Emerson Process Management Capabilities for SCADA Security Systems

Many of our users in the energy production, transmission and utility industries as well as the water and wastewater industries are realizing the value of their SCADA systems when applied to security measures.

As shown in Figure 1, the SCADA system is usually distributed throughout the entire operation. A wide area network links vulnerable areas to operations.

Utilizing the SCADA system to its fullest is the best way to leverage existing infrastructure and available resources. With such capabilities and coverage at your service, the SCADA system should not merely be one aspect of your operation to consider in a security assessment. Many companies have decided to make it central to their entire security effort.

A major advantage of SCADA systems is that security measures are coordinated with operations. Many security systems and other recommended measures are not necessarily coordinated and require significant effort to do so.

Emerson Process Management has tested or is currently testing security systems and equipment, including video cameras, motion detectors, contact switches, and keyless entry devices, with our Network 3000 controllers and RTU's as well as OpenBSI and OpenEnterprise software.

Accessing live security information from such equipment, over the SCADA system, can reduce or eliminate the need for regular site visits or security patrols. Security breaches are reported to the operations staff in the same manner as process failures—via the SCADA alarm system.

Emerson has paid particular attention to the alarm system and put much of the intelligence in the RTU's. This provides extra security, as alarm processing continues even if there are problems with network communication or the SCADA master station.

Alarms are time-stamped as soon as they are detected by the RTU. Normally, this takes place within a second of the physical event and allows immediate control actions by the RTU as well as coordination with other live, time-based information such as video frames. Most other SCADA systems time-stamp alarms when the master station detects them. This could involve considerable delays.

Time-stamped alarm records are not only reported over the network as soon as possible but are also maintained locally in an audit trail. The audit trail provides redundancy in data storage and is extremely important to investigations, after-the-fact.

Emerson RTU's can automatically react to conditions and perform control actions, such as emergency shutdowns of processes, starting or stopping pumps, opening/closing valves, etc. Input for these actions can come from anywhere on the network.

Whether the SCADA system is allowed to take such actions is up to management. The SCADA system can automatically isolate a portion of your system by stopping compressors or pumps and closing valves or it can inform operators of the process conditions and let them decide.

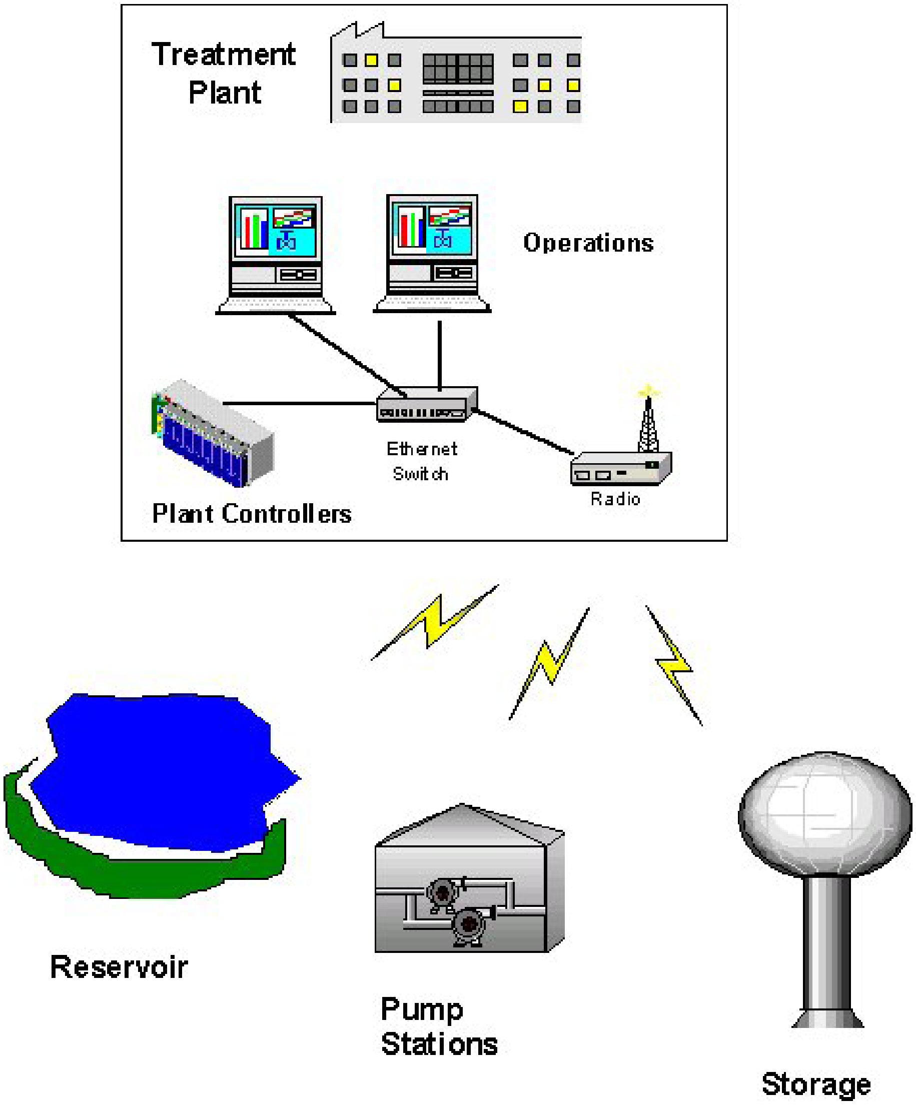

Figure 1: Plant

Implementing Security Measures

SCADA systems are particularly effective in addressing the following security areas:

- Access control to vulnerable areas, such as pump stations and chemical storage
- Threats to the process (e.g. contamination of a water supply)
- Cyber security and other threats to the SCADA system, itself

This application data will describe how Emerson's products and systems address these areas.

Vulnerable Areas

Water Industry – Pump Station

In the water industry, a pump station is an example of a vulnerable area in which an RTU is normally present. Functions of the RTU are generally limited to pump control, using input from flow or level sensors.

ACCOL programming allows pump operations to be fairly sophisticated. The RTU usually alternates pumps, runs them for maximum efficiency, schedules them at off-peak times as much as possible, and keeps records for run time maintenance purposes. Some systems work in conjunction with modeling software, in which case the RTU will start or stop pumps in anticipation of changes in demand.

The RTU can also report a number of alarms, which keep operators informed of the pump auto/manual status, changes in operation and failures. If the pump station is working in conjunction with a storage tank, the RTU can also report limit alarms and rate-of-change alarms for the water level.

The most basic security measures are in the form of contact switches (or “intrusion sensors”) for a gate, building door and the RTU enclosure door. These alarm devices are widely available and are wired to discrete inputs on the RTU. They simply allow the RTU to report an alarm if any is open.

If any contacts open when no water company personnel are known to be in the area, that’s cause for alarm. Until recently, this level of security was considered reasonable.

Figure 2 shows such an installation augmented with an access control and surveillance system that is resistant to concerted attempts to overcome security. Determined intruders can either avoid or fake out intrusion sensors. Wired contacts are relatively easy to defeat. A chain-link fence will simply delay an intruder by seven-to-eleven seconds. Entry through vents, windows or manholes circumvents locked doors.

One or more strategically placed motion detectors will indicate the presence of an intruder who has overcome entry devices. Provided all other accesses are secured, a keyless entry device will limit access through a locked door to authorized personnel.

Both devices are also widely available and interface to discrete inputs on the RTU. It is not unreasonable to expect an existing RTU to have at least two, spare discrete inputs. Reprogramming the additional alarms is also very easy in ACCOL.

Also available are more sophisticated keyless entry devices, which use serial interfaces. They provide additional information, such as the card code or key code. Emerson is currently testing the serial interface to two brands of access control devices.

Functionality is up to the user. In the simplest implementation, the RTU is not in the loop, which enables the door to open. Instead, it records the information in the audit trail and informs the operators of the entry. We are also able to load all valid card codes or key codes into a data array so the RTU can validate the entry. In this case, security maintenance is performed using the RTU.

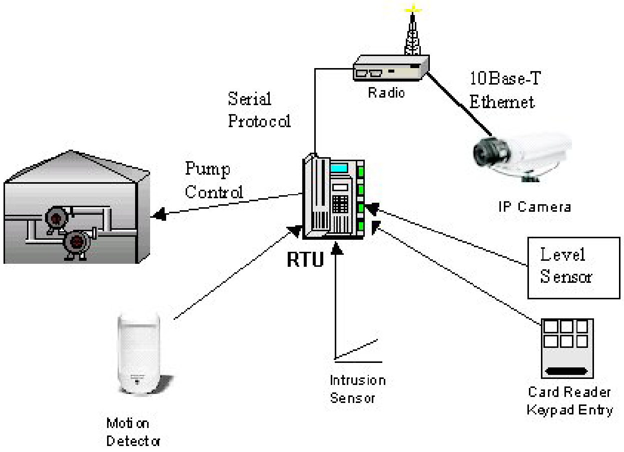

Figure 2: Pump Station

Most existing RTU's are far less likely to have spare serial ports than discrete inputs. However, Emerson products usually do have spare ports. With four serial ports, even the RTU 3305 is likely to have at least one unused at a pump station. (By the way, if you are out of discrete inputs, you can use a spare serial port to interface with a remote I/O module.)

A combination of access control and alarm devices, including intrusion sensors and motion detectors, is arguably very satisfactory for sites such as pump stations.

If additional surveillance information is required, a network video camera is the best solution. In response to an alarm or at any time upon request, an operator can view the site via live video. In the SCADA world, the old proverb can be restated, "a picture is worth a thousand discrete inputs."

Emerson has tested an IP video camera manufactured by AXIS Communications. IP cameras are Internet-Compatible and include web servers. If a public network is available at the site, the user can access the camera via the Internet. However, our implementation is via the Ethernet/IP SCADA network.

To accommodate bandwith limitations in the SCADA network, the resolution, compression and frame rate are configurable in the camera. On Ethernet, we have shown that live video can be viewed while all SCADA updates continue on the network. Using wireless Ethernet, we recommend that live updates are at reduced rates (e.g. once per five seconds) or operators only view video when an alarm occurs. OpenEnterprise can automatically show a video window if an alarm occurs in the associated RTU.

Even at the site, there are various ways to operate the camera vis a vis the RTU. Using the MDS iNET, the camera can interface to the network independent of the RTU. Alarms in the RTU can still trigger viewing the video on OpenEnterprise.

Some cameras, such as the AXIS model we have tested, also set an alarm from an internal motion detector. A buffer, internal to the camera, keeps a number of images during the timeframe just before and just after the alarm. The alarm can be reported via an e-mail message or via a contact output to the RTU.

Independent of the SCADA system, a PC can keep an image archive. This is similar to the operation of a VCR in a CCTV system. Like our audit trail, the image archive is very important to after-the-fact investigations.

There is a wide variety of implementations of an IP camera. Here's a run-down:

View images over the Internet: If an Internet connection is available at the site, the user can access the camera virtually anywhere in the world and view images on a PC. This is totally independent of the SCADA system. High-speed connections (e.g. DSL) allow live updates and full support of pan/tilt/zoom functions. Lower-speed connections will likely limit the update rate and provide less precise control of pan/tilt/zoom functions.

View images via 10mb or 100mb Ethernet: Also independent of the SCADA system, users can view live images and have full control of pan/tilt/zoom functions.

View images via 10mb or 100mb Ethernet SCADA network: If the SCADA system uses the Ethernet, users can view live video and control pan/tilt/zoom from an operator workstation. We have tested this capability with OpenBSI and OpenEnterprise. On an OpenEnterprise screen, the operator can view live video in a window along with other windows, which depict SCADA information, such as live graphic display, alarm list and trend graph. Busy networks may require tuning. In other words, you will likely need to use compression of frames but you should still be able to view live images.

View images via a Wireless Ethernet SCADA network: High speed, 802.11 networks: Unless there is major SCADA traffic, operators will still be able to view live images and control pan/tilt/zoom. This configuration is one in which users will most likely need to tune the network through configuration of updates and use compression. You may have to settle for periodic updates at rates typically better than once every five seconds and do without pan/tilt/zoom.

View images over a lower speed SCADA network: Networks operating at less than 115kb will not allow viewing of live images. Users attempting to do so will encounter significant delays (on the order of 5 to 20 seconds) and can very well miss an intruder or other problem at the site. In such networks, we recommend that operators allow the system to trigger viewing upon an alarm and, otherwise, occasionally view still images.

Water Industry - Chemical Storage

Storage facilities for chemicals, particularly chlorine, have been identified as vulnerable areas. These are typical of areas that lack SCADA coverage, not to mention, in many cases, security.

Nevertheless, such sites can economically be added to the system. As shown in Figure 3, an RTU is not necessary. Via Ethernet or a serial port, a remote I/O module can link process I/O and security devices to the SCADA system.

Threats to the Process

The water industry has considered the possibility that terrorists can find a location in a distribution system to inject a biological or chemical contaminant. Can the SCADA system provide a way to detect this activity?

Ideally, on-line analyzers would exist for all possible contaminants to the water supply. They would provide standard interfaces, which allow alarms to be immediately reported through the SCADA system.

Today, on-line analyzers are available for a broad array of contaminants. Many water systems currently use devices such as chromatographs to measure the presence of a variety of chemicals. Dedicated analyzers measure chlorine content and dissolved oxygen. Instrumentation is also available for variables such as color/turbidity, conductivity, pH, pressure and temperature.

This technology is well known and can be readily used in conjunction with any SCADA system. With their capabilities for alarming, audit trails, historical data storage and process control, Emerson's RTU products provide many strong possibilities in dealing with contamination.

However, many biological and chemical tests are still "off-line" and provide no interface. In addition, technology for many contaminants is emerging. We can only hope that new sensing technology will result in SCADA-compatible instrumentation (and we are willing to work with anyone performing R&D of such technology).

In the meantime, we feel that SCADA suppliers would be out-of-line if we stated that our products or systems provide a solution that addresses contamination by biological, chemical or nuclear materials. These are distinctly separate technological areas and users will need to rely on the professionals in the respective fields.

Another emerging area is use of SCADA systems in conjunction with process modeling software. Today, software from companies such as Haestad Methods can be used to simulate addition of contaminants to a system and see how they move through the system. This software has been used in after-the-fact investigations.

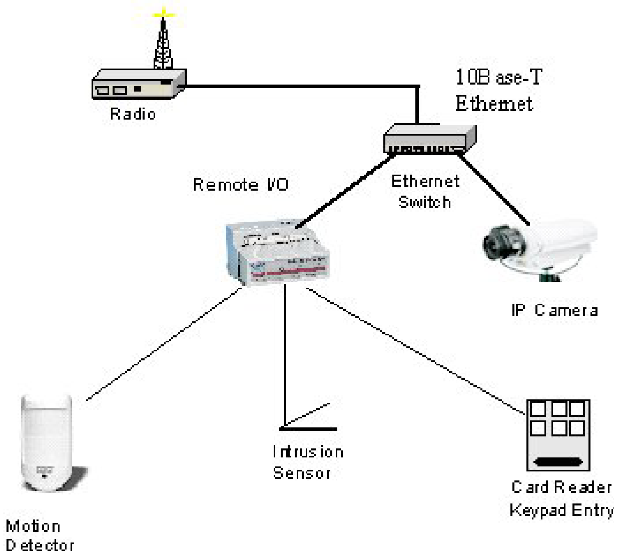

Figure 3: Chemical Storage

We are entering talks with Haestad Methods regarding use of their modeling software with our SCADA system. The SCADA system can provide actual information regarding operation of the distribution system. This information can be used to develop the model and, in turn, allow operations management to determine process control actions, which the SCADA system can take in response to various security breaches.

The model can also be used to run the water distribution system more efficiently. For example, the model might show that energy use is reduced if additional load is shifted from one storage tank to another.

In the oil and gas industries, our SCADA systems have been used in conjunction with modeling software. We feel this is an emerging area with many strong possibilities.

While the cyber security threat is addressed in the next section, process safety practices are worth mention, here. If anyone, whether a hacker or legitimate operator, performs actions such as starting or stopping pumps, the SCADA system will report the actions as alarms or events. It is important that all such operations are visible.

Other checks are easy to implement. Alarm limits can dynamically follow the process. For example, a ratio alarm could be set if the chlorinator feed rate were inappropriate to the water flow rate, even if it were within fixed high and low limits. If someone tampered with the chlorinator setting, this setup would catch it and report an alarm. Note that a chlorine analyzer further downstream should also back up this system.

Security of the SCADA System, Itself

If you are going to count on your SCADA system for security measures, the question is, how secure is the SCADA system, itself?

One utility manager mentioned that, in his company's security assessment, the Emerson SCADA system scored better than any other facet of the operation.

Many practices typical in the SCADA world are, in fact, perfect for security. SCADA systems very commonly employ measures such as back-up power systems, redundancy, password security, distributed workstations and remote paging.

Emerson's practices, including the alarm system, audit trail, historical data storage at the RTU, and assured delivery provisions of our communication protocol, provide the user advantages over other SCADA systems.

In SCADA systems, threats can be categorized in two main areas, infrastructure security and cyber security.

Infrastructure Practices

SCADA systems can be extremely effective in reporting threats to the operations infrastructure and can be resistant to damage to the SCADA system, itself. Following is a run-down of infrastructure-related practices, which should be employed in a SCADA system:

Back-up Power – If you're going to disable a site, the first thing to do is to cut the power source. However, an RTU equipped with a backup battery will continue running and immediately report a power failure alarm. Of course, the battery, as well as the RTU, should be in a locked enclosure with a contact alarm for the door. Otherwise, the RTU is as easy to defeat as the main power.

Communication Alarming – If you disable communication to a vulnerable area, the SCADA system should quickly detect the fact that it cannot communicate with that particular RTU. This puts the site "in the dark," a cause for immediate attention. The SCADA communication system should be checking sites as often as possible. An Emerson system will be able to distinguish failures of entire communication lines from failures in communicating with individual nodes.

Protocol Security – Of course, the communication link could simply be unreliable. But Emerson systems are able to distinguish a marginal line from a hard communication failure. BSAP has provisions for assured delivery, including handshaking, multiple attempts and error detection and can deal with marginal communication.

LAN Redundancy – Methods used to increase network reliability also enhance security. Redundancy is a common technique, especially for plant LAN's. Two, live networks are used. If one is damaged, communication continues on the other. To further increase reliability, each run in a redundant physical network can use different routing. However, the additional expense may not be worthwhile because LAN damage is reported as an alarm and can be quickly isolated.

Intelligent RTU's Operate Independently – If the network is cut off, the controllers and RTU's simply continue monitoring and controlling their processes. Once communication is re-established, Emerson RTU's are able to report alarms, events and historical information for the time that the network was out of service.

Wide Area Network Redundancy – Remote sites, such as pump stations, can also use redundant networks. For example, CDPD or dial-up can back up a leased line. Communication networks that use two different technologies can be difficult to defeat. An excellent combination is one that uses both hard-wire and wireless communication. This keeps the site "out of the dark" but you have to decide if it is worth the cost.

SCADA Master Station Redundancy via Off-site Workstations – These can be extremely valuable in the event that the control room is disabled. Workstations can be located not only elsewhere in the water system but also at operators' homes. Wherever the workstation is located, password security is employed.

Dial-up/Pager Systems – Even if off-site workstations are not used, Emerson SCADA systems offer provisions for off-site personnel to stay informed. Many facilities are unoccupied at least 16 hours a day. For such situations, you can use dial-up or remote paging in response to alarms. Some systems are being programmed to dial-up the local police in case of certain, high-priority alarms. In addition, some users are backing up the SCADA system with independent dial-up units for some sites.

Cyber Security

What can hackers accomplish by accessing the SCADA system? They can modify process operations (and, in fact, damage process equipment), cause major nuisance problems and cut-off service to your customers. They can also thoroughly corrupt the programs and stored information throughout.

Keep the Network Private – Hackers simply cannot access a private network from any off-site location. Keeping SCADA computers "disconnected" from the outside world, including the Internet, isolates the system from an awful lot of risks.

Employ Cyber Security Measures – The only problem, today, is that there are too many benefits in connecting to the outside world. Numerous information services are available via the Internet. Equipment suppliers can perform maintenance via the Internet. You can make operations information available anywhere in the world. If you want your system "connected," prudent use of firewalls and cyber security measures is mandatory.

In a paper presented at the Water Security Summit (12/4/01, Hartford, CT), FBI Special Agent Martin J. McBride recommended that users not only install firewalls and cyber security software, but make sure they go through the full configuration process. Hackers can readily defeat the default set-ups. He also recommends that users limit the number of PC's that do have outside access and make sure they are fully aware of all such PC's in the system.

Password Security – Password security is a minimum measure to be sure that access to workstations is limited to qualified operators. To ensure this is not the weakest link in security, management must establish passwords, other than the defaults, and periodically change them. Of course, access to the control room should be limited. Access control devices such as card readers should be employed at such locations.

Limit Capabilities of Off-site Workstations – It is important that off-site access be limited. Command sets can be proprietary and restricted. If system management capabilities such as programming and downloading are available, hackers can potentially do a lot of damage.

Don't Assume Proprietary Systems are Secure – Many users feel secure because of the proprietary nature of their systems. For instance, many users consider BSAP proprietary, even though it meets three ISO standards. "Cryptic" command sets, communication protocols and programming tools can be sufficiently discouraging. But we have seen the results of work by determined terrorists. Anyone willing to invest the time can figure out proprietary systems. Therefore, you need to follow the other measures suggested in this section.

Program Revision Control, Filing and Back-up – Finally, users should abide by good practice when it comes to maintenance of all software, including load images of the RTU programs and all historical data. Periodic back-ups should always be kept on a computer or medium that is physically isolated from the rest of the system. Back-ups are invaluable when the system is corrupted for whatever reason.

The contents of this publication are presented for informational purposes only. While every effort has been made to ensure informational accuracy, they are not to be construed as warranties or guarantees, express or implied, regarding the products or services described herein or their use or applicability. RAS reserves the right to modify or improve the designs or specifications of such products at any time without notice. All sales are governed by RAS' terms and conditions which are available upon request. RAS does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any RAS product remains solely with the purchaser and end-user.

Emerson Process Management
Remote Automation Solutions

Watertown, CT 06795 USA	T 1 (860) 945-2200
Mississauga, ON 06795 Canada	T 1 (905) 362-0880
Worcester WR3 8YB UK	T 44 (1) 905-856950

Website: www.EmersonProcess.com/Remote

EMERSON™
Process Management