have a long-lasting effect.

Control Systems Can Be Vulnerable to Cyber Attacks

Entities or individuals with malicious intent might take one or more of the following actions to successfully attack control systems:

- disrupt the operation of control systems by delaying or blocking the flow of information through control networks, thereby denying availability of the networks to control system operators;
- make unauthorized changes to programmed instructions in PLCs, RTUs, or DCS controllers, change alarm thresholds, or issue unauthorized commands to control equipment, which could potentially result in damage to equipment (if

tolerances are exceeded), premature shutdown of processes (such as prematurely shutting down transmission lines), or even disabling control equipment;

- send false information to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators;
- modify the control system software, producing unpredictable results; and
- interfere with the operation of safety systems.

In addition, in control systems that cover a wide geographic area, the remote sites often are not staffed and may not be physically monitored. If such remote systems are physically breached, attackers could establish a cyber connection to the control network.

Securing Control Systems Poses Significant Challenges

The control systems community faces several challenges to securing control systems against cyber threats. These challenges include (1) the limitations of current security technologies in securing control systems, (2) the perception that securing control systems may not be economically justifiable, and (3) the conflicting priorities within organizations regarding the security of control systems.

Lack of Specialized Security Technologies for Control Systems

According to industry experts, existing security technologies, as well as strong user authentication and patch management practices, are generally not implemented in control systems because control systems usually have limited processing capabilities, operate in real time, and are typically not designed with cybersecurity in mind.

Existing security technologies such as authorization, authentication, encryption, intrusion detection, and filtering of network traffic and communications, require more bandwidth, processing power, and memory than control system components typically have. Controller stations are generally designed to do specific tasks, and they often use low-cost, resource-constrained microprocessors. In fact, some control system devices still use the Intel 8088 processor, which was introduced in 1978. Consequently, it is difficult to install current security technologies without seriously degrading the performance of the control system.

For example, complex passwords and other strong password practices are not always used to prevent unauthorized access to control systems, in part because this could hinder a rapid response to safety procedures during an emergency. As a result, according to experts, weak passwords that are easy to guess, shared, and infrequently changed are reportedly common in control systems, including the use of default passwords or even no password at all.

In addition, although modern control systems are based on standard operating systems, they are typically customized to support control system applications. Consequently, vendor-provided software patches may be either incompatible with the customized version of the operating system or difficult to implement without compromising service by shutting down “always-on” systems or affecting interdependent operations. Another constraint on deploying patches is that support agreements with control system vendors often require the vendor’s approval before the user can install patches. If a patch is installed in violation of the support agreement, the vendor will not take responsibility for potential impacts on the operations of the system. Moreover, because a control system vendor often requires that it be the sole provider of patches, if the vendor delays in providing patches, systems remain vulnerable without recourse.

Information security organizations have noted that a gap exists between currently available security technologies and the need for additional research and development to secure control systems. Research and development in a wide range of areas could lead to more effective technologies. For example, although technologies such as robust firewalls and strong authentication can be employed to better segment control systems from external networks, research and development could help to address the application of security technologies to the control systems themselves. Other areas that have been noted for possible research and development include identifying the types of security technologies needed for different control system applications, determining acceptable performance trade-offs, and recognizing attack patterns for use in intrusion detection systems.

Industry experts have identified challenges in migrating system components to newer technologies while maintaining uninterrupted operations. Upgrading all the components of a control system can be a lengthy process, and the enhanced security features of newly installed technologies - such as their ability to interpret encrypted messages - may not be able to be fully utilized until all devices in the system have been replaced and the upgrade is complete.

Securing Control Systems May Not Be Perceived as Economically Justifiable

Experts and industry representatives have indicated that organizations may be reluctant to spend more money to secure control systems. Hardening the security of control systems would require industries to expend more resources, including acquiring more personnel, providing training for personnel, and potentially prematurely replacing current systems, which typically have a lifespan of about 20 years.

Several vendors suggested that since there have been no reports of significant disruptions caused by cyber attacks on U.S. control systems, industry representatives believe the threat of such an attack is low. While incidents have occurred, to date there is no formalized process for collecting and analyzing information about control systems incidents, thus further contributing to the skepticism of control systems vendors. We have previously recommended that the government work with the private sector to improve the quality and quantity of information being shared among industries and government about attacks on the nation's critical infrastructures.

Until industry users of control systems have a business case to justify why additional security is needed, there may be little market incentive for the private sector to develop and implement more secure control systems.

Organizational Priorities Conflict

Finally, several experts and industry representatives indicated that the responsibility for securing control systems typically includes two separate groups: (1) IT security personnel and (2) control system engineers and operators. IT security personnel tend to focus on securing enterprise systems, while control system engineers and operators tend to be more concerned with the reliable performance of their control systems. These experts indicate that, as a result, those two groups do not always fully understand each other's requirements and so may not collaborate to implement secure control systems.

These conflicting priorities may perpetuate a lack of awareness of IT security strategies that could be deployed to mitigate the vulnerabilities of control systems without affecting their performance. Although research and development will be necessary to develop technologies to secure individual control system devices, existing IT security technologies and approaches could be implemented as part of a secure enterprise architecture to protect the perimeters of, and access to, control system networks. Existing IT security technologies include firewalls, intrusion-detection systems, encryption, authentication, and authorization. IT security approaches include segmenting control system networks and testing continuity plans to ensure safe and continued operation. To reduce the vulnerabilities of its control system, officials from one company formed a team composed of IT staff, process control engineers, and manufacturing employees. This team worked collaboratively to research vulnerabilities and to test fixes and workarounds.

Efforts to Strengthen the Cybersecurity of Control Systems

- Research and development of new security technologies to protect control systems;

• Development of requirements and standards for control system security;

• Increased awareness of security and sharing of information about the implementation of more secure architectures and existing security technologies;

• Implementation of effective security management programs, including policies and guidance that consider control system security.

Conclusions

The systems that monitor and control the sensitive processes and physical functions of the nation's critical infrastructures are at increasing risk from threats of cyber attacks. Securing these systems poses significant challenges. At international level, numerous agencies, critical infrastructure sectors, and standards-creating bodies are leading various initiatives to address these challenges. While some coordination is occurring, the cybersecurity of critical infrastructures' control systems could benefit from greater collaboration among all entities.

BIBLIOGRAPHY:

[1]. Col. John R. Martin, *Defeating terrorism*, , January 2002, http://books.google.com/books.

[2]. *Making the Nation Safer, The Role of Science and Technology in Countering Terrorism*, National Research Council, The National Academies Press, http://books.google.com/books.

[3]. *Cybersecurity for Critical Infrastructure Protection*, http://books.google.com/books.

[4]. *An army at war – Change in the mist of conflict. The proceedings of the Combat*, Studies Institute 2005 Military History Symposium, http://books.google.com/books.

[5]. *US Foreign Policy,* Agenda, Vol. 6.