

“SCADA Security, Compliance, and Liability – A Survival Guide”

By: Clint Bodungen, Jeff Whitney, and Chris Paul – July 8, 2008

Two of the hottest topics currently in the industrial world are security and compliance. The controversy surrounding these topics, centers on the interpretation of how they should be addressed in the current environment. Although regulatory bodies, industry trade groups and industry participants are working diligently to provide clear and concise guidance to industry participants, no prescriptive or definitive roadmap exists to achieve full compliance. As a result, operators are being confronted with an almost overwhelming amount of standards, guidelines, and “best practices” that require interpretation with little guidance. Exacerbating the issue is the fact that operational and security requirements are often confusing and sometimes inconsistent. As examples, security related documents often purport to be the required standard, even when they are not, while security programs are not tailored to meet the needs of specific operations.

Addressing the issues involving these topics requires an understanding of the requirements and the development of an appropriate solution. While a one-size-fits-all solution is not possible, there is a process (hereinafter, the “Holistic” approach) that aggregates the requirements and best practices available to industry, allowing each company to design and implement a solution that makes sense for its organization and facilities. The Holistic approach provides a roadmap to help achieve compliance, while avoiding the fatal error of looking at security as simply an “add-on” issue to operations. The pitfall with the widely used add-on approach is that these narrowly focused security solutions often temporarily address technical requirements, while failing to consider additional requirements related to compliance with evolving regulations and standards.

SCADA (Supervisory Control and Data Acquisition) systems users have been the most severely impacted by the increase in recent activity. On the security side, SCADA operators are confronted with the lingering “IT vs. SCADA”, or “them vs. us”, issue, along with the cyber security threat debate. One faction swears up and down there is a real and valid cyber threat to critical infrastructure. Another claims there isn’t enough evidence to support such a claim and that the real threat actually lies in other factors such as physical or human risk factors. We believe that both threats are real and need to be addressed. With compliance activity on the increase, the challenge is for operators to interpret and potentially comply with the myriad of standards, guidelines, and best practices that have been released. Unfortunately, these documents provide very little guidance on exactly which standard or best practice addresses the various threats currently confronting operators. Even in more regulated industries, such as Electric Utility where definitive regulatory guidance has been established with NERC CIP, the requirements are still so vague and watered down that neither security nor compliance is assured. All of these issues have the potential to cause serious repercussions to your organization, as an incident or an audit failure could result in significant financial loss. This article addresses these issues, taking the Holistic approach.

Where is the threat anyway?

Is there the potential for an actual cyber threat or is it just media hype? In short, yes, cyber threats do exist for SCADA systems. Is the potential for cyber threats as great as some claim them to be? Probably not. Many have asked, "If there is no hard core evidence of a significant [outside] cyber attack on an industrial network, where is the threat?" The answer is that these types of threats are becoming more likely, as current SCADA systems and networks increasingly utilize commercially off-the-shelf (COTS) software, connect to the enterprise layer and move toward IP connectivity. These recent changes have contributed to higher threat levels and increased vulnerability.

A few short years ago, the chances of someone finding these vulnerabilities and exploiting them were very slim. This was due to the fact that process control systems and SCADA networks were unheard of by the general population and systems were based on specialized platforms that were segregated from the enterprise layer. In recent years, industrial systems have begun to take a front seat in the spot light, due to the focus by the Department of Homeland Security on national critical infrastructure and some unfortunate media coverage. Despite current efforts, there is a high probability that something bad is *eventually* going to happen. Evidence recovered from Al Qaeda suggests that terrorists have taken an interest in our SCADA networks (see, for example, Washington Post article dated March 11, 2005, entitled, "Hackers Target U.S. Power Grid"). In addition, the number of "SCADA hacking" presentations is increasing at security and "hacker" conventions, with the number of vulnerabilities discovered within these systems increasing. Bottom line, our little corner of industry is no longer isolated and the word is now out.

While cyber security is being given the lion's share of attention, with "hackers" already attracting premature blame from a few recently publicized incidents, the widespread disregard for physical and operational security within many organizations has become a huge concern. Many companies are heavily focused on shoring up their cyber security, with little or no regard for physical security. When asked about their physical security, they too often reply as follows: "Well, we know our physical security is weak... but what can you do?" Even though most of the current standards emphasize cyber security, it is important to remember that physical and operational security weaknesses can provide an alternate attack vector to SCADA systems and networks. When asked to perform penetration testing of company systems, we have experienced a 100% success rate at gaining unauthorized cyber access by taking advantage of neglected physical and operation security controls. Companies that have addressed cyber, physical and operational security will be much better positioned to defend themselves. Taking this Holistic approach will address both the threats posed to their systems and the threats posed by persons in government, the media, and lawyers who will want to assign fault in the event a security breach results in an incident.

Regulatory Confusion

Beyond potential cyber, physical and operational threats, operators must now also contend with regulatory compliance. The compliance landscape is currently a complex environment in that each industry vertical must navigate through multiple regulatory requirements, industry standards, guidelines, and best practices. Exacerbating this challenge, most of these documents are very ambiguous, with little consensus on strategic guidance or tactical implementation. The bottom line is

that asset owners and operators across all industry verticals are not only unsure as to exactly *how* they must meet compliance and secure their systems, but also to what standards, guidelines, or best practices they may be held accountable. As a result of the lack of clearly delineated requirements, operators are susceptible to various interpretations. This could lead to an audit failure or out-of-context scrutiny subsequent to an incident penalties and potential legal liabilities.

Where are the liabilities?

The regulatory environment is placing increased demands on SCADA systems, driving data capture and retention, documentation, training, security, policy, and reporting requirements. As a result, operators and vendors are taking steps to incorporate the impact of regulatory and legal issues (sometimes referred to collectively as “compliance” issues) into the design and use of the systems.

Legal requirements and trends have placed new emphasis on maintaining compliance, because compliance issues are subject to increasingly aggressive enforcement. Compliance is of great significance in any incident where SCADA systems may be a core component of an investigation, lawsuit, or regulatory enforcement action. Compliance failures have resulted in large fines, jail time, injunctive relief and bad press.

Threats to operators also include the potential for misinterpretation and misuse of data. Knowledge of the data, and the obligation to understand what it means or implies, will be imputed to operators and management. This means responsibility and punishment will reach into the highest levels of management. Operators and management are now facing the potential of charges of negligence being changed to allegations of willful misconduct. In addition, they are confronted with the possibility of criminal liability and increased civil exposure.

Businesses with any form of SCADA-controlled operations must be aware of potential liabilities and take prompt and appropriate actions to minimize them. Personnel with the responsibility and expertise to manage SCADA for and in these businesses are the first line of defense against charges of noncompliance violations and lawsuits. They should be able to recognize the various exposures faced by the company if the SCADA system (or an operation controlled by SCADA) fails operationally, suffers a security breach, or is in violation of compliance issues.

The following scenario illustrates the types of issues that can flow from a failure in an operation, especially a failure where an incident occurs.

If an operation fails in any way that is significant outside of the company, then it usually follows that agencies and other outsiders will become involved. “Significant outside of the company” can mean an adverse economic impact on a third party (“the pipeline went down because of a leak, resulting in gasoline supply disruption”), injury or damage to the environment, or injury or death of any person (including an employee).

The outsiders will look at the failure and the company, either because they have the public charter to do so (the FTC at supply disruption, DOT at pipeline safety issues, OSHA at injuries or deaths of employees, law enforcement or injury or death of third parties, the EPA at environmental issues, etc.), or because they see an opportunity to make money (plaintiff lawyers). The outsiders will look at operations with

20/20 hindsight and, depending on the incident, may look deep into records, security, policies and procedures and the decisions of the company.

Although a failure may be SCADA related, the cause of the problem is usually external to the SCADA system. Provided the SCADA system is integrated correctly (incorporating the Holistic model consisting of operations, security, and compliance), it can actually help supply the answer to what caused the problem.

The SCADA records likely will have a critical place in the midst of the scrutiny. The first hurdle facing the company is ensuring that the records can be produced. There are certain requirements in regulatory schemes for records retention (for example, see 49 CFR 195.404 regarding liquid pipelines in the United States). Failure to produce the required records may not only be a violation, but may also raise a presumption that the company destroyed the data because it has something to hide. If a civil lawsuit is filed, rules regarding evidence preservation may come into play, along with issues regarding records that are part of common law requirements as well as regulations like Sarbanes-Oxley in the United States.

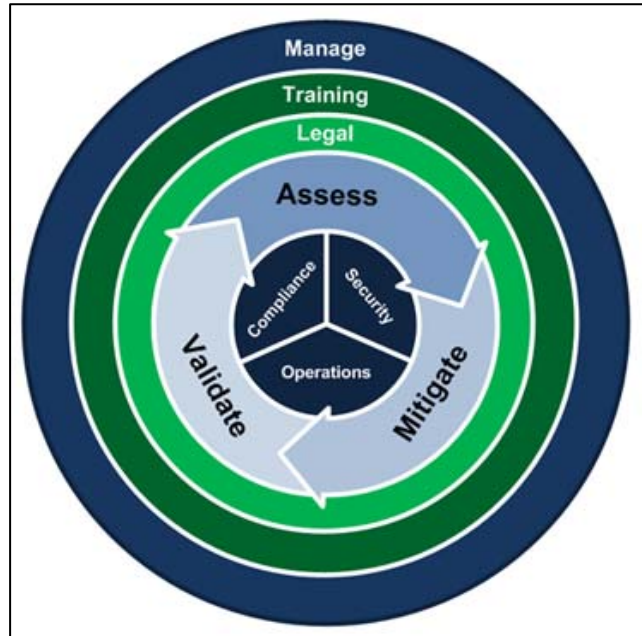
Assuming the records and data are available, they will be dissected to find any "problems" in operations. The scope of the investigations will not end there. Regulators and plaintiff lawyers will look at compliance, training given to operator personnel, the manuals and policies underlying training, the age of the system, physical security of the system, the ergonomics of the SCADA control room and system, and many other factors to find fault with the company. Even if the incident resulted from a security breach caused by a criminal act of a third party, the company will be held responsible on the theory that its security, because it was breached, was obviously insufficient.

Vendor exposures are also multi-faceted. During the course of an investigation, vendors will be subject to subpoena and discovery by regulators and plaintiff lawyers seeking information about the activities of the vendor on behalf of an operator. Vendors will need to have maintained their working files in accordance with the requirements of the operator's contract. Although contracts normally require the vendor to provide prompt access to its records and files, such access is predicated on auditing by the operator of the vendor's work, rather than seeking to preserve records that may become important during an investigation or litigation.

In the best of circumstances, vendors can plan on having their business disrupted if their client has a problem. In worse cases, the vendor can plan on being a defendant itself. In this scenario, the vendor may face the choice between accepting some liability or blaming its customer for the failure. The latter action may result in the vendor crippling its business prospects with not only the customer involved, but other operators in the industry.

How do I address the current environment? The Holistic Lifecycle Model for Security and Compliance™

The most comprehensive way to address each of these issues is with a Holistic Lifecycle approach that spans across compliance, security and operations. The Holistic Lifecycle Model for Security and Compliance™ consists of proven methodologies aimed specifically at Critical Infrastructure and Industrial environments. It is designed to assist operators with maximizing security and achieving regulatory compliance, while minimizing liability from legal action and broad auditor interpretation. The model is a complete and thorough set of processes that go far beyond just the typical SVA (Security Vulnerability Assessment), gap analysis, or self assessment (which are all actually smaller pieces of an entire compliance process). Each phase of



the model builds on the other as an integral part of a complete lifecycle, creating a seamless set of security methods and solutions supported by solid due diligence for compliance. The model spans across all aspects of compliance, security and operations by including methods for proper standards/guidelines/best practices selection, security assessments (physical, facility, cyber, and operational), gap analyses, risk analyses, organizational threat modeling, mitigation/remediation strategies and integration, legal support, and management/maintenance programs.

How it works

The following section will address the basic flow for each phase of the model. Much of the technical detail for this section goes beyond the scope of this article and is highly dependent on direct interaction with each individual operator's environment.

Phase 1 - Assessment

Whether you are using a self assessment tool such as CS2SAT, or a 3rd party consultant to perform an SVA or Gap analysis, the goal of an assessment is to identify vulnerabilities and/or gaps in your current environment. An SVA or gap analysis alone, however, will not ensure that your organization is secure or compliant. In fact, if done improperly, they can actually create liability for your organization. Many organizations are not aware that there are many necessary steps to a proper assessment, which are all part of a larger lifecycle that help build solid due diligence. A complete assessment phase consists of the following steps:

1. Standards Identification and Selection – The first step in achieving security and compliance is to initiate an exhaustive search of all the regulatory requirements, industry standards, guidelines, and best practices that may fall within your industry vertical. Even if some of the standards,

guidelines and best practices were originally intended for another industry vertical, it is recommended that you review and/or include them in the list of potential requirements to achieve compliance. For example, a petroleum company may fall under CFATS if they transport certain chemicals. This list can then be narrowed down to the hand full of documents that you believe provides the best set of requirements matching your organizations infrastructure. The idea is that you can show you have performed due diligence in your research and exclusions to achieve compliance, in the event an auditor or attorney doesn't see a specific document referenced. All of these documents must now be put into a matrix, identifying a comprehensive list of categories, cross referenced to the relevant sections in each document.

2. Policies and Procedures Analysis – Once you have created the regulatory requirements, industry standards and best practices matrix, your organizations internal policies and procedures must be added to ensure compliance with Corporate mandates. A policies and procedures analysis should be performed. Personnel interviews should be added as well for improved accuracy. This will give you a clear picture of how well your current written policies and procedures cover the regulatory requirements, industry standards and best practices contained in the matrix.
3. Critical Asset Identification and Classification – Certain industry verticals such as Electric Utility and Chemical, for example, require identification of critical assets by quantifying certain attributes. This should be done according to the standards for that particular industry vertical, with the understanding that this process may be governed by specific regulations regarding confidentiality and management of information.
4. Security Vulnerability Assessment (Cyber, Physical, and Operational) – The majority of standards, from all industry verticals, prescribe at least some version of a vulnerability assessment (SVA - Security Vulnerability Assessment). These assessments typically focus on cyber elements, leaving gaps in compliance and security. Even if, in your current role, you are only concerned with the cyber aspects of compliance and security, you are still leaving vulnerabilities in your cyber security, as the physical, operational, and human elements can provide an attack vector to your cyber systems. As a result, it is highly recommended that, in addition to your SVA, you also perform additional tests to include a physical SVA and/or a “Red Team” test. These tests will help evaluate all aspects of your cyber, physical, operational, and “human factor” security.

(TECHNICAL NOTE: Only proper, SCADA or process control system (PCS) approved assessment methods should be used to assess these environments. Such methods should only be performed by individuals with extensive experience in assessing and testing SCADA and PCS environments. For example, all tests should be run on a backup system, in a test lab or another form of non-production environment of like systems and configurations. Only very specific true passive tests that have been proven safe on non-production systems should be performed on production environments).

(LEGAL NOTE: It is critical how an operator documents and communicates the results of any security vulnerability assessment. Failure to manage the documentation may result in the

assessment simply serving as a road map for attorneys or agencies to attack security programs. Such misuse can happen even if such attacks take the necessary self-critical analysis involved out of context and fail to consider that the company based security decisions on a risk matrix that carefully considered probability and consequences to address the most viable and serious threats).

5. Assessment Validation – All analysis and SVA results must be validated. This can be accomplished by a combination of results analysis, penetration testing and interviews. For Cyber assessments, simply running vulnerability assessment tools such as Nessus and reconnaissance tools such as NMap will not achieve a complete and proper vulnerability assessment. In addition to leaving gaps in security, these tools can produce false positives as well as false negatives.

(TECHNICAL NOTE: It is critical that proper SCADA or process control system approved testing methods should be used to test these environments.)

6. Risk Analysis – All of the data that has been gathered thus far in this phase must be analyzed to provide a clear picture of the current levels of security, compliance and risk. Any risk formulas and threat models used, should be specific to your industry and customized for your organization. This can be a complex step, requiring an experienced professional versed in risk analysis formulas and threat modeling.

Phase 2 - Mitigation/Remediation

In this phase, policies and procedures will be revised and enhanced to reflect the current environment. A mitigation strategy will be built, based on the data from the Assessment Phase, with mitigation/remediation solutions identified and put in place. We are often asked, “How do you know that your interpretation of the standards is correct when developing policies and procedures and mitigation/remediation solutions?” What is important to remember here is that the standards, guidelines and best practices are not being interpreted. They are being referenced by specific sections in the matrix. If you can show that you have performed exhaustive due diligence, in an effort to clarify and satisfy any vague requirements of a particular standard, you should have a solid defense in the event of an audit or possible litigation.

Phase 3 - Validation

Validation verifies that implemented remediation and mitigation have been deployed and are being effective at improving security and achieving compliance. This is accomplished by revisiting certain aspects of the Assessment Phase. A complete vulnerability assessment should be re-run, along with any other step from the Assessment Phase, in order to address any key areas of concern. Use this phase to fine tune strategies and solutions as needed. The Validation Phase should also be revisited at least once a year or as prescribed by changes in regulatory, industry and corporate requirements in the particular industry vertical.

Phase 4 - Legal

Many organizations are not aware that simply performing an SVA or other self-critical analysis can actually create liability if the data is not properly handled. It is also very important to remember that improper standards and best practices selection can create liability as well. The following questions must be asked - Has the organization performed the necessary due diligence and covered all angles necessary to prevail should someone take legal action against you as a result of an incident? Is the organization prepared for auditor interpretation that could lead to regulatory fines? The Legal Phase is active throughout the entire Holistic model lifecycle, ensuring no other processes undertaken in good faith to reduce risk have the unintended result of creating liability, both short and long term, for the organization, and that regulatory changes are worked into the model.

Phase 5 - Management

Once remediation and mitigation have been deployed and validated, a long-term program must be put in place to ensure that all processes, procedures, and technical safeguards are monitored, maintained and kept current with emerging threats and changing industry requirements.

Phase 6 - Training

Training is a critical part, if not the most critical part of the Holistic Lifecycle model to achieve security and compliance. All stakeholders must be trained in understanding the strategic approach and tactical implementation of the model or the organization will not achieve the desired outcome. Training is reference in many of the regulatory requirements and industry standards as a critical component of security and compliance. A training program should be developed and implemented, with a strong communication component, to ensure success. All stakeholders should have a clear understanding of roles and responsibilities, communication security and protocol, and document security and transmission protocol.

Conclusion

Security issues with SCADA systems are rapidly expanding, creating new challenges for operators. This escalation in security concerns is due to increased awareness of these systems, changes in systems and configurations, creating new and in some instances increased vulnerabilities, and personnel (training) related issues in increasingly complex environments. Taking the necessary steps to identify and address these risks is not an option, but an imperative. Coupled with emerging security challenges, changes in the current regulatory environment of increased enforcement has compelled operators to address Compliance with regulatory requirements, industry standards, industry guidelines, industry best practices and corporate policies and procedures.

Companies have a duty to address compliance and security issues. The Holistic Lifecycle Model for Industrial Security and Compliance™ provides the framework to develop an on-going process to achieve necessary levels of security, while addressing compliance. It was designed to assist operators of Industry Control systems with meeting security and compliance in the rapidly changing environment. Operators that use this approach will have a greater understanding of current and emerging requirements, their

current infrastructure and the solutions required to achieve security, compliance and operational objectives.

Authors' Note

The information herein is not, nor is it intended to be, legal advice. You should consult an attorney regarding your particular situation. We reserve the right to determine whether to accept any matters referred to us for representation. Until we have agreed to being hired by you in regard to any legal matter, we are not your lawyers. Never send confidential or sensitive information to us by email without our permission. By sending such information, you may be waiving any potential attorney-client confidentiality privilege.

The Authors

Clint Bodungen has over thirteen years of experience in both physical and systems security, most of which has been dedicated to industrial systems, process control, and SCADA. He began his professional career as a Computer Systems Security Officer and Operational Security Manager in the United States Air Force, where he participated in both physical and cyber red team (covert) Operations. Following the Air Force, he was employed by a major security software vendor to test Network Intrusion Detection Systems (IDS), including authoring several custom IDS evasion and penetration testing tools. Over the past decade, Mr. Bodungen has built corporate security departments from the ground up, led numerous security assessments and penetration testing teams, and has played a key role in securing some of the nation's top organizations within the heart of our nation's critical infrastructure industries. These industries include the DoD, DoE, top Oil & Gas companies, financial institutions, utility companies, and major telecommunications companies. Mr. Bodungen was the Co-Founder of the Critical Infrastructure Institute and the founder/principal analyst of CIDG, Corp. (Critical Infrastructure Defense Group), where he continues to perform PCN/SCADA security assessments, red team testing, and regulatory compliance consulting.

Chris Paul focuses his practice on transactional and regulatory matters, including related litigation. He provides counseling to refining, manufacturing, and transportation operations on subjects including liabilities and exposures, regulatory and compliance programs, risk management, and development of training and management systems. He has extensive experience with pipeline issues, including transactions, integrity programs, SCADA auditing, contracting, and emergency response and litigation. Chris is admitted to practice in Oklahoma, Pennsylvania, Arkansas and Kansas, the United States Supreme Court, and various United States District Courts. He is also an instructor on Oklahoma State University's Environmental Management Program. Prior to his present practice as an attorney and counselor, Chris worked in-house with Sun Company and as the environmental manager of its Tulsa Refinery. Prior to his commercial endeavors, Chris was a United States Army JACG lawyer with the Seventh ID(L) and a Special Assistant United States Attorney.

Jeff Whitney is an entrepreneur and computer professional with over twenty-five years of management and technical experience in Real Time (Mission Critical) Process Control Systems. He has extensive

experience assisting pipeline companies with SCADA system integration, SCADA security, SCADA consulting and Compliance. His SCADA experience includes Pipeline Control Center consolidations, SCADA system migrations, SCADA system upgrades, SCADA Security audits and Industry and Regulatory Compliance for major Oil & Gas Companies. He currently serves on several non-profit boards, as well as the University of Houston Industrial Advisory Board, and is an owner/principal of Berkana Resources Corporation (BRC). BRC provides integration, security, compliance and audit services to customers utilizing Supervisory Control and Data Acquisition (SCADA) applications. As an independent integrator, BRC provides these services using a wide range of SCADA applications in the Oil & Gas, Water and Utilities markets.