

RTAP Users Group Meeting 2005 A Broader View of SCADA

By: Jeff Whitney, Berkana Resources Corporation &
Chris A. Paul, Counsel for Berkana Resources.

Introduction

SCADA systems have evolved to provide information and control over complex and critical processes. The operational component has consistently and justifiably remained the focus of SCADA, as this is the primary function of the system. Systems integration has therefore emphasized operational stability by addressing technical issues, while continually expanding efforts in improving ergonomics and systems security.

This paper will discuss a broader view of SCADA integration that addresses issues with not only the operational, but also the security, regulatory and legal components of SCADA. The paper will also provide suggested solutions, incorporating expanded integration efforts to meet the challenges posed by the issues of security and compliance in the current environment of increased regulatory scrutiny and legal exposures.

The Changing Environment

Future systems integration efforts must take an expanded view of the role of SCADA, as Operators and Vendors take steps to incorporate the effects of regulatory and legal issues (sometimes referred to collectively as “compliance” issues) into the design and use of the systems. Regulatory requirements place demands on SCADA systems, driving data capture and retention, documentation, training, security, policy and reporting requirements, among others.

Emerging legal requirements and trends have placed new emphasis on maintaining compliance, as Regulations are increasingly subject to enforcement. Compliance is of great significance in the event of any incident where SCADA systems may be a core component of any investigation, lawsuit or regulatory enforcement action. Operators now can point to specific events where failure with compliance has resulted in bad press, large fines, and jail time.

In this new environment, threats for 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, can now be imputed to Operators and Management. This represents a significant shift in liability, moving responsibility up the chain of Management. Operators and Management are now facing the potential of changing charges of negligence to allegations of willful misconduct. In addition, they are confronted with the possibility of criminal liability and increased civil exposure.

What can go wrong?

Too often, a corporation's Management, Operators and Counsel accept the status quo as adequate performance. They fail to see their practices as they might be viewed by regulators or the public, who may mistrust business and fear unknown impacts from the business operations. Many businesses believe that because a certain facility or operation has not received a Notice of Violation from the governing agency, the current state of operations is within compliance and that there is no exposure. Businesses often fail to consider how a civil law suit will result in the mining of company data and files for information, which becomes fodder for plaintiff lawyers. These lawyers will attempt to convince a jury that the company needs not only to pay for a perceived wrong, but that it should be punished for the wrong as well. *Management often believes that because "it has always been done this way," it must be sufficient to avoid liability. The problem is, the way it has always been done may be precisely the reason exposures and liabilities exist.*

Any business with any form of SCADA controlled operations should be advised of potential liabilities and guided to minimizing them. Personnel with the responsibility and expertise to provide advice to these businesses, are the first line of defense against charges of violations and lawsuits. These personnel should have an in depth understanding of the business and operations of the company. In addition, they should be able to recognize the various exposures faced by the company, if the integrated SCADA system (or an operation controlled by SCADA) fails operationally, suffers a security breach or the company is confronted with compliance related issues.

The first step that companies sometimes undertake is an audit. Audits can be performed on the entire SCADA system, including the PCN, Application layer, operation systems, field devices, communications, etc., or focused just on SCADA security or Compliance. These are necessary and important activities, but, as discussed below, need to be conducted in a fashion that avoids the creation of unnecessary liabilities or issues. Along with an audit, programs need to be in place that provide mechanisms for addressing the issues raised in audits. These programs should recognize and document changes in operations on an ongoing basis, to include training personnel to recognize and address these changes.

So what can go wrong? Although a number of examples will be discussed during this presentation, they were not included in this paper for brevity. The examples discussed in the presentation will show that the problems generally flow from the following pattern:

Something in an operation fails (an incident occurs). Although it may be SCADA related, the cause of the problem is usually external to the SCADA system. Provided the SCADA system is integrated correctly (incorporating operations, security and compliance), it can actually help supply the answer to what caused the problem.

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

The outsiders will look at the failure and the company, either because they have the public charter to do so (the FTC or DOT at supply disruption, OSHA at injuries or deaths, the EPA at environmental issues), 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, procedures and the decisions of the company.

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 the Sarbanes-Oxley scheme.

Assuming the records and data are available, they will be carefully reviewed to point out any problems in operations. Unfortunately, the scope of the investigations will not end there. Regulators and plaintiff lawyers will look at training given to Operators, the manuals and policies underlying training, the age of the system, system security, 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, since breached, was obviously insufficient.

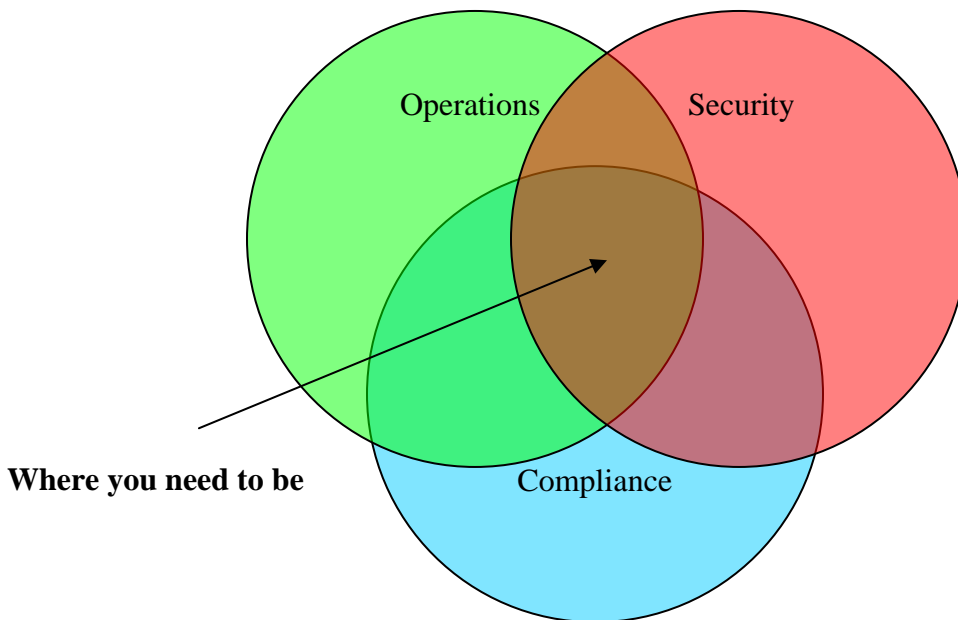
Another example of the changing environment facing SCADA vendors and users involves security audits. Failure to conduct an audit may result in operational failures, as well as severe legal implications. As noted above, failure to actively look at systems to evaluate adequacy may itself be a negligent act subjecting the company to regulatory action or a civil lawsuit in the aftermath of an incident. Again, the government may hold Operators liable for failures of their security, even if a breach is caused by third party criminal conduct.

Conducting an audit creates its own set of issues, as any form of system analysis may create evidence of an incriminatory nature that could be used against an operator by a regulator or plaintiff attorney. This internal information, created by an audit, could be used as a platform to claim defects in the system that resulted in some noncompliance or damages, however remote from the actual facts. Therefore, it is critical that audits be done, but be done in such a manner as to minimize exposure.

The good news is that there are ways to determine how your company will fare in the event it is placed under the spotlight of public and regulatory scrutiny. *The key is to take steps for Management to learn about the impact of the U.S. Federal Sentencing Guidelines and similar tools from discussions with their personnel rather than from a judge imposing a prison sentence.*

How should I approach the new Environment?

The following chart represents a highly simplified 30,000-foot view of the three primary factors influencing SCADA Operators and Management in the current environment and the effects of placing emphasis on specific factors:



Major Emphasis	Advantage	Disadvantage
Operations	Maintain 99.999% uptime, improve ergonomics and functionality.	Little to no emphasis on Security or Compliance, leaving operations, operational personnel and Management exposed for security and regulatory scrutiny and/or action, and increased exposure in lawsuits.
Security	Maintains maximum protection from threats to PCN.	If not properly integrated, may sacrifice some business objectives and operational functionality. Security and Operational policies and practices may not meet regulatory compliance mandates.
Compliance	Protection against adverse regulatory actions and lawsuit exposure if an event occurs.	Don't want lawyers running your SCADA operation. If not done properly may compromise some business objectives and operational capabilities. Security and Operational policies and practices will need to be aligned with regulatory compliance mandates.

Operations and Security	Maximize capabilities while maintaining a secure environment.	May expose operational personnel and Management to regulatory scrutiny and/or action, and increased exposure in lawsuits.
Operations and Compliance	Allows focus on operational capabilities while addressing compliance.	Requires increases staff involvement to accomplish. Security issues may develop between enterprise layer requirements and regulatory security mandates.
Security and Compliance	Aligns security policies and practices with regulatory compliance mandates.	If not properly integrated, may sacrifice operational capabilities and business objectives.
Operations, Security & Compliance	Maximizes operational efficiency and security while minimizing regulatory and lawsuit exposure.	Staff may need to cross internal political boundaries to accomplish.

Solutions

The following are suggested solutions to assist companies with SCADA operations to achieve a balance between Operations, Security and Compliance. They are not meant to be “all inclusive”, nor do we suggest that implementing these suggestions will ensure that you maximize Operational efficiency while addressing Security and achieving Compliance. They are just suggestions to get the reader thinking about aligning these objectives. Suggested solutions for Operations are not provided, as business objectives, technology and infrastructure vary from company to company, with the subject matter too broad to address in the scope of this paper.

Compliance

Ironically, the key to solving many of these issues is found in review of the very guidance the government would use if a company was about to be sentenced for violation of rules.

The *best protection* that Management can provide to minimize liability is enactment of *corporate policies and practices* through an integrated program that reduces the likelihood that problems will arise, and that rapidly handles problems that are discovered. If implemented prior to criminal conduct or an incident that results in some civil exposure, compliance programs may be a useful tool in convincing prosecutors (or a jury) that the company and its Management took all reasonable steps to prevent illegal or negligent conduct. *If a company is convicted of a crime or found guilty of negligence, the absence of a compliance program grounded in working policies and procedures virtually guarantees serious problems at sentencing or a larger jury verdict.* Therefore, the viability and effectiveness of policies and procedures can best be measured by how well these would fare when the government makes decisions about how it would handle violations.

The solutions therefore require the following:

1. A written corporate policy that addresses compliance with all applicable laws.

- a. *Write policies and procedures so they are effective communications.* Avoid technical and legal language whenever possible.
 - b. *Make sure policy is workable and addresses various scenarios.* Have you successfully budgeted for expenditures? Do you have a system for monitoring proposed regulatory changes? Do you handle compliance with new and changing regulations with a logical, systematic process?
 - c. *Publicize the policy.* Ensure that it is sanctioned by senior Management.
 - d. *Explain the policy to the people who must make it work.* No matter how clear it is, some people will not read it or will claim not to understand it. Explain, train, and make records of training.
2. *Delegation of responsibility* for compliance to trained individuals, whose performance review includes this responsibility.
 3. *Endorsement of compliance policies* by the highest levels of Management and communication of policies throughout the company, demonstrating strong institutional policy to comply with requirements.
 4. *Audits* to measure compliance and effectiveness of systems, done with protections to avoid having the audit become a problem rather than a useful tool.
 5. *Procedures for identifying potential problems, reporting* them to the appropriate persons to correct them, and tracking issues to resolution, including a *reporting system* for employees to report criminal conduct by others within the organization without fear of retribution.
 7. *Commitment of adequate resources* for compliance, including a program to train employees.
 8. Procedures for keeping the company aware of *changes in regulations and trends in the law.*
 9. *Records retention programs* (complying with applicable records maintenance requirements) showing that the company has acted thoroughly and promptly to assure compliance.

10. The company taking *prompt corrective actions* to address identified problems.

Security Policy

As new standards have developed, multiple organizations/agencies have sifted through the myriad of documents from government agencies and other sources to assist integrators, applications providers and end users with achieving compliance and addressing security, while maintaining operational efficiency. One of these agencies is Sandia National Laboratories. The following (included with Sandia's approval) represents their latest concerning Security Policy:

Framework for SCADA Security Policy

Dominique Kilman Jason Stamp
 dkilman@sandia.gov jestamp@sandia.gov
 Sandia National Laboratories
 Albuquerque, NM 87185-0785

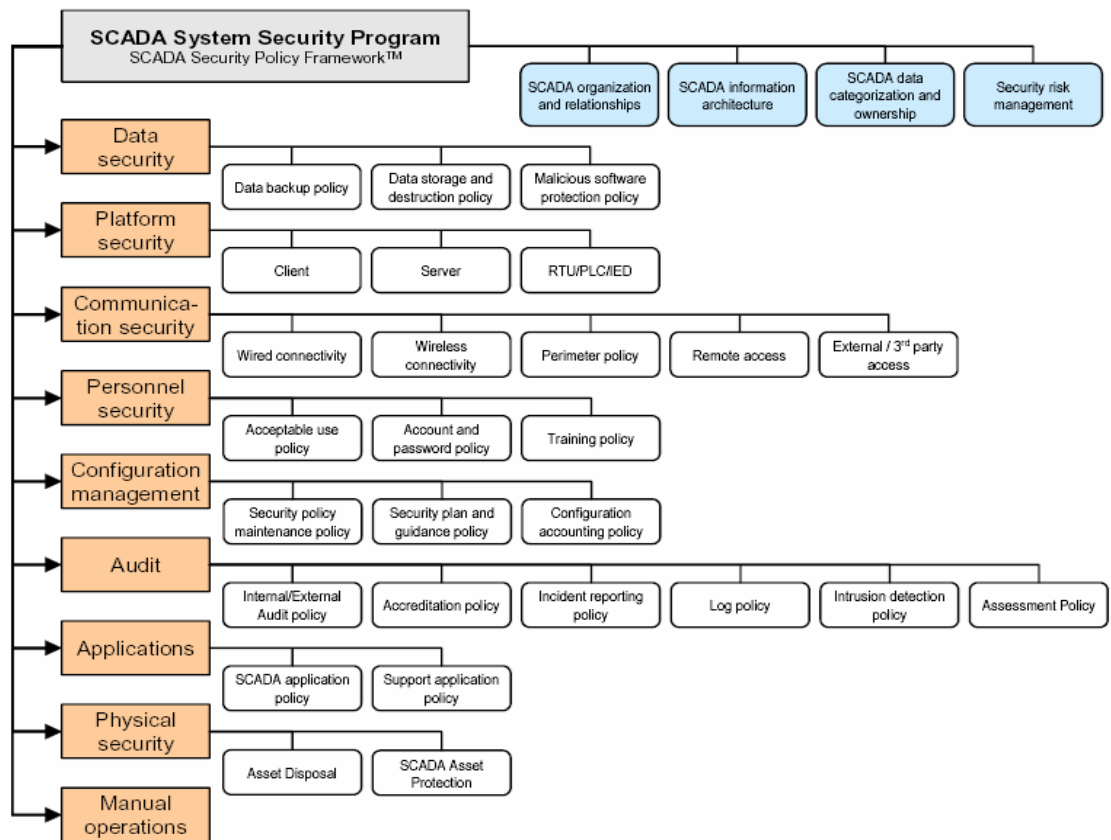


Figure 1. SCADA policy framework.

Copyright © 2005, Sandia Corporation.
 The submitted manuscript has been authored by a contractor of the U.S. Government under contract No. DE-AC04-94AL85000. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes. Unlimited release – approved for public release.
 Sandia National Laboratories report SAND2005-1002C.
 Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.



Sandia incorporated information from some or all of the following sources:

American Petroleum Institute (API),
Industrial Automation Open Networking Association (IAONA)
International Electrotechnical Commission (IEC)
Institute of Electrical and Electronics Engineers (IEEE)
Instrumentation, Systems and Automation Society (ISA)
North American Electric Reliability Counsel (NERC)
American Gas Association (AGA)

Conclusion

The approach to SCADA Integration must be expanded to include Operations, Security and Compliance. Taking this holistic approach will help maximize operational efficiency, maintain a secure operating environment and minimize the risk regulatory scrutiny and/or action while achieving business objectives.