Vigilinx
Digital Security Solutions

Protecting SCADA and the Vital Energy Infrastructure

A White Paper from Vigilinx

Executive Summary

A year has passed since the events of September 11. In that year, determined to bolster the private-public partnership that protects our critical infrastructure, our legislators and government agencies have been busier than ever establishing the methods and means for that protection. Although talk of the physical threat dominates, the genuine threat of cyber-attack vies for our attention, even reaching the mainstream media.

Accordingly, agencies charged with the oversight of energy and other utility services have retrenched, first becoming more proactive in their *advisory* and information sharing roles and now moving towards cyber-*regulations* with compliance deadlines.

SCADA[1] systems provide much of this service infrastructure. Our energy infrastructure and our water works depend on it, and other services such as telecommunications depend on monitoring and control not functionally dissimilar from those provided by SCADA.

Once it presents the basic threat scenarios against SCADA, this white paper recommends an assessment approach that is holistic, attentive to these threats, and mindful of the shifting agency roles. It explains and emphasizes the need to look beyond the technical controls immediately applied to the SCADA environment, illustrating the potential outside dependencies on technical controls in the greater corporate environment and at outside third parties. In a similar way, it recognizes and details the part that others beyond the immediate custodians of the SCADA infrastructure may play in implementing the necessary *operational* and *administrative* controls that complement the technical controls. It elaborates on a prospective framework for information security that logically breaks down responsibilities between corporate information security and the business unit SCADA custodians.

With such an assessment the organization will have the breadth and depth of perspective that enables it to prioritize, act, comply, and protect. Done by Vigilinx the assessment becomes a foundation for an ongoing relationship – with Vigilinx leveraging its Professional, Knowledge, and Managed Service offerings and taking a leading role in devising, building, and sustaining the company's framework for continuous information security improvement. As also discussed in this white paper, Vigilinx can help construct an action plan for an information security program to put the organization on a trajectory for effective SCADA asset protection and regulatory compliance.

[1] Supervisory Control And Data Acquisition

Background

President Clinton's 1996 Executive Order 13010 set a number of activities in motion intended to solidify the protections we place on our critical national infrastructure services. The events of September 11, 2001 have injected a tremendous sense of urgency into what the (ever-so-promptly-passed) USA Patriot Act calls the "public-private partnership."

Executive Order 13010 designates eight critical infrastructure services considered vital to the defense and economic security of the United States. These services are Telecommunications, Banking and Finance, Water Supply Systems, Transportation, Emergency Services, Government Operations, Electrical Power, and Gas and Oil Storage and Delivery.

In 1997, concerns about lax cyber security were reinforced during a test conducted by the Department of Defense (DoD) named "Eligible Receiver." The test tasked a group of government employees, using only commercial and open source products, to "find out if they could disrupt the infrastructure of the United States" within three months. The test demonstrated that not only could the group disrupt and take down critical infrastructure services within 90 days, but also that taking such action required only "modest" knowledge and skills.

In 1998, the Department of Justice (DoJ) and the Federal Bureau of Investigation (FBI) established the National Infrastructure Protection Center (NIPC) to coordinate private sector and U.S. government national critical infrastructure threat assessments, warnings, vulnerabilities, law enforcement investigations, and responses.

Later in 1998, Presidential Decision Directive (PDD) 63 called for a further partnering between the Public and Private sectors, designating for each of the sectors a "Lead Agency" with a "Senior Liaison Official" to work with the service providers in that private sector. The water supply sector's lead agency is the Environmental Protection Agency (EPA). The Energy sector's lead agency is the Department of Energy, which has in turn designated the North American Electric Reliability Council (NERC) and the National Petroleum Council (NPC)[2] as coordinators for electric power and oil and gas storage and pipelines, respectively.

Each lead agency has taken steps to fulfill the goals set forth by PDD 63, issuing security guidelines, establishing Information Sharing and Analysis Centers (ISAC) for incident reporting and threat notification, and providing self-assessment materials. Although much of the new information security materials provided by these agencies are advisory in nature, as the concern over terrorism grows, so does the specter of increased cyber-regulations. For example, in mid-July 2002, the Federal Energy Regulatory Commission (FERC) issued a draft proposal for information security standards for the wholesale electric grid operations with the expectation of compliance by January 2004. Similarly, the Nuclear Regulatory Commission (NRC) has issued orders on cyber-security that expand upon the definitions of critical assets and sensitive data that must be protected against cyber attack.

The nature of the public-private partnership is changing. It seems inevitable that the guidelines the agencies are putting forth will evolve into enforced, regulated standards. Yet, whether or not the decision to act comes from within the private sector, the impetus for action is clear. The level of exposure is high, and our adversaries are highly motivated.

[2] The NPC designation as coordinator is expected to change.

Introduction

The efficient management of much of our country's critical utility infrastructure depends on near real-time monitoring and control. For the Water Supply Systems, Electric Power, and Gas and Oil Delivery, the complementary infrastructure that provides that monitoring and control is typically called SCADA (Supervisory Control And Data Acquisition). SCADA encompasses the network and distributed systems that enable the communications and processing of data from numerous remote control points. In addition to monitoring the infrastructure and providing manual and automatic controls, SCADA provides data for longer-term analysis (e.g., failures, loading), accounting, energy marketing, and energy trading.

What has made these SCADA systems, and the underlying infrastructure they support, more vulnerable in recent years is their increased connectivity to the rest of the world. For example, as electricity is moved from one provider to another provider's domain, each with its own SCADA system, there is a need to share information about the current and planned loads. In addition to the basic operational need, there is the requirement that scheduling and loading information be shared equitably to multiple parties for energy trading applications. There is similarly a need to provide this and other information to intracorporate enterprise servers for different administrative back-office, customer-service, and engineering functions. Those systems, in turn, are exposed to the Internet.

Through this connectivity, a malicious insider or outside hacker could potentially misuse or undermine the SCADA controls. This paper elaborates on the threat and details a holistic approach to assessing the security of the SCADA system – and the rest of the infrastructure -- against this threat. Implied by this holistic assessment approach is the subsequent, and also holistic, approach to the remediation of any of the assessment's findings. We recommend some common initial action steps.

Although this paper focuses primarily on the infrastructure for the generation, transmission, and distribution of electricity, the principles covered apply well to infrastructure for water systems, gas storage and delivery, and telecommunications. They also apply to localized controls such as those for a Distributed Control System (DCS) for a power plant.

The Threat: "Where There Is Control..."

Where there is control, there is the opportunity for abuse of that control. There is the potential for unauthorized access and the potential for unauthorized changes by authorized insiders.

These risks can be assessed largely in light of three possible threat scenarios.

1. That, by improperly using the SCADA infrastructure, an individual shuts down or sabotages the underlying infrastructure being monitored and controlled (e.g., the transmission grid).

2. That, by sabotaging key components in the SCADA infrastructure (e.g., networking components or key servers), an individual inhibits the ability of operations to properly monitor or control the underlying infrastructure.

3. That, by either not having the necessary recovery mechanisms or by an individual knowingly disrupting them, the operations organization finds itself unable to recover the infrastructure in a timely manner -- or in the worst case scenario, the operations organization finds itself unable to recover the infrastructure at all.

The first scenario is serious enough, but when combined with the second, and potentially the third, cumulatively it becomes a genuine crisis. It is exactly this potential exposure that the custodian of vital infrastructure must avoid.

To the general public, the implications of these kinds of scenarios might be the economic disruption of a blackout or an interruption in telephone and Internet services, or death or injuries from an explosion.

A Holistic Approach to a SCADA Security Assessment

When assessing the level of exposure to this threat, one is well advised to take a broad-minded approach. The connectivity to the SCADA systems cited above naturally suggests the need for carefully considered technical controls (e.g., firewalls, server hardening, intrusion detection). Yet with the multiple parties that can be involved and with the complexity of developing, implementing, and maintaining those controls, it is equally important that there be administrative and process controls that complement those technical controls. Technology solutions alone do not suffice.

Also, these controls should be examined for the immediate SCADA operations group *as well as* for internal Corporate IT group and any outside third-party groups that may play a role in safeguarding the SCADA systems.

The SCADA data and process owners, who have the direct custodial responsibility for the SCADA environment, have to go beyond ensuring that SCADA operations are properly safeguarding those assets. Where there are dependencies on the corporate IT group and outside third parties (e.g., partners and outsourcers), they must also partner with corporate information security and try to ensure that these other parties are implementing proper safeguards. The mechanisms to extend those controls to the corporate IT group and third parties include Service Level Agreements (SLA's) and contracts that have specific clauses that detail security requirements and ensure legal recourse. To be effective, the SLA's and contracts must be monitored and managed for compliance.

Although the most prudent information security tact is to minimize dependencies on outside groups, given the interconnections that already exist, segregation and isolation are feasible only to a point. In fact, economic factors may be pushing the company towards outsourcing or corporate "shared services" to fulfill particular needs. Even if the outside dependencies can be reduced, the residual risks must still be managed.

Administrative and Process Controls

SCADA itself provides a decent analogy for information security administrative and operational controls. SCADA keeps the infrastructure in balance, and these information security controls also maintain a balance – between acceptable risk and cost-effective controls.

In their typical implementation, these information security controls are similar to the SCADA controls for power generation. For a number of reasons, as shown in Figure 1, power plants maintain either all or the majority of control for their generation local to the plant. In many instances, however, the generated output can be fine-tuned from a remote centralized location to track and optimize the balance between what is generated and what needs to be delivered through transmission.

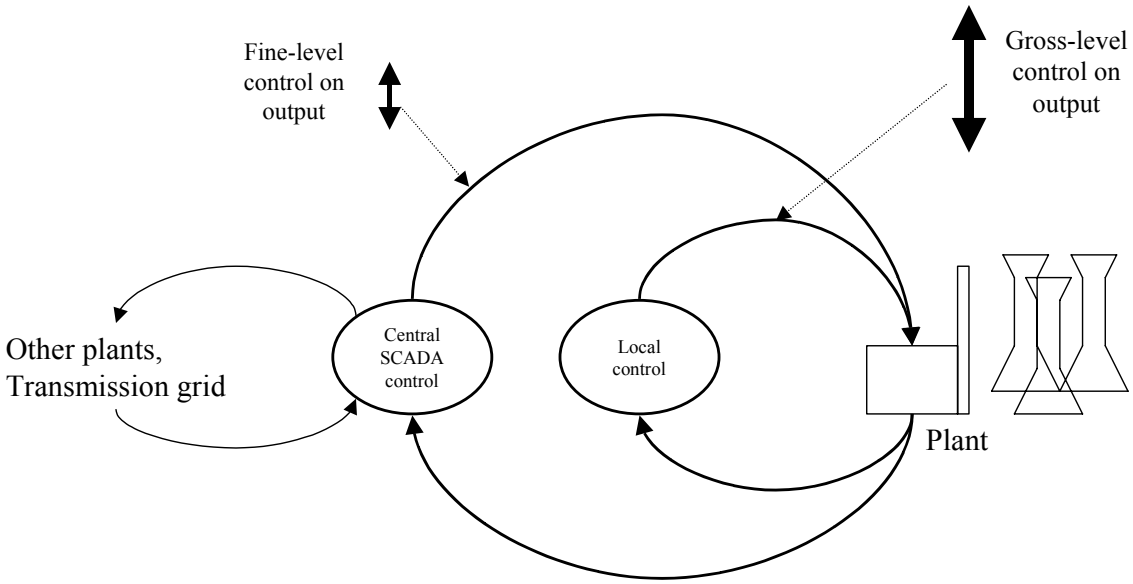

Figure 1: Controls on Power Plant Output

One might liken this joint SCADA control to the common organizational models for information security. Companies entrusted with a significant portion of our national infrastructure are generally diversified with multiple lines of business, certainly large enough to have an independent centralized information security organization. At the same time, the majority of the operational controls depend on the direct custodians of the SCADA environment, engineering and operations teams from within the given line of business.

Just as the central SCADA controls must for power generation and transmission, the corporate information security group must coordinate the activities in multiple locations (or lines of business). The corporate information security group accomplishes this by setting a larger framework and providing a set of services that the individual lines of business can leverage.

An assessment of a corporate information security organization would look for characteristics that would effectively aid the SCADA custodians, characteristics commonly noted in standards such as ISO 17799:

- *Risk management*: The corporate group has a clear methodology that puts the corporate group's own assessments in a consistent context, and may provide the line of business with tools for self-assessment[3].
- *Information classifications*: The corporate group has devised classifications that are clearly defined and cover the sensitivity of confidential data and the criticality of data for its availability and integrity.
- *Policies*: The corporate group has developed policies that are thorough, relevant, well articulated, and visibly supported by senior management.
- *Technical standards*: The corporate group has standards that make the policies "actionable" for employees, contractors, outsourcers, system administrators, etc., that cover technologies relevant to the business units, and that can be adapted to the specific needs of the business unit.
- *Incident response*: The corporate group has established methods, procedures, tools, and templates that the line of business can adapt to their specific needs.

[3] Many of these lines of business have mature risk assessment models, but they may need assistance in applying them to information security risk.

- *Security monitoring*: The central group may install intrusion detection and other log analysis or alerting tools and monitor and maintain them on behalf of the line of business.
- *Computer forensics*: Given the specialized expertise to properly conduct forensic investigations, the central group may provide these services on an as-needed basis to the business units.
- *Awareness training*: The corporate group provides awareness training and material that is adaptable to the needs of a given business unit.
- *Security architecture*: Having investigated, designed, and implemented solutions for single-sign-on, web authorization, two-factor authentication, asset inventory, virus protection, etc., the corporate group may have solutions that can enhance the security of the business unit's SCADA environment.
- *Vulnerability management*: The corporate group provides the tools to the business units to characterize the risks and identify the appropriate solutions to their system vulnerabilities (e.g., Vigilinx's Intellishield).

To leverage these services, the business unit must have a proactive liaison to a responsive individual in the corporate group. To complete the picture, the business unit must also infuse information security responsibilities through its organization. Because it is likely to be infeasible to dedicate individuals to information security roles in the business unit's day-to-day operations, it becomes necessary for each individual to understand his or her responsibilities to the information security of the environment and for their business unit managers to, similarly, provide a framework to support those individuals.

An assessment of the information administrative and operational controls at the business unit level would emphasize the following characteristics:

- *Change control:* There is a process for planning, reviewing, approving, and documenting changes to the operating environment so that security controls are at least maintained.
- *Software Development Lifecycle*: The business unit has a defined process for planning, developing, testing, and deploying software changes to the environment in a way that ensures the security and integrity of that software and the environment as a whole.
- *Account management*: There are individuals responsible for ensuring that each system has the proper set of users with only the levels of privilege required to successfully carry out their jobs.
- *Incident response*: Although the larger framework for incident response may come from corporate, the individuals who must carry out the response are the SCADA custodians, and the types of incidents – the taxonomies – are often unique to the given operational environment.
- *System management*: The local team must adopt the technical standards from corporate, implement those standards, and ensure that both configuration controls and vulnerability patching are kept current. They must also faithfully conduct the system backups and reliably know that they can restore a critical failed system or critical data. Close monitoring of the system is likely to help identify anomalous, and potentially suspicious, activities.
- *Network management*: The local team must take similar steps for the network devices.
- *Information handling*: Both the owners of the data and their custodians are within the business unit, and must agree on and carry out suitable safeguards for the most critical and sensitive data. An example would be storage and transport of backup tapes.
- *Management practices*: Local managers can reinforce or detract from information security controls by adopting strong or weak management practices. Strong practices might include adherence to principles of least privilege, encouraging job rotations, and requiring week long vacations.

Other administrative and operational areas that share common values with those for information security are (1) personnel controls, (2) business continuity and disaster recovery, (3) physical security, and (4) building services. Each of these too typically has a corporate and a business unit component with corporate establishing a framework that the business unit adapts to its specific needs. The confidentiality, integrity, and reliability of the business unit's data rely heavily on these four areas.

Increasingly, the documents produced by the lead agencies (and their designated coordinators) recognize the crucial role that administrative and operational information security controls play in the licensee's security posture. NERC's *Security Guidelines for the Electricity Sector*, FERC's *Proposal for Security Standards*, and the NPC's report on *Securing the Oil and Natural Gas Infrastructure* all cover topics discussed in this section.

Technical Controls

One manifestation of solid operational controls is solid technical controls. Although the technical controls implemented in the SCADA environment are the most vital, typically the security of the SCADA environment depends also on those implemented within the greater corporate network.

In fact, for each company who is a custodian of our critical service infrastructure there is a blending of the SCADA environment and the greater corporate environment. Consider the following questions:

- Do operators need Internet access? How is that provided?
- Is there a distinct boundary between the SCADA and corporate networks? Are there firewalls, or other network controls, between the SCADA network and the corporate network?
- Are there trust relationships used in the administration of servers between a domain within the SCADA environment and one or more outside?
- Is there remote access to the SCADA environment for support purposes? How is that provided?
- Who are the users for the data acquired by the SCADA network? Where are they located? What data do they require to get their jobs done? How do they access that data?
- Who does network and server management? What tools do they use to monitor and manage the resources within the SCADA environment versus those on the outside?
- How do third parties providing higher-tier software or integration support access the SCADA systems when called upon?
- How are operators accessing corporate applications such as email? How are viruses and Trojans prevented, detected, and corrected?

A *complete* assessment of the technical controls to the SCADA environment **also includes** an assessment of the technical controls to the greater corporate network.

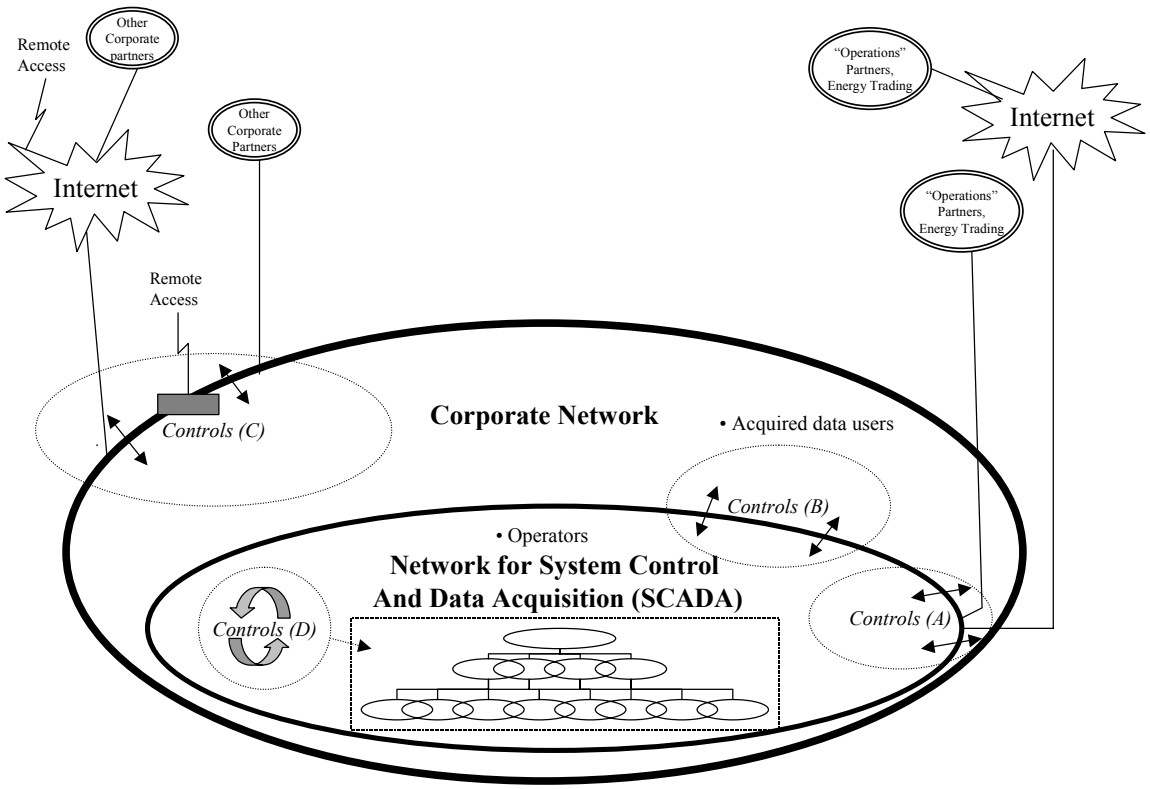

Figure 2: SCADA configuration and technical controls

Figure 2 is central to the rest of this section's discussion of the technical controls. Table 1 covers each of the "control points" labeled in the figure (A though D), illustrating first the probable need for a given traffic flow and then discussing the points one should assess to ensure the attendant controls.

Beyond the steady-state controls (as covered in the table) that must be in place under normal operating conditions, one must also consider the potential need to isolate the SCADA environment in the event of a security incident. For example, this could mean shutting down access at point A, point B, or both (as shown in the figure). The network access controls must make this kind of response not only possible, but also subject to prompt execution.

Control Points (As labeled in Figure 1)	**Associated Traffic Flows and Functions**	**Technical Assessment Topics**
A	Third parties will have either direct access to the SCADA systems or, more optimally, access to the data produced by SCADA systems. That access might be machine-to-machine (e.g., through Inter Control Center Protocol, ICCP) or through a man-to-machine interface (e.g., a browser). These third parties, labeled in Figure 2 as "operations partners", may require and may provide information such as actual or scheduled resource utilizations. The communications path might be over the Internet (via Secure Socket Layer or Virtual Private Network) or over a frame relay network or a dedicated line. Also data is likely to be sent out as input to logistics or energy trading back-office functions.	For the outside users of SCADA data (per A or B in Figure 2), an assessment should examine *at least* the following: • Location and sensitivity of data • Topology • Network access controls • System access controls • User Authentication • User Entitlements • Auditing and logging • Intrusion detection • Physical controls The assessment should also test the effectiveness of the controls through penetration testing of the relevant applications and vulnerability scanning of the supporting infrastructure. *
B	There are either (1) internal users of the SCADA resources or SCADA data or (2) providers of support through corporate IT services. Note: Those outside SCADA data users' access may need to be restricted not only to comply with sound general security practices protecting against the aforementioned threat scenarios, but also to comply with specific laws that "firewall" regulated and non-regulated businesses within the (e.g., NERC 888/889).	For the inside support services (per B and, if remote, per C in Figure 2), an assessment should examine *at least* the following: • The security of common points of management (e.g., Simple Network Management Protocol, or SNMP, consoles) • Trust relationships at the Operating System (OS) level • Protection of key shared resource infrastructure (e.g., domain controllers, Domain Name Services, authentication services) The assessment should also include vulnerability scans and penetration tests, both (1) from the corporate network to the SCADA network and (2) of the key shared resource

* Given the criticality of the SCADA systems, these tests should be performed by independent security experts with industry experience and unquestionable integrity.

Control Points (As labeled in Figure 1)	**Associated Traffic Flows and Functions**	**Technical Assessment Topics**
		infrastructure. This would ensure that technical controls on the network boundaries and network systems are implemented appropriately*.
C	Employees will require remote access to the corporate network. Corporate partners for other lines of business will require access to specific resources. Consumers and other interested members of the public (e.g., stockholders) will have access to Internet web sites.	For the outside access to the corporate network (per C in Figure 2), an assessment should examine *at least* the following: • Firewall topology and rule base; other Internet controls like content filtering • Authentication • Auditing and logging • Intrusion detection • Wireless Local Area Networks (WLANs) • Operating System hardening The assessment should also include an external vulnerability scan and penetration test as well as war dialing to ensure that remote access and Internet controls are not being circumvented all together*.
D	Within the SCADA network itself there are users, operators, and administrators of applications, operating systems, and network equipment, each with their own appropriate roles, each subject to particular controls.	Within the SCADA environment (per D in Figure 1), an assessment should examine *at least* the following technical controls: • Server hardening • Network equipment access controls • Server access controls • Physical security • Console security • Authorization according to principles of least privilege and segregation of responsibility • Secure communications • Wireless Local Area Networks (WLANs) The assessment should also include an internal vulnerability scan on the devices within the SCADA

Control Points (As labeled in Figure 1)	Associated Traffic Flows and Functions	Technical Assessment Topics
		environment to assess the damage that a motivated internal attacker could cause*.

Table 1: SCADA Technical Assessment Topics

Another important facet of the technical controls within the SCADA environment (D) is the security of the Remote Terminal Units (RTU's) at the multitude of monitoring and control points. Although these are, more often than not, polled or set through dedicated connections, there are many exceptions that require consideration. They are frequently accessed through modems on the public telephone network, through semi-public X.25 networks addressable through Switched Virtual Circuits (SVC's), through VSAT, and spread spectrum radio. The level of accessibility, and hence exposure, of any given RTU or collection of RTUs, varies for each; and the impact of an exploit would also vary depending on the compensating pneumatic controls and the criticality of the given control point(s). Although it is true that the obscurity of RTU register positions and wiring would require a perpetrator to gather a significant amount of intelligence to coordinate an effective attack, the technical controls at the lower tiers of the SCADA architecture are as critical as those at the top. In some SCADA environments, the manipulation of a few key end-points could have a large cascading effect.

Tactical Steps

As discussed, there are a large numbers of factors that affect the information security posture of the SCADA environment. Beyond conducting an assessment to determine the organization's relative strengths and weaknesses, one might well ask: "What initial steps should an organization take to establish necessary information security framework, or the kind of framework envisioned by the 'lead agencies?'"

Naturally the priorities depend, and will depend, on the regulatory requirements. Although the power grid has its own distinct threats, the FERC "Proposal for Security Regulations" provides some prioritization helpful to most SCADA configurations. That document has an addendum that is a checklist for self-assessment with about 15 to 20 items. Those items fit within the following general areas:

A. SCADA security owner
B. Identification (and classification) of critical assets and perimeter definition
C. Policy development, documentation, and maintenance
D. Screening, training, and physical security procedures
E. SCADA perimeter logical access controls
F. SCADA perimeter physical access controls
G. Incident response, incident reporting, and business continuity planning

These seven areas roughly build upon one another suggesting the priorities and the order in which they should be tackled. As illustrated in Table 2, each has some key initial steps. Further details that depend on the organization and the results of an initial assessment.

Critical Area	Key Initial Steps	Comments
SCADA security owner	Assign an officer as an owner for security of the given SCADA-controlled operational environment.	This will inevitably lead to the question of who the owner's asset custodian(s) will be.
Identification (and classification) of critical assets and perimeter definition	Identify the assets that are most critical to the operations of the underlying infrastructure (e.g., power grid). Include systems and groupings of data. Classify the systems and data groupings according to a corporate standard. That standard will key on availability (how vital the system or data) and integrity (how critical the system or data)	Prior Y2K efforts may provide some guidance. Prior business continuity and disaster recovery efforts may prove useful as well. Lead agencies such as FERC will want classification that distinguishes between criticality to the company and criticality to the national infrastructure. This will be useful in defining the "perimeter" noted at left. Having a solid understanding of one's computing and data assets and how they are critical to the operation of the SCADA environment is fundamental to knowing what to protect – and how to protect it.
Policy development, documentation, and maintenance	Focus first on policies that mandate information security-related roles and responsibilities, associated training, and employee screening according to those responsibilities. Define authentication and authorization policies for computer systems, and within the policy authorize the creation of complementary standard practices. Prioritize, and create authentication and authorization standard practices for platforms most critical to the SCADA system; and for the SCADA network perimeter and its access controls. Create policy that authorizes an incident response team to investigate information security incidents. Ensure that corporate privacy policies invest company with the authority to investigate possible employee wrongdoing, and are general enough to include use of all SCADA-related systems. Create policy detailing procedural requirements for secure areas (e.g., escorting visitors, no tailgating).	
Screening, training, and physical security procedures	If there are applicable regulations, identify all of the SCADA custodians and operators who must undergo screening. Institute screening exactly as specified in regulations.	

Critical Area	Key Initial Steps	Comments
	Once physically secured (as below), make SCADA custodians and operators aware of procedural requirements associated with SCADA-related secure areas. Create material, and conduct general information security awareness training, keying on the importance of vital SCADA assets, their general custodial responsibilities, and the absolute need to report security incidents and perceived weaknesses (i.e., "concerns"). Develop job descriptions or responsibility statements that cover information security and follow from the policies. Review these with each SCADA operator and custodian.	Training on specific information security tasks within those job descriptions will follow later.
SCADA perimeter logical access controls	Identify the traffic flows in from and out to outside systems and users. Design the perimeter controls. Consider techniques such as the use of shared-resource DeMilitarized Zones (DMZ's), two-factor authentication, segregation of domains, and "pushing out" SCADA data. Pilot, test, and implement.	Depending on the interconnectivity that already exists, this is potentially the longest lead-time area in this table. It is also potentially quite disruptive if not done systematically. Fortunately, the design principles should be largely reusable for different SCADA environments within a larger company. Network analysis tools are likely needed to identify what traffic is flowing, although they won't necessarily identify what should be flowing. The design is highly dependent on the detail of the company, its standard technologies, its operations organizations, etc.
SCADA perimeter physical access controls	In conjunction with the design noted in the previous area, be sure that the access controls assigned to various secure space is consistent with the levels of trust assigned (logically) to different network regions. As needed, add physical access controls for secure areas (with vital central SCADA systems) such as card readers, a solution that provides accountability for the users, the authorizers, and the administrators.	
Incident response, incident reporting, and business continuity planning	Make the creation of a Computer Incident Response Team a priority initiative for the corporate information security group. Document standard practices; identify, purchase, and receive	The corporate group will need to be conversant with the unique threats facing the SCADA environment and the technologies used within the SCADA infrastructure. A third-party security knowledge solution such as Vigilinx's

Critical Area	Key Initial Steps	Comments
	thorough training on forensics tools; create forms; devise communications methods; work closely with the constituency (here, the SCADA custodians); if possible, conduct drills. Educate the SCADA custodians on their reporting responsibilities and the "do's and don'ts" in initial incident handling.	Intellishield covers this "threatscape" as well as vulnerability management for these technologies. The suggestion that this function reside with the corporate group is based on the specialized expertise to handle computer forensics.

Table 2: Key Initial Steps

Conclusion: Vigilinx Ties It Together With Recommendations and Metrics

Vigilinx uses this holistic approach in its SCADA assessments. By examining the technical controls at these critical points in your overall network topology and by assessing the "people" and "process" aspects of your overall information security program in our *Vigilinx Business Security Assessment (VBSA)*, Vigilinx provides the "infrastructure services custodian" with specific recommendations and a complete gauge of the security posture as it relates to the three key threat scenarios defined earlier in this white paper.

From the onset our assessment approach is to be open in our communications and to be problem solvers. We endeavor to make our recommendations specific, timely, prioritized, risk-based, and easily assignable, so that you can embark on immediate fixes and begin to formulate longer-term plans.

From the assessment, whatever the maturity of your information security program, Vigilinx looks to be a partner in further mitigating the risks to the SCADA infrastructure and cost-effectively improving your posture to SCADA security threats. With an array of Professional, Managed, and Knowledge Services, Vigilinx can play a leading role in establishing the framework discussed in this white paper, both at the corporate and at the business unity level.

The benefits go beyond compliance to industry regulations on information security. The company may demonstrate sector leadership on information security compliance; and a sustained and improving information security program will lower financial risk, promote services reliability and integrity, and thwart a determined enemy.

For more information about Vigilinx's SCADA assessment and other service offerings, see our web site at www.vigilinx.com or contact us toll-free at 1-866-481-4101.

References

1. Vigilinx Intellishield Service, *Vigilinx Geopolitical Analysis Report: Potential Infrastructure Cyber Attacks*, October 18, 2001
2. Federal Energy Regulatory Commission, *Proposal for FERC Security Standards, Draft V0.5*, July 17, 2002
3. National Petroleum Council, Committee on Critical Infrastructure Protection, *Securing Oil and Natural Gas Infrastructures in the New Economy*, June 2001
4. North American Electric Reliability Council, *Security Guidelines for the Electricity Sector*, June 14, 2002