# SCADA Security Update

## *Introduction*

This white paper is an update on best practices in securing SCADA systems. It addresses threats and corresponding implementation measures with a focus on SCADA RTU installations and the processes they monitor and control.

During presentations on this subject over a number of years, people have continued to ask whether there have been any attacks or intrusions into SCADA systems. A major supplier in the industry and a technical partner of Semaphore's, Industrial Defender, maintains a list of "critical infrastructure incidents." The latest is available on their website, www.industrialdefender.com.

An attack, which occurred a few years ago, reigns as the most famous. It took place in Australia in 2001. Key to this attack is the fact that it was targeted to the remote sites; hence, our focus on this particular aspect of a SCADA system.

As reported by news.com.au and other sources, Vitek Boden, a disgruntled former employee of the contractor who installed a computer system for the Maroochy Shire Council, near Brisbane, later hacked into the system. According to a court statement, "He applied for a job with the council but was rejected and later hacked into the council's sewage control computers, using radio transmissions to alter pump station operations.

"Up to one million litres of raw sewage flowed into the grounds of the Hyatt Regency Resort at Coolum and nearby Pacific Paradise, where it ended up in a storm water drain." The court statement went on to describe a great deal of environmental damage those attacks caused.

Could this sort of attack happen to your system?

## *Overview*

Significant recent developments in SCADA security include the release of two, key standards, ANSI/ISA-99 Part I and NERC CIP.

Entitled, "Terminology, Concepts and Models" Part I of ANSI/ISA-99-00-01-2007 "Security for Industrial Automation and Control Systems" lays a solid groundwork for upcoming standards on establishing and operating a security program and technical security requirements. Approved on October 29, 2007, it introduces significant, "common ground" in definitions of security-related concepts, assets, risks, threats, and vulnerabilities.

The NERC (North American Electric Reliability Council) CIP (Critical Infrastructure Protection) cyber security standards CIP-002-1 through CIP-009-1 (formerly known as the 1300 standards) have been approved as of January 17, 2008. CIP-002-1 through CIP-009-1 includes numerous provisions that require compliance.

Among numerous concepts in ANSI/ISA-99 Part I, one of the most important is the Reference Architecture, which includes a security zone model. The model recognizes the reality that various portions of a control system or SCADA system, whether logical or physical, vary in terms of risks, vulnerabilities, and, therefore, security requirements. It is noted that there is a distinct advantage in aligning security zones with physical areas or zones — for example, aligning a control center with a control security zone.

ANSI/ISA-99 Part I defines zone characteristics — each zone has a set of characteristics and security requirements that are its attributes. They take the form of:

a) Security Policies
b) Asset Inventory
c) Access Requirements and Controls
d) Threats and Vulnerabilities
e) Consequences of a Security Breach
f) Authorized Technology
g) Change Management Process.

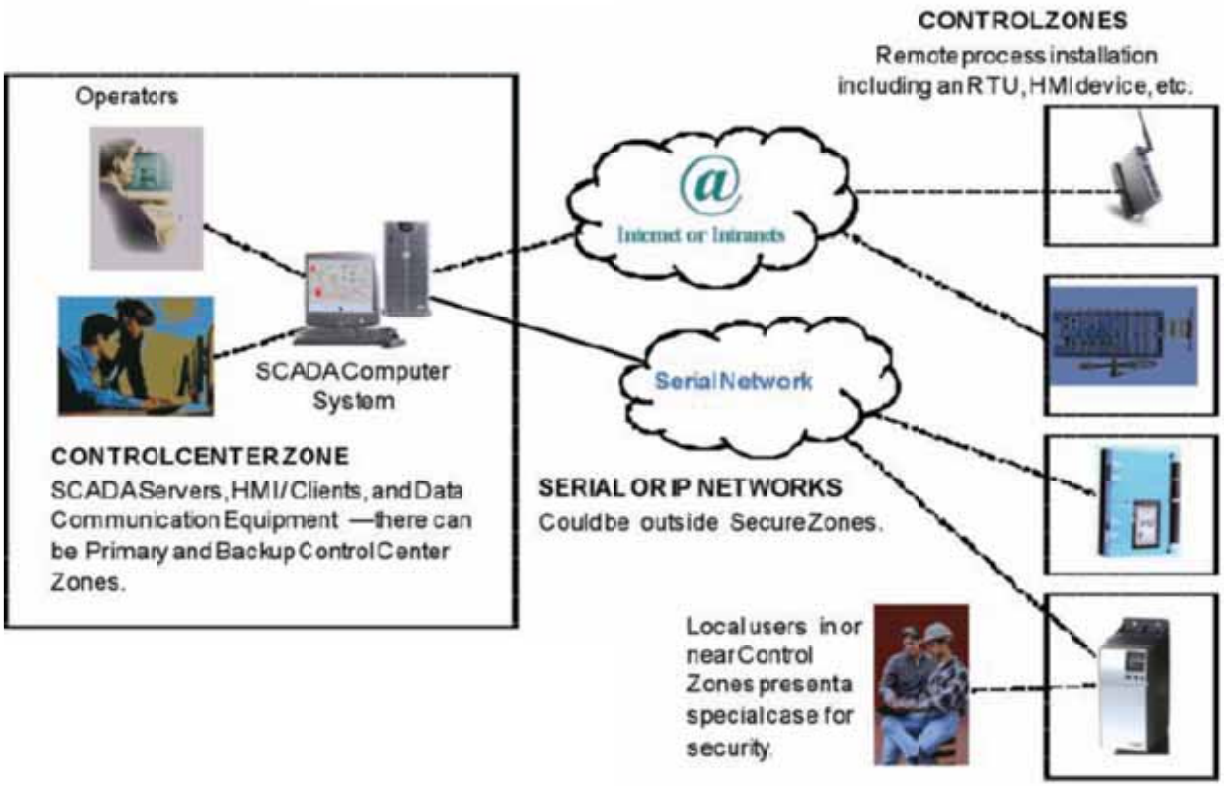
For a SCADA system, ANSI/ISA-99, Part I defines various, logical zones to include the "Enterprise Zone," which is generally considered the IT system, and the "SCADA Zone," which includes the subsystems we normally associate with a SCADA system:

- Control Center Zone or Primary and Backup Control Center Zones
- Serial or IP Network
- Control Zones, which are the remote sites normally associated with RTU installations

ANSI/ISA-99, Part 1 includes two versions, one of which encloses the entire SCADA system in a single security zone. The other is the "separate zones" model.

In the separate zones model, control center zones and control zones are defined with differing characteristics. The control zones are the locations, which are usually remote from the control centers and include the RTU equipment. It is conceivable that one control zone can have much different characteristics from another. For example, one location could be classified as more vulnerable or have higher risks than another.

NERC CIP-005-1 requires an electronic security perimeter for what are termed, "critical cyber assets." While it is not explicitly stated in CIP-005-1, the electronic security perimeter concept does apply to ANSI/ISA security zones and there is general consistency, between the two standards, in definitions of assets and other terms. CIP-006-1 provides physical security requirements and, again, is not inconsistent with ANSI/ISA-99 Part I. This white paper will describe measures in terms of applicability to ANSI/ISA-99 as well as NERC CIP as much as possible.




The white paper will focus on the control zones and their interfaces to the wide area network. Remote sites provide numerous characteristics, which differ significantly from those associated with the Enterprise Zone or Control Center Zones. Since the latter two have been explored much more thoroughly, there is more to offer if we focus on control zones. In addition, the wide area network in SCADA systems presents a very interesting set of characteristics, as it is typically outside of any of the operator's security zones.

## *Securing the RTU Devices at Remote Sites*

In SCADA systems, the control zones are normally in remote areas, away from control center zones. This presents a number of unique characteristics, which are notably different from control centers as well as plant processes. We will consider both the cyber and physical threats and offer measures in terms of monitoring for intrusions as well as prevention.

The term, "RTU," will be used for the electronic monitoring and control device at these locations. Please keep in mind that the device could actually be a PAC, PLC, or a product that uses some other, three-letter abbreviation.

## *Addressing RTU Cyber Threats — Prevention*

In many systems, it is simply too easy to gain access via an RTU local serial port or, even worse, a dial-up, radio or other network link that makes the RTU accessible from practically anywhere in the world.

How important is this aspect compared to the rest of the SCADA system? In the attack in Australia, Vitek Boden targeted the remote stations by using a radio to access serial ports and was able to operate pumps.

RTU ports can basically fall into one of two groups: local and remote. Local ports are wired directly to nearby equipment such as analyzers, flow meters, pressure transmitters and a PC or other HMI device. Wireless interfaces are becoming more popular for local links, e.g. wireless HART between an RTU and pressure transmitter and Bluetooth between a lap-top PC and the RTU.

If the RTU is not in a physically secure zone, a major risk is that anyone can plug into — or wirelessly access — the local port that is intended for configuration, taking readings and other, local operations via a PC.

Unfortunately, it is too easy to say that it is mandatory for the RTU to be physically secure and be done with it. Today's trend toward wireless communications, even for "local" functions, reintroduces the risk of intrusion because the radio range can extend beyond the physically secure zone. A wireless local link, thus, shares a major risk with a remote port, which is defined as one with a modem, radio or other physical connection to a wide area network.

Since much of a SCADA wide area network is located, both physically and logically, outside of any of the operator's secure zones, this is a major cause for concern.

Authentication has emerged as the cyber security provision-of-choice when it comes to remote port access.

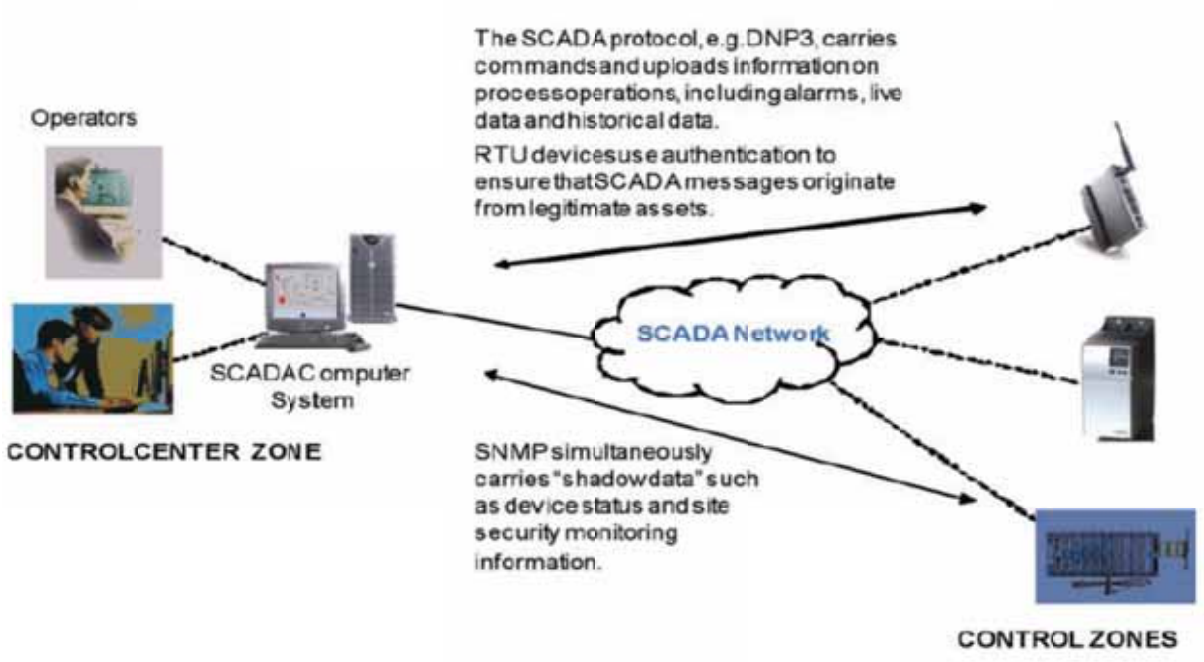
In some cases, protocol standards are being amended to adopt authentication. The DNP Users Group Steering Committee has recently ratified a security extension that mandates the authentication of master devices through the use of one-way cryptographic hash functions employing a shared key in order to access critical DNP functions. These critical functions include write, select, operate, direct operate, cold restart, warm restart, initialize application, start application, stop application, enable unsolicited responses, disable unsolicited responses, record current time and activate configuration.

Authentication ensures that messages arriving at the RTU come from the control center, or other, legitimate asset in the SCADA system. Since the SCADA wide area network can be located mostly outside of any security zones, it is subject to eaves dropping.

A number of years ago, Bill Rush of the Gas Technology Institute (GTI) proposed SCADA message encryption to address this risk. As Bill pointed-out, if someone can eavesdrop and learn to recognize messages, the party can likely also practice "spoofing," that is, inject commands, which can operate process equipment or corrupt proprietary information.

This is the thrust behind the SCADA encryption standardization effort, which was originally proposed as American Gas Association (AGA) Report No. 12. Since then, the technical standards community has favored authentication over encryption primarily because it is much less resource-intensive and can more reasonably be retrofitted in existing systems.

In any event, encryption standardization efforts continue and encryption is finding its way into new installations. Some data communication devices, such as radios, offer it as an option. Many IP-based systems use encryption and, for those users replacing direct-wire local links with wireless, it is also a feature of Bluetooth.




### *Addressing RTU Cyber Threats — Monitoring and Detection*

At a minimum, the RTU must be able to log all activity on local or modem ports and report it to operators on the SCADA network. NERC CIP-005-1 requires24/7 logging at all access points to the electronic security perimeter.

The Simple Network Management Protocol (SNMP) is emerging as a vehicle for security monitoring in SCADA networks. Traditionally used by IT to monitor components such as routers, servers and switches, SNMP is now being employed to monitor remote sites. For example, such control zone parameters as main power status, battery voltage, cabinet temperature, and door switch status can be reported via SNMP.

Similarly, SNMP can report activity on RTU serial ports. That information can be used for intrusion detection. SNMP operates over TCP/IP links and can function concurrently with other SCADA protocols. While DNP3 or IEC60870-5 protocols are used to transfer process or operational information between the SCADA server and the RTU's, SNMP is used, over the same physical network, in a background mode, transferring "shadow data" that is used for system health monitoring and security.

In this architecture, a Semaphore RTU is "Industrial Defender Enabled." The Industrial Defender Risk Mitigation platform is a central monitoring system for the health, status and security state of critical cyber assets. By using Industrial Defender to maintain an ongoing inventory of cyber assets, automatic reporting is provided for CIP-005-1 compliance. The monitoring and reporting feature within Industrial Defender greatly reduces any manual reporting burden on the entity's IT staff.

### *Addressing RTU Physical Threats — Prevention*

Following are measures to physically secure the RTU installations in your SCADA system:

The best practice for RTU location is to place it in a physically secure area. Risk is significantly decreased if the RTU is installed in a location with access control.

Keep information about RTU locations secured. Risk is also significantly decreased if as few people as possible know the location of the RTU in the first place.

Similarly, power and network cabling should be kept secure and out of sight. Information on their routing and termination locations should be secured.

In case of a main power failure, the RTU should include adequate battery backup to continue all operations for a time you determine. This time depends on how long you feel it could take to restore main power. Note that this does not mean how long it could take for operators to find out about the problem. The alarm system must inform operators of a main power failure immediately — we will cover that more in the next section on monitoring and detection. Typical RTU backup times are between eight and 72 hours — the latter taking three-day, holiday weekends into consideration.

The backup batteries should be secured inside a locked cabinet with ventilation. For outdoor locations, the most appropriate rating is Nema 3R or IP14. You must periodically maintain the batteries on a schedule provided by the battery supplier. You can expect a maximum of a five-year lifetime from lead acid cell batteries but you should check them at least once per year. In areas in which temperatures are often at the extremes of the operating range, battery lifetime is significantly reduced. The RTU should continually monitor the batteries and set an alarm if they lose their charge. If their condition is in doubt, replace the batteries.

Include line filters and surge suppression on the power input. Accidentally or otherwise, and battery-backed or otherwise, power problems should not take the RTU out.

Always keep RTU cabinet doors closed and secured. Once the door is opened, it is just too easy to cause any number of problems.

If the RTU is not in a physically secure area, then you must keep keypads, pushbuttons, and switches secured. Users should have to open up a door, that is secured by access control — which could be as simple as a key lock — in order to access these devices.

Of course, this is all easy to say but what do you do about an existing installation? In most cases, it has been feasible to secure the room or building in which the RTU is located. In cases this has been impossible, it was better to secure the RTU inside a locked cabinet or put a gate around it. Ideally, both the room and the RTU enclosure are secured. However, you may have to settle for one or the other.

Finally, be on the alert for innovative methods of disabling the RTU. In other industries, computer equipment has been disabled through the use of fire extinguishers, other chemical spray, excessive dust or sand, flooding, sprinkler systems, radio interference and surges on wiring. Vulnerability assessments must include such scenarios, even though they would likely be far down the list in terms of risk. Best practices in terms of locating and physically securing the RTU should prevent these problems.

### *Addressing RTU Physical Threats — Monitoring and Detection*

The RTU should detect entry into the physical secure zone via an access control device, that is, when a door or gate is opened, and alert operators via an alarm.

The RTU should continually monitor main power and report an alarm on main power failure.

The RTU must be able to report that a user has plugged a hand held device or PC into the local port — or gained access via Bluetooth or other, local wireless link. This could be an alarm but some users simply log it as an event.

Log an event when the user signs on by entering a password. Log an event for each value change the user makes. Operators must be aware that value changes are being made, locally. Log an event when the user signs off and either log an event or clear/reset the alarm when the user unplugs the hand held device or PC. If the user forgets to sign off, the RTU should automatically do this after a set time.

Alarm clear/reset when the door closes. What if the user forgets to close the door? The original alarm, set upon opening of the door, should continue to be displayed as a live alarm. As a further provision, you can consider escalating that alarm after a certain time.

Coordinate the alarms, mentioned thus far, with operating procedures. These procedures should include schedules for site visits and ways to keep operators informed regarding them. Don't disable alarms just because operators know that a site visit is taking place. Keeping alarming active reinforces procedures and allows the alarms to be kept in a history.

The RTU should not only report alarms, over the SCADA network on a priority basis, it should also keep a date and-time-stamped record of all alarms and events locally in memory. The memory must be non-volatile. RAM must be backed up by a battery and Flash, which does not require battery backup, is now being used more often.

Many of today's RTU products incorporate data logging capability, including maintenance of an alarm/event log. In the gas flow computer business, this is known as the "audit trail."

One problem with an alarm/event log is a "noisy" alarm condition whose recurring messages fill it up. Not only is this very annoying but, worse, meaningful messages drop out and are permanently lost. In most cases, it is simple to automatically filter out these transitions or disable the alarming characteristic of the misbehaving input.

The alarm/event log is an excellent backup in case of problems with the SCADA host or network, which could cause alarm reports and event logs to be lost. Typically, it allows the user to access all such information, locally. In addition, many RTUs will allow the audit trail, as well as historical averages and totals, to be transmitted to the SCADA host once communication is restored.

You have seen that many of the security tactics in this section involve use of the RTU for alarm reporting. Please be aware that a common problem with SCADA alarm systems is that engineers are tempted to define too many points as alarms. These quickly become "nuisance" alarms, which are ignored. You should avoid this situation because the alarm system should never lose credibility with operators for any reason.

Far worse than that is it creates a situation in which an operator can be easily overloaded and overlook an important development. It is even possible that a security violation can occur because operators are decoyed by a deliberate overload.

Your alarm system design should define alarms points as sparingly as possible and it should use alarm management as a further measure to reduce the quantity of alarms generated from any process or zone.

Finally, for remote site security, using the RTU to report alarms for fire, smoke, water spray or water flooding is also very feasible. The RTU can also be put in the security loop through interfaces with access control devices and video cameras. This will be the subject matter of another white paper from Semaphore.

### *Design Practices in Case of Failures*

Best practice system design calls for provisions in case of various failures (or breaches) of the SCADA system.

In case the host computer or network fails, the RTU should independently monitor and control the process. Remote processes, today, should not depend on the availability or performance of the network.

The RTU should continue operating even in case the network is jammed or one or more ports are kept busy. While this would amount to a denial-of-service attack on the RTU, we have seen many cases in which the SCADA network was simply overloaded. The multitasking kernals in today's RTUs prioritize tasks and allow the measurement and control functions to continue even with heavy activity on the network.

You should also consider a redundant network. Competition in the communications industry has resulted in decreasing pricing for hardware that includes cellular radio, licensed radio, spread spectrum radio and wireless Ethernet. I know some users will scoff at this because they've found that selecting even one network is difficult enough!

But, increasingly, users are installing redundant SCADA networks. Most SCADA software will automatically switch over to a standby network if the primary network fails. At the RTU, the standby network uses a separate communication port that is not affected by problems on the primary network port.

To detect tampering with process equipment, you can use sanity limits or sanity condition tables to validate commands or process conditions. Even though no RTU includes expert system software, you can still put your expertise in the RTU program, whatever the programming language. If you know that all three influent pumps shouldn't be on when the settling basin is at 12 feet, put that in the RTU. The RTU should know that the chlorinator shouldn't be set on maximum when the flow is only 0.4 MGD.

Your first reaction might be that this would add too much complexity to the RTU but some languages make the programming almost as easy as making the statement. If access control is violated and someone manually changes a process equipment setting, the RTU could detect it and report an alarm.

Finally, best practices for system design call for provisions in case of RTU failure, regardless of security issues. Upon failure, what happens to the control outputs, with or without power, is a basic design issue. If power remains available, many devices allow selection of a "safe mode" for the outputs. Process equipment continues to run in a reasonable manner. You also need a separate provision to cover the case in which the RTU fails and all power is lost. Equipment run using backup power must have a "safe" default setting.

Many users have rock solid procedures for activity at the sites in response to any failure or security breach in the SCADA system. You need to be in this category.

## *Conclusion*

Today, information that is widely available and products and technologies, which are now on the market, allow SCADA system operators to install and maintain very secure systems.

Utilities need to be well aware of NERC CIP, which requires compliance in your planning, processes and procedures. Meanwhile, ANSI/ISA-99 is a work-in-process. Part I, which is now available, establishes important, "common ground" in definitions of security-related concepts, assets, risks, threats, and vulnerabilities.

Users, today, can assess threats, both physical and cyber-related, and implement measures for detection as well as prevention of intrusions and attacks in their SCADA systems.

## *SCADA Security Checklist*

**Prevention**

1. Use authentication (e.g. Secure DNP3) on all remotely-accessible serial ports.
2. Use encryption if available, e.g. on Bluetooth and IP connections.
3. Note that password security is a minimum measure, which does not eliminate cyber risks.
4. Locate the RTU in a physically secure area with access control.
5. If the RTU is not in a physically secure area, then you must keep keypads, pushbuttons, and switches physically secured, e.g. behind a locked door.
6. Always keep RTU cabinet doors closed and locked.
7. Keep information about RTU locations secured.
8. Power and network cabling must be secure and out of sight.
9. Keep information on cable routing and termination locations secured.
10. Use battery backup in case of main power failure and consider backup times up to 72 hours.
11. Backup batteries must be physically secured.
12. Keep up with battery maintenance.
13. Include line filters and surge suppression on the power input.
14. Vulnerability assessments must consider risks from chemical spray, wind-blown dust or sand, flooding, sprinkler systems, radio interference and surges on wiring.

**Monitoring and Detection**

1. Log all activity on all serial ports, local and remotely-accessible, e.g. SNMP reporting of "shadow data" to the Industrial Defender Risk Mitigation platform.
2. The RTU should detect entry into the physical secure zone via an access control device and alert operators via an alarm.
3. The RTU should continually monitor main power and report an alarm upon failure.
4. The RTU must be able to report an alarm or event when a user has plugged a hand held device or PC into the local port — or gained access via Bluetooth or other, local wireless link.
5. Log an event when the user signs on by entering a password.
6. Log an event for each value change the user makes.
7. Log an event when the user signs off.
8. Either log an event or clear/reset the alarm when the user unplugs the hand held device or PC or disconnects a wireless link e.g. Bluetooth.
9. Clear/reset the "door open" alarm when the door closes.
10. Coordinate all alarms and events, mentioned above, with operating procedures.
11. Don't disable alarming when users are visiting a site.
12. The RTU should maintain a local, date and time-stamped, alarm/event log in non-volatile memory as a backup of the alarm reporting mechanism over the SCADA network.
13. "Noisy" alarm or event conditions must automatically be filtered out or disabled and, of course, the root cause must be addressed ASAP.
14. The alarm system design should define alarms points as sparingly as possible and it should use alarm management as a further measure to reduce the quantity of alarms generated from any process or zone.

15. For remote site security, go ahead and use the RTU to report alarms for fire, flooding, intrusion, and smoke as well as to transfer video images.

**Design Practices in Case of System Failures**

1. The RTU should independently monitor and control the process, ie. it should not be dependent on the host computer or SCADA network.
2. The RTU should continue operating even in case the network is jammed or one or more ports are kept busy.
3. Users should consider a redundant network.
4. Use sanity limits or sanity condition tables to validate commands or process conditions in order to detect tampering with, or malfunctioning of process equipment.
5. Finally, best practices for system design call for provisions in case of RTU failure.