The Role of SCADA in Securing Our Critical Infrastructure
By Hany Fouda

Supervisory Control and Data Acquisition (SCADA) systems are critical to the safe, reliable and efficient operation of many essential services that affect the daily lives of millions of North Americans. These services include power generation plants, potable water systems, wastewater treatment facilities, oil and gas production and transportation/distribution networks. SCADA systems typically consist of standalone or networked computers, application software, communication media and protocols, field controllers such as PLCs/RTUs, sensors, intelligent electronic devices (IED), back-up batteries and other auxiliary equipment. System size and complexity can range anywhere from a few remote sites, with a handful of parameters, to several hundreds of sites comprising thousands of measurement and control parameters. By monitoring and controlling remote equipment and resources such as pumps, valves, tanks, wells and pipelines; and collecting and analyzing sensitive data such as production parameters, consumption and distribution schemes; SCADA systems provide greater efficiency, in terms of faster and more coordinated system control, than human operation; as well as lower operational costs and better use of scarce human and financial resources.

The Sobering Fact
Yet despite the many benefits and undisputed efficiency and reliability of SCADA systems, they can present a security risk. SCADA systems are mainly designed to maximize functionality, operational efficiency and robustness. Consequently, not enough attention is paid to security. By nature, SCADA systems monitor/control equipment and assets that are dispersed over a vast geographical area, from a central location. However, many sites are in remote locations, making them ideal targets for intruders and vandalism. In addition, the adoption of standard technologies with known vulnerabilities, the widespread use of commercial off-the-shelf equipment, and the increased connectivity of SCADA systems to the Internet, have only aggravated matters. This has made some systems potentially vulnerable to cyber attacks, vandalism and other types of malicious mischief that could result in disruption of services, process re-direction and manipulation of operational data. All these weaknesses put public safety at risk.

Several verified security-breach incidents include:

- In March 1997, a teenager in Worcester, Massachusetts, remotely disabled part of the public switching network, which disrupted telephone service to residents and the fire department, and caused a malfunction at the local airport.
- In the spring of 2000, a former employee of an Australian industrial software company used a radio transmitter, on as many as forty-six separate occasions, to remotely hack into the controls of a sewage treatment system at Maroochy Shire, Queensland, ultimately releasing approximately 264,000 gallons of raw sewage into nearby rivers.
- In November 2003, a Washington man admitted to tampering with more than twenty high-voltage transmission towers in four western states. He wanted to point out the power system's vulnerabilities. He succeeded!
- In August 2003, an SQL server worm, known as Slammer, infected a private computer network at the Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. Furthermore, the plant’s process computer failed, and it took about 6 hours for it to come online again. Slammer also affected communications on the control networks of at least five other utilities by propagating so quickly that control system traffic was effectively blocked.

These incidents, among many others, highlight the importance of physical and cyber security in SCADA systems.
The Role of SCADA in Security
Since most utilities operate with budget restraints and limited personnel, keeping an eye on remote
equipment and resources is challenging. However, modern SCADA systems can significantly extend the
ability to secure remote assets and provide the tools necessary to mitigate current and future risks.
The issue of physical security, i.e. access-control, intrusion-detection, perimeter-control and cameras, can
be tied to an existing SCADA system in order to provide a wider view of the situation at remote sites and
allow for coordinated responses from the utility. For example, a keyless entry device such as a card
reader, connected serially to a PLC/RTU, would allow site access to be automatically time-stamped in the
controller as well as at the central site. A motion or intrusion detector can be connected to the PLC/RTU
digital input board, providing instant alarm notification and logging at the central site. Intrusion sensors
can also be deployed at access gates, doors, ladders and manholes. Alarm records would then be
correlated with other operational information to obtain a very precise picture of the overall situation.
Furthermore, due to the widespread use of high-bandwidth wide area networks (WANs), inexpensive IP-
based web cameras can be utilized to provide video frames from remote locations. These video pictures
would be transmitted over a wireless IP radio network, such as Ethernet Spread Spectrum radios and Wi-
Fi technology, or by using conventional wire-based networks such as fiber optic and high speed leased
lines.
Physical security can also be part of a SCADA system’s comprehensive control and operation strategy. For example, if a remote site has been breached, the SCADA system can automatically perform a safe shutdown of the remote assets in order to isolate the problem and limit widespread service disruption or contamination. SCADA systems can also be utilized as an advance warning system against biological and chemical threats. The release of harmful amounts of water treatment chemicals, such as chlorine, into the public’s drinking systems would be devastating. A water system that continuously monitors and logs water quality parameters such as pH, turbidity, chlorine level, and dissolved oxygen can quickly detect equipment malfunction, contamination or raw sewage spillage.

In addition to enhancing physical security, cyber security (also known as network security) must not be ignored. Traditionally, in medium to large utilities, physical and cyber security were two completely independent functions handled by separate groups. Recently, however, the line separating both functions has disappeared, bringing an increased focus on protecting both bricks and bytes. SCADA systems, like all computer networks, are vulnerable to hacking, intrusions, viruses, data loss, data alteration and the like.

The implementation of cyber security involves a number of strategies, including:

- Initially identifying all available connections to the SCADA system. These include local access to other enterprise networks, remote access via modems and wireless radios, and the Internet.
- The use of Intrusion Detection Systems (IDS) as a first line of defense. IDS act like a burglar alarm for the computer network by detecting unauthorized access attempts. There are basically two main types of IDS being used today: network-based (packet monitoring), and host-based, which typically inspects system logs for evidence of malicious or suspicious real-time application activity.
- Firewalls, which, when properly configured, provide protection against intrusion at a point of entry. A firewall monitors traffic across the network and examines every packet of data before allowing it to pass through.
- Remote Access Service (RAS), which allows legitimate users to access the SCADA system from off-site locations. RAS should be used in call back mode only. This means that when an administrator makes a dial-in attempt, in order to check for alarms or system status, the RAS hangs up and initiates a call back from a pre-configured list of phone numbers.
- Anti-virus protection software that should be deployed and regularly updated on the network to protect the system from computer virus threats as well as spy ware and keystroke loggers.

The aforementioned tools should be augmented by strong password practices. Modern PLCs/RTUs support multi-level password authorization to protect against program/application changes and can transfer data, using standard protocols such as DNP 3.0, to multiple locations, thereby allowing data-sharing and dissemination among a number of pre-selected users/operators in a secure environment. Since the user is only allowed to receive the data but cannot talk directly to the RTU, the security risk is low. This scenario is common in oil/gas custody transfer stations.

Authentication, a method by which the system ensures that the user is in fact a legitimate one, is supported by most industrial software applications that normally reside at the central location. Security-based authentication schemes enforce various account policies and provide seamlessly integrated security throughout the system.

Encryption of wireless communication traffic is another aspect of cyber security that should be considered. Wireless radio networks that utilize spread spectrum technology are inherently secure to attacks by outsiders. This is due to the ability of spread spectrum radios to transmit data while hopping among a number of unique frequencies in a pseudo-random sequence. This proprietary frequency-hopping technique cannot be intercepted by other commercial radios on the market. In addition to frequency hopping, most radio manufacturers use their own proprietary modulation technique that is not publicly made available. Without proper documentation, hackers need very sophisticated and expensive
equipment to be able to record and analyze the wireless transmissions. For additional security, some radio manufacturers encode a unique serial number or identification number into the radio firmware, allowing the user to determine with which other radios a given site will communicate. If a radio is stolen, the user can eliminate its serial number immediately from the master radio list, blocking it from accessing the communication traffic. Furthermore, third-party encryption/decryption modules that encrypt data before it gets to the radio network can be deployed for added security.

Increasing the security of critical services by utilizing existing infrastructure such as SCADA systems is an attractive proposition from the value perspective. As most utilities have already invested in building their SCADA systems, coupling them with strong physical and cyber security measures is a natural progression. Conducting routine self-assessments and scenario planning can help utilities identify security risks and develop counter measures before incidents occur.

Mr. Hany Fouda is the Industry Director, Water/Wastewater at Control Microsystems. He has over 15 years experience in Telemetry, SCADA Systems, radio communications and process control automation. Prior to joining Control Microsystems in 1995, Hany worked for Yokogawa Electric, a global supplier of instrumentation and control equipment. He can be reached at hfouda@controlmicrosystems.com.

For more information on how SCADA systems can help secure your operation, visit www.controlmicrosystems.com.

48 Steacie Drive, Kanata, ON, Canada K2K 2A9
Tel: 1 (613) 591-1943
Toll Free: 1 888 267-2232
Fax: 1 (613) 591-1022
sales@controlmicrosystems.com
www.controlmicrosystems.com