# Framework for SCADA Security Policy

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

***Abstract* – Modern automation systems used in infrastructure (including Supervisory Control and Data Acquisition, or SCADA) have myriad security vulnerabilities. Many of these relate directly to inadequate security administration, which precludes truly effective and sustainable security. Adequate security management mandates a clear administrative structure and enforcement hierarchy. The security policy is the root document, with sections covering purpose, scope, positions, responsibilities, references, revision history, enforcement, and exceptions for various subjects relevant for system security. It covers topics including the overall security risk management program, data security, platforms, communications, personnel, configuration management, auditing/assessment, computer applications, physical security, and manual operations. This article introduces an effective framework for SCADA security policy.**

***Index Terms* – SCADA systems, policy, administrative control, security administration.**

## 1. SCADA Management Controls

SCADA systems support our critical infrastructures such as electrical power generation, transmission and distribution, oil & gas transport, and water supplies. The primary purpose of SCADA systems is to monitor and control infrastructure equipment. The Sandia interpretation of the terms PCS and SCADA include the overall collection of control systems that measure, report, and change the process. Essentially, any subsystem that electronically measures state, alters process control parameters, presents/stores/communicates data, or the management thereof is subsumed in our definition of SCADA.

One of the most common problems seen in modern SCADA environments is the lack of a SCADA-specific security policy. Other vulnerabilities include poor account maintenance, insecure network connections, and a lack of maintenance and monitoring of equipment. See [1] for an in-depth discussion of observed vulnerabilities.





### 1.1. SCADA-Specific Security Administration

SCADA systems need a separate, SCADA specific security administration structure to ensure that all the specialized features, needs, and implementation idiosyncrasies of the SCADA system are adequately covered. [2] contains a table which lists the key differences in IT and SCADA system designs which can affect security and policy decisions.

Acceptable use of SCADA should be narrower than IT systems due to its different mission, sensitivity of data, and heightened criticality. SCADA systems are oftentimes used to control time-critical functions. When time is an important factor, some standard IT security practices may not be appropriate for SCADA. For example, since anti-virus scanning can sometimes slow down a system, these may not be acceptable for some SCADA platforms. Therefore, the blanket recommendation in IT policy to include anti-virus scanning on every machine would not be appropriate for SCADA.

The mission in these automation systems may have safety-critical tasks which would preclude any significant downtime. While an IT system can at times allow downtime of hours, an electrical power plant cannot tolerate important safety functionality being lost for any period of time during operation. Also, since automation systems have more immediate physical consequences, interconnections between SCADA systems and external networks must be better controlled, and access must be more strictly enforced and monitored

Immediate adoption of security patches that are essential in IT may be impractical in SCADA. At times, vendor contracts preclude SCADA systems from installing patches that have not been approved and vetted by the vendor. Also, the possibility of a patch disrupting critical functionality is not tolerated in a SCADA system.

Finally, the data produced by a SCADA system may have different sensitivity than the data generated in the business side of the operation. SCADA data also has a different lifetime, so some SCADA data may only need protection for several minutes as opposed to days/months/years for personnel data residing on a business network.

Administration and enforcement is simpler with a separate policy. Trying to tailor a traditional IT policy to include SCADA may seem like a time saving effort, but in reality it is probably not. Trying to capture all the caveats needed for SCADA could be counterproductive and may produce a document which is not easily understandable. The resulting policy will often be so convoluted, watered

down, inaccurate and vague that it is difficult to know what is and is not allowed. Since SCADA systems also have a small audience (including SCADA engineers, technicians, operators, and administrative personnel), the detail of the policy sections can be more precisely targeted. Finally, legislative requirements on automation systems are different than other IT systems.

### 1.2. Enforcement Hierarchy

Policy is the cornerstone of any sustainable security system. Systems without security policy and administration do not possess measurable, self-perpetuating security, and experience has shown that every ungoverned information network will eventually sprout vulnerabilities.

Business objectives are also a driving factor of policy. As a business, environments that use SCADA need to identify confidentiality, availability, and integrity requirements for the SCADA network and the data available from the SCADA system. These requirements will drive policy statements.

Risk assessment drives policy by identifying where the system is vulnerable to attack. The risk assessment process involves evaluation, reduction, transference, and mitigation. Security policy addresses the reduction, transference, and acceptance steps. Policy also details when, who, and how evaluations will be performed.

A defined policy is the first step in creating a security program which is self-sustaining and enforceable. Once a policy has been created, other specific security documents (including system security plans and implementation guidance) can be created to define the particular practices to be used within the SCADA environment.

## 2. Security Policy Concepts

SCADA security policy can be defined as follows:

> "Security policy for SCADA administration translates the desired security and reliability control objectives for the overall business into enforceable direction and behavior for the staff to ensure secure SCADA design, implementation, and operation." [3]

### 1.3. Policy Introduction and Background

A security policy is a formal statement of what will and will not be done by persons and systems within an organization. The policy statements are derived from business goals and risk assessments. Policy statements are rules – not suggestions or guidelines that users choose to follow. As rules, they require clear and consistent enforcement. Users must observe the mandatory rules within a company. Without consistency, it is very difficult to punish infractions.

Policy must be vendor- and manufacturer-independent. As technologies change and new acquisitions occur, the policy must remain effective. When vendor- or technology-specific statements are used, the maintenance burden for the policy increases. Then, the policy must be changed any time there is a new purchase or an advance in technology. If the policy is not updated, the policies themselves become obsolete, which is not an acceptable situation.

Security policies do not include configuration rules, system setup guidelines, or specific security settings. These elements are important in any sustainable security program, but policy is not the proper place for this type of information. Security plans and implementation guidance is where these should go.

### 1.4. Important Policy Sections

A well written policy document must follow an easy-to-read and easily understandable format. Each policy will include:

*Purpose:* The purpose section explains why this policy section exists.
*Scope:* The scope specifies what is covered by the policy (for example, machines, people, and/or facilities).
*Policy:* These are the actual statements of the organization's rules on the topic – what can and cannot be done by people, equipment, etc.
*Responsibilities:* Who must do what in regards to this policy is specified here.
*References/Authorities:* Here, the policy is tied back to other policies that must be followed due to the organizational structure. Also, external references to the policy are cited (for example, legal requirements).
*Revision History:* This is a record of what changes were made, by whom, and when they were done.
*Enforcement:* This specifies the consequences of not following the policy. This may be general and apply to all policies (i.e. subject to disciplinary action up to and including termination) or they may be specific (immediate dismissal for knowingly and flagrantly disregarding a specific policy). Enforcement may also describe if legal action may be pursued.
*Exceptions:* Exceptions might not be needed, but if they exist, each must be documented in the policy. This includes how to get an exception, who can approve it, and were the documentation will be stored. Also, the details about how often the exception must be re-approved are described.

Some of the preceding sections must be included for every part of the security policy that is written, such as policy and scope. Others can be stated once and that statement will apply to all policies (enforcement is a good example). See [4] for more policy design basics.

## 3. SCADA Security Policy Framework™

The SCADA policy framework™ (Figure 1) has been developed to make it easier to create a SCADA security policy. Using a framework allows authors to apply a systematic approach that ensures that all critical topics have been adequately addressed by policy. The framework also compartmentalizes the policies, allowing multiple authors to work at the same time with little or no overlap. Less overlap means less work is required when changes must be made. Overlap can also lead to conflicting policy statements which reduces the effectiveness of the policy. Once

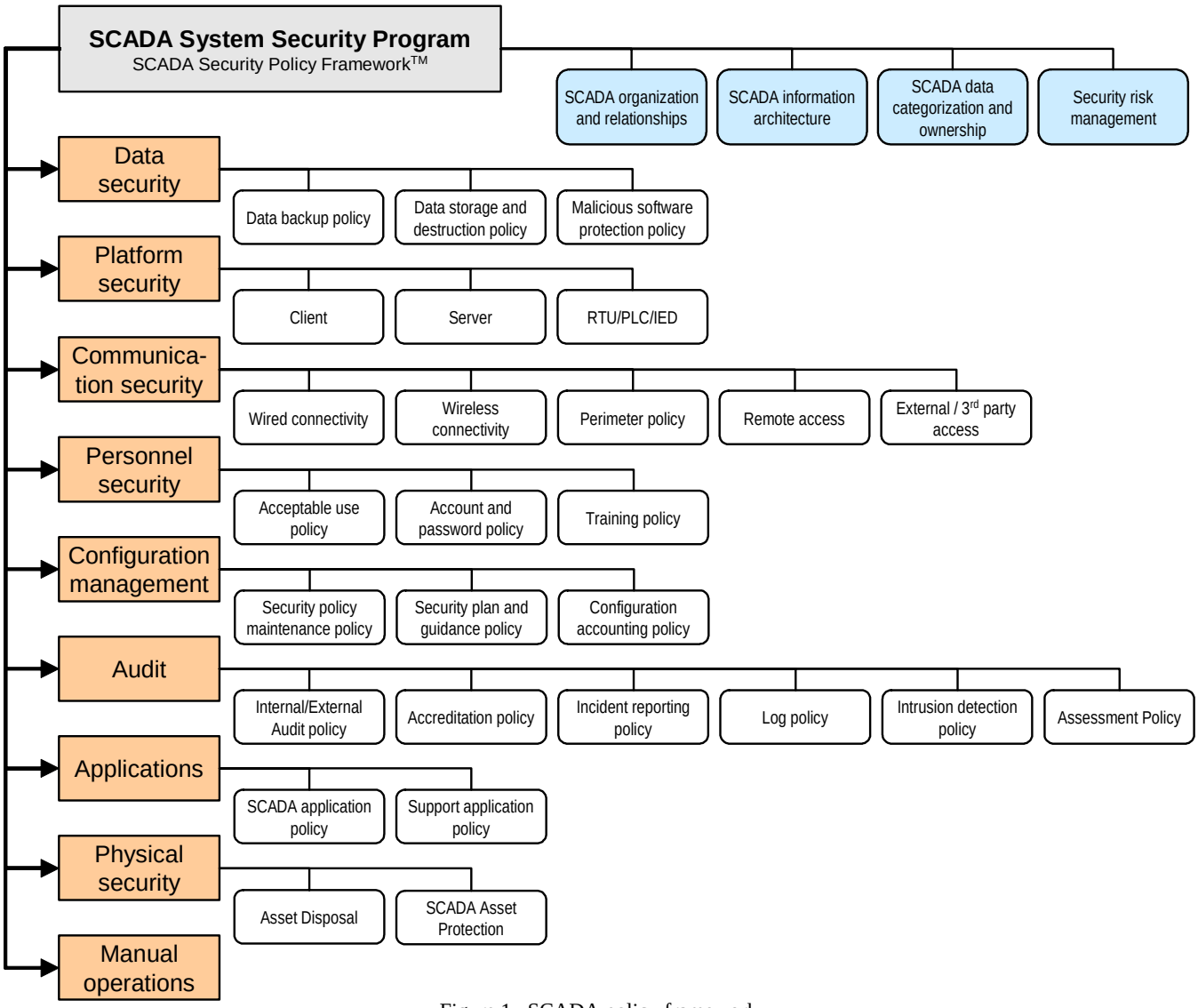


Figure 1. SCADA policy framework.

the format has been determined and critical policies identified, each policy can be written in isolation. If a particular policy section (i.e. wireless) does not apply to an organization, it can be truncated or eliminated. (However, if new technology or procedures are not adequately covered by the policy due to missing sections, they cannot be used until the required policies are in place.)

The framework as presented here is the result of multiple assessments of SCADA systems and our work to facilitate the creation of SCADA-specific policies. It has been through much iteration over several years and is still re-evaluated and refined periodically. The framework itself can be tailored to any organization. The hierarchical nature of the framework allows the policy document to adapt to each organization that uses it. Each box does not have to be a separate policy; some organizations will be able to cover every subsection in a policy area with one policy. Others may need the more distributed structure displayed in Figure 1 to adequately meet their needs.

The following sections provide details regarding what should be included within each portion of the policy framework.

### 1.5. SCADA Security Program

The first box in the policy framework serves as an introduction to the target system and provides context for the rest of the policy. The information contained in this group will rarely be policy statements, but they will provide important details and concepts that are necessary for the rest of the policy.

Step one in creating a policy structure is defining the SCADA system's operation. The criticality of the SCADA system to users and its relationship to other systems and operations must be well-defined.

#### *1.5.1. Organization and Relationships*

No SCADA system operates in isolation. Determining the organizational structure and relationships to outside entities is important when identifying which mandatory and optional policy standards written by other bodies must be

followed. For example, some water systems must adhere to the guidelines set forth by the EPA (and in many cases) DoD guidelines. NERC 1200 [5] specifies requirements for cyber security needed to by electric utilities for compliance with NERC.

The internal hierarchy of an organization is also vital to a well-developed security program. Roles and general responsibilities for individuals must be defined. This enables the assignment of responsibility in subsequent policy sections. Without any assignment of responsibility, policy implementation and enforcement will often be ignored.

*1.5.2. Information Architecture*

The SCADA information architecture will provide a common reference point for all readers of the policy. This section will define the system boundaries and equipment, identify common terminology, and any relevant engineering/performance standards. If the system is comprised of independent subsystems, each subsystem must be described in terms of its relationship to other parts.

*1.5.3. Data Categorization and Ownership*

The data contained, processed, created, and used by the system must be analyzed. Most systems will define classes of data in order to easily identify different types of data and identify the different protection and storage requirements for each category. Each data category should also have an assigned owner, who is the person ultimately responsible for the data and who will be answerable if data is mishandled. Examples of data types include configuration, historical/archived, current/live, administrative, etc.

*1.5.4. Risk Management*

All system security administration revolves around a risk management program. Risk management is the reason that policy will be created initially. It is also the driving factor behind security technology and implementation. The goal of all risk management programs is to create an acceptable level of risk, through identification, analysis, and reduction/transference. This level is distinct for every system. Risk, cost, and performance are trade-offs that must be negotiated. Risk assessment as a driving factor in policy creation has been discussed earlier.

1.6. Data Security Policy

The data security policy determines the treatment of the data categories defined in the Security Program. Different data categories may have distinct requirements for protection which should be specified in this policy. All forms of data (be they paper, digital, video, etc.) must be protected commensurate with their criticality to the system. Data marking and need-to-know controls are important considerations.

*1.6.1. Data Backup Policy*

This policy will define all of the details concerning what data must be backed up, how often, and where the backups will be stored. The retention schedule for the backups will also be identified. If there are classes of devices which will be exempt from backup requirements, they must be identified.

*1.6.2. Data Storage and Destruction Policy*

Data must be protected during its complete lifecycle, including creation, storage, and destruction. Destruction is as important as creation and storage, and it is often an adversary's easiest means of data theft.

*1.6.3. Malicious Software Protection Policy*

Malicious code can cause irreparable harm to any computer system by either stealing or destroying data. Controls must be set forth which prevent the inadvertent or intentional installation of any malicious code.

1.7. Platform Security Policy

Platform security will identify secure configuration defaults that are required within the SCADA system. The procedures for account creation and termination are specified. Clients, servers, and SCADA devices (RTU/PLC/IED) will each have a separate set of rules which govern what entails a secure configuration. Important concepts such as virus checking, intrusion detection, access control, and encryption must be addressed. The process for acquiring exceptions to this policy is necessary due to the differing capabilities of machines.

1.8. Communication Security Policy

Communication security identifies the paths which data will take through a network, details protection mechanisms for different network segments, identifies security zones, and specifies external connection permissions.

*1.8.1. Wired Connectivity*

This section defines how to communicate within the wired portions of the automation network, including all parts of its LAN, MAN, or WAN segments. Cryptographic requirements are specified based on data categorizations.

*1.8.2. Wireless Connectivity*

Wireless connections to a network will need to have special consideration due to the broadcast nature of the medium. This section should designate what type(s) of data may traverse the wireless network, and how connections to the network will be established. Also, the acceptable configurations for wireless connections to the wired network are specified. Schedules and responsibilities for wireless coverage assessments will be here.

*1.8.3. Perimeter Policy*

This policy specifies how data is input and output from the SCADA system with other networks. The types of controls needed and the location of these controls will be identified. Security zones will be specified which will help to determine the cryptographic controls needed.

*1.8.4. Remote Access*

Here is defined if and how users can connect to the automation system from remote locations. Remote access is often a requirement in geographically large installations to effectively maintain the system. Vendors also use remote access for off-site maintenance and product upgrades. This policy details how to request access, who approves the access, and any time restrictions for the access.

Once the acceptable uses for remote access have been defined, the security controls needed for access control must be specified. The minimum requirements for the equipment performance will also be specified in this policy.

*1.8.5. External/3rd party connections*

This section specifies if, when, and how outsiders will access information and equipment on the automation network. This policy details how to request access, who approves the access, and any time restrictions for the access.

The monitoring and logging requirements will be stipulated, as well as prohibited actions. If there are time, equipment, or other requirements, these will also be enumerated.

1.9. Personnel Security Policy

Workers on the automation network will have different functions and security needs compared to others on the conventional IT network. This policy will express the job requirements and hiring policy for SCADA staff. These requirements may include citizenship and educational requirements, background investigations, and clearance needs.

*1.9.1. Acceptable Use*

This policy defines what users can and cannot do with equipment and network resources. Due to the criticality of the SCADA system, personal use should not be allowed on this equipment. Software on the SCADA system should be SCADA-specific. Any access to other networks, network monitoring, and a statement detailing what the SCADA system entails must be stated here. A 'rules of behavior' document should be created which every employ is required to read and sign.

*1.9.2. Accounts and Passwords*

The account and password policy will describe proper care of passwords and accounts including storage, creation, and sharing. Some policies will give minimum requirements concerning the format for passwords, while other will simply state that the current best practice must be used. Any shared passwords (for example admin passwords on equipment) will have special protections regarding creation, storage, and change requirements.

Account creation and destruction policies will explain how users may use their accounts, and who is responsible for creating and removing accounts. Account creation must be individual for accountability purposes and based on job function. Any additional protection requirements such as screen locks, time-outs, or login limits will also appear here.

*1.9.3. Training*

Staff must be familiar with the security needs of the system and understand why the security controls are in place. When staff understands why they do something, they are less likely to circumvent the protections. This policy will list what training is required, the frequency of training, and who must be trained. If specialized training is required for certain staff positions, those requirements must be listed here. Contractors should receive training commensurate with permanent staff training.

1.10. Configuration Management Policy

The configuration management policy ensures that a sustainable configuration management process is implemented. The policy will list the necessary documentation and processes needed for a sustainable security system. The details regarding revision process and timelines for security plans, policies, and implementation guidance must be expressed, as well as elements of change control and change evaluation (including patching).

1.11. Audit Policy

Both audits and assessments are important for a system. An audit will determine if the protections which are detailed in policy, security plans, and implementation guides are being correctly put into practice on the system. Assessments are performed on systems to ensure that the protections on the system are adequate for the information and functionality.

The audit policy defines the scope of auditing and assessment activities. The individual who is responsible for scheduling and reviewing audits must be identified. Schedules for projected audits are delineated.

*1.11.1. Internal/External Audit*

Both internal and external audits have an important place in a comprehensive risk management program. This section will give the details of each type of audit as well as identifying the internal organization responsible for performing, or contracting for, the required audits.

*1.11.2. Accreditation*

If an organization must be accredited, this section of the policy will give the details of the responsible parties, timelines, and participating entities.

*1.11.3. Incident Reporting*

The individuals who are responsible in the event of an incident will be identified here. If there is a chain of reporting that must be followed, those details must be captured here. The protection level of the incident details are defined so the results and reports will be protected at the appropriate level. An incident response procedure must be developed to address issues of evidence preservation, investigation authority, reporting requirements, etc.

*1.11.4. Logging*

This policy will define the logging requirements such as what will be logged, storage requirements, and revision requirements.

*1.11.5. Intrusion Detection*

Intrusion detection is an important tool for detection of anomalous behavior. SCADA operations will require specific policies regarding its requirements and limitations for IDS.

*1.11.6. Assessment*

The assessment portion of this policy will specify the responsible parties, timelines, and data protection for assessments performed upon the system.

### 1.12. Application Policy

The application policy ensures that applications are configured and used in a manner commensurate with the security needs of the automation system. This policy will cover the details of program-level access control, application training, as well as test and development requirements.

#### *1.12.1. SCADA Applications*

SCADA specific application will at times have requirements for administrator access. These applications may also allow data separation, separate user logins, and password protections. This section will focus only on those applications which are written to interface with SCADA devices and functionality.

#### *1.12.2. Support Applications*

Support applications such as office software, databases, and logging will need to have a different set of security guidelines. The applications usually do not interface directly with SCADA equipment and automation functions, but may reside on the same computers or networks where SCADA applications are running.

### 1.13. Physical Security Policy

It is impractical to separate the physical protection of the SCADA system from the cyber protections. Often cyber protections become more effective with the addition of physical protections. The equipment used by the SCADA system must be protected from physical damage, unauthorized access, or destruction. Access to any equipment by visitors and personnel must be controlled and monitored.

#### *1.13.1. Asset Disposal*

Physical asset disposal can be just as critical as data disposal. Physical equipment must be sanitized before it can be released from the control of the system. This policy will express the guidelines and requirements for users who have physical assets that are no longer necessary for the system operation. Important concepts are sanitization, tracking, and disposal technology.

#### *1.13.2. SCADA Asset Protection*

SCADA equipment will have different requirements than the standard office equipment used in the system. The differing characteristics of this equipment demand a separate statement of protection guidelines.

### 1.14. Manual Operations Policy

Due to the critical nature of automation systems, the functions of the automation system must still be performed even in the event of system failure. Important considerations for a manual operations policy include: manual backup procedures, chain of command, periodic inspection, training in manual operations, tests and drills on manual operation procedures, and a disaster recovery policy.

## 4. CONCLUSION

The Security Policy Framework™ developed at Sandia National Laboratories is a valuable tool in developing SCADA policies. The framework ensures coverage over all critical areas of security as well as flexibility in developing customized policies for specific SCADA operations.

## ACRONYMS

DoD ..... Department of Defense
EPA ..... Environmental Protection Agency
IED ……. Intelligent electronic device
IT ..... Information technology
LAN..... Local area network
MAN ..... Metropolitan area network
PCS..... Process control system
PLC ..... Programmable logic controller
RTU..... Remote terminal unit
SCADA ..... Supervisory control and data acquisition
WAN ..... Wide area network

## REFERENCES

[1] *Common Vulnerabilities in Critical Infrastructure Control Systems*, Jason Stamp, John Dillinger, William Young, and Jennifer DePoy, Sandia National Laboratories report SAND2003-1772C, Albuquerque, New Mexico (2003).

[2] *Integrating Security into SCADA Solutions*, Bernie Robertson, PA Consulting Group, NISCC SCADA Security Conference (2003).

[3] *Sustainable Security for Infrastructure SCADA*, Jason Stamp, Phil Campbell, Jennifer DePoy, John Dillinger, and William Young, Sandia National Laboratories report SAND2003-4670C, Albuquerque, New Mexico (2003).

[4] *A Short Primer for Developing Security Policies*, Michele D. Guel, SANS Institute (2001).

[5] *Urgent Action Standard 1200*, North American Electric Reliability Council (NERC) (2003).