SANDIA REPORT
SAND2007-2070P
Unlimited Release
September 2007

Security Metrics for Process Control Systems

Annie McIntyre, Blair Becker, Ron Halbgewachs

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2007-2070P
Unlimited Release
September 2007

Security Metrics for Process Control Systems

Annie McIntyre
Energy Systems Analysis

Blair Becker
Cryptography & Information System Surety

Ron Halbgewachs
Effects-Based Studies

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1108

Abstract

This document describes the foundations of metrics, discusses application of these metrics to control system environments, introduces a metrics taxonomy, and suggests usage of metrics to achieve operational excellence.

The security metrics work package began as part of the overall National SCADA Test Bed Program to address the applicability of security metrics to control system and operational environments. One of the four fundamental goals delineated within the *Roadmap to Secure Control Systems in the Energy Sector (2005)* is the development of the capability to measure and assess security posture. This metrics team was tasked to develop an approach to security metrics as they pertain to control systems, including development of a metrics taxonomy and guidelines for using metrics. This approach is targeted at the organizational level for an audience of asset owners and control systems management.

Acknowledgements

The author would like to acknowledge that the work that produced the results presented in this paper was funded by the U.S. Department of Energy/Office of Electricity Delivery and Energy Reliability (DOE/OE) as part of the National SCADA Test Bed (NSTB) Program.

Executive Summary

This document describes the foundations of metrics, discusses application of these metrics to control system environments, introduces a metrics taxonomy, and suggests usage of metrics to achieve operational excellence.

The increasing need to protect national critical infrastructure has led to the evolving use of security metrics to assist asset owners in creating inherently secure operating environments. Asset owners seek to protect their environment and critical assets while ensuring that operational objectives are met. Approaching security layer by layer and in an operational context can make securing a control systems environment less complicated. This approach can also assist in reducing complexities that surround control systems such as legacy issues, upgrades, connectivity, and accessibility.

The security metrics work package began as part of the overall National SCADA Test Bed Program to address the applicability of security metrics to control system and operational environments. One of the four fundamental goals delineated within the *Roadmap to Secure Control Systems in the Energy Sector (2005)* is the development of the capability to measure and assess security posture. This metrics team was tasked to develop an approach to security metrics, as they pertain to control systems, including development of a metrics taxonomy and guidelines for using metrics. This approach is targeted toward the organizational level for an audience of asset owners and control systems management.

– This page intentionally left blank –

Table of Contents

Table of Figures

1 Introduction

The increasing need to protect national critical infrastructure has led to the evolving use of security metrics to assist asset owners in creating inherently secure operating environments. Asset owners seek to protect their environment and critical assets while ensuring that operational objectives are met. Large-scale, all-encompassing approaches to security can be daunting to an asset owner with numerous priorities and limited budgets. Approaching security layer by layer and in an operational context can make securing a control systems environment easier. This approach can also assist in reducing complexities that surround control systems such as legacy issues, upgrades, connectivity, and accessibility.

This security metrics project team, as part of the National SCADA Test Bed (NSTB) Program, was tasked to develop an approach to security metrics as they pertain to control systems. The developed approach includes a metrics taxonomy and guidelines for using metrics. This project is divided into three major areas:

1. Identification and documentation of existing security metrics and relevant attributes of these metrics
2. Development of a security metrics taxonomy
3. Analysis of the applicability of existing metrics to the measurement of compliance with best practices and security guidelines

This document describes the foundations of metrics, discusses application of these metrics to control system environments, introduces a metrics taxonomy, and suggests usage of metrics to achieve operational excellence.

1.1 Background

1.1.1 Description

The "Security Metrics for Control Systems" Work Package was created to address the need for metrics outlined in the *Roadmap to Secure Control Systems in the Energy Sector* [1]. Components of the work package included research on applicability of metrics to control systems, developing a metrics taxonomy, and addressing the use of metrics to benchmark control systems security.

1.1.2 Historical Information

The security metrics work package began as part of the overall National SCADA Test Bed Program to address the applicability of security metrics to control system and operational environments.

1.1.3 Significance

One of the four fundamental goals delineated within the Roadmap [1] is the development of the capability to measure and assess security posture. The roadmap states that reliable and widely-accepted security metrics are needed to enable security posture measurements; the expressed need is for "Common metrics available for benchmarking security posture".

1.1.4 Literature Review

In a number of instances, documents, reports, and reference articles have attempted to utilize Information Technology (IT) security requirements to address control system security. In a similar manner, metrics identified in such approaches have focused on the concerns of IT security. In both instances, the results have been determined unsatisfactory for control system security. Over the past few years, an emphasis has been placed upon the definition of cyber security standards specifically for control systems. However, the necessary metrics definitions have not kept pace with these new standards and requirements.

Control system security standards and guidelines were reviewed to assist in selecting representative metrics to serve as building blocks within the taxonomy described in this report. There are now numerous documents available on control system security. However, many of these documents are still in draft form or are in the process of being revised. Appendix E of the report on *Control System Security Standards Accomplishments and Impacts* [7], identifies the list and current status of these documents.

The team researched several standards and guidelines extensively, choosing several to assist in developing the deliverables. The taxonomy relies on three documents that were chosen because they provide a comprehensive view of the latest control system security requirements and best practices (two of the documents are in the final draft stage) [2], [3], [4]. In addition, two of these documents with extensive bibliographies/reference lists serve as suitable guides to more detailed documents, allowing the asset owner to determine the level of detail for a control system security plan. The documents have a fair amount of overlap.

An additional document that was researched, but not cited for the taxonomy, stated that in 2006 over 38 industry organizations and standards bodies were involved in control system security recommendations or standards, and all but two of them did not realize that anyone outside their industry was working on the same topic [5]. The large share of overlap among such documents indicates that some type of consensus has formed. The main difference among the three cited documents is in how requirements, standards, and guidelines, are grouped.

1.2 Purpose

1.2.1 Reason for investigation

Large-scale, all-encompassing approaches to security can be daunting to an asset owner with numerous priorities and limited budgets. Facilitating the ease of implementing standards creates inherently secure systems, improving the overall robustness of control system architectures. The utilization of metrics to implement standards and best practices is divided into approachable areas that meet operational goals.

1.2.2 Roadmap Challenges

Having the ability to measure and assess security posture is one of the four fundamental goals given in the *Roadmap to Secure Control Systems in the Energy Sector* [1].

1.2.3 Audience

The approach presented in this paper is targeted at the organizational level for an audience of asset owners and control systems management.

1.2.4 Desired Response

The final products of this project include the taxonomy, this report, and presentation to stakeholders as needed. For asset owners, this means there should be a way to measure and determine their current security posture and the improvements that will be attained upon implementation of standards for those control systems. It is anticipated asset owners will use these products to assist in arriving at a security plan that involves identification of critical areas within the architecture, the selection of applicable best practices, and the definition and application of relevant metrics in those areas.

1.3 Scope

1.3.1 Extent and Limits of Investigation

There are numerous documents available on control system security. We selected the three ([2], [3], [4]) that, we believe, best provide a comprehensive view of the latest control system security requirements and best practices. These three documents are the basis for the taxonomy presented in this report.

1.3.2 Goals

The overall project goal is to create a taxonomy that an owner/operator can utilize at his or her site to apply cyber security metrics in key operational areas.

1.3.3 Focus and Objectives

In developing the project goal, a careful selection of key project aspects was made to ensure several benefits to industry asset owners and stakeholders. Engaging industry early in the project to seek guidance on objectives led to the identification of several required aspects to the project. These included:

- Ongoing communication with industry
- Maintaining an operational focus and holistic approach
- Taking a flexible approach with a model and taxonomy that can mold to industry needs
- Creating a take-away taxonomy product for industry
- Building upon multiple standards and maintaining flexibility for new and evolving standards

Communication with industry and scoping of the work package indicated that stakeholders' use of actionable metrics could result in several key benefits. These include:

1. Improvement of overall security posture through increased knowledge, awareness, and control of the architecture and operational environment.
2. Providing situational awareness information, allowing stakeholders to understand their current state of security and what, if any, action is required.
3. Assistance in procurement decisions by providing information about what assets and control elements need protecting and what key attributes are required of the protective mechanism.
4. Application of resources effectively, providing knowledge of critical areas, functions, and requirements.
5. Definition and application of security controls, providing technical requirements for solutions and an understanding of *how* to best protect operating environments.
6. Risk reduction through knowledge leading to well-fit, customized security solutions.
7. Improvement of overall operational excellence by matching specific operational requirements with applicable, cost effective solutions.

2 Approach

The viability of metrics within the information technology community has been well accepted. This application of metrics is not, however, directly transferable to other sectors, such as critical infrastructure. To address the applicability and usage of metrics in oil, gas, and electric sectors, the project was divided into several steps. The results of each step served as a foundation for the remaining tasks.

First, the team assessed the viability of using security for control systems. This was completed through research and communication with industry. Determination of why metrics are or are not being used by asset owners was addressed in attempts to identify key barriers in application of metrics. Industry feedback was critical in this step.

Second, a metrics taxonomy was constructed. This taxonomy was structured to assist asset owners in applying metrics to specific areas of their operations with attempts to overcome some of the identified barriers. The taxonomy was constructed with operational objectives in mind and it identified operational areas or layers, which serves to break apart the security concept into manageable pieces. This taxonomy was built upon an operational model, detailed later in this paper. The taxonomy is designed to be a take-away guideline for the oil, gas, and electric industries to assist in applying metrics to their operational environments.

Third, with a taxonomy structure in place, analysis was performed that assessed the usage of security metrics to meet industry guidelines or recommended best practices. This analysis assessed the use of metrics for benchmarking security in a control systems environment, an idea already well accepted in information technology sectors. However, metrics that had been used in IT would not all directly apply to control systems and thus required a fresh approach. To complete this analysis common metrics suggested in existing guidelines were categorized and placed within the taxonomy. It was concluded that metrics could be a viable tool in applying security guidance and have the potential to provide asset owners with critical information required to secure their operations.

Throughout the research and analysis phases, key information sources were utilized. These included industry members, standards bodies, existing metrics research, commercial products, and research forums. As part of the research, other metrics activities were monitored and coordination among projects occurred where applicable.

The final products of this project include the taxonomy, this report, and presentation to stakeholders as needed.

3 Results and Discussion

3.1 Metrics Definitions

Determining application of metrics to control systems first requires a clear understanding of metrics and how they should be defined in the context of control system operations. Metrics are often thought of as basic measurements and in the case of security, they could be thought of as how well something is protected. This is, of course, a simplified description. However defined, metrics provide useful data that can be analyzed and utilized in technical, operational, and business decisions across the organization. In this discussion, metrics can be qualitative or quantitative, and can be considered as a measurement or reading resulting from an operating state or situation.

Metrics assist industry in meeting overall mission goals, such as continuity of operations, safety, reliability, and security. For the purposes of this paper, metrics are categorized into organizational, operational, and technical areas, as shown in Figure 1.

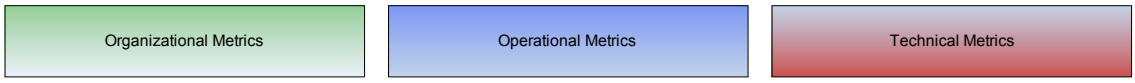


Figure 1. Categories of Metrics

3.1.1 Organizational Metrics

In this paper, organizational metrics apply to people and their interaction with each other and with critical functions. These metrics apply anywhere personnel exist in operations. Examples of organizational metrics include background checks, need-to-know rules, and vetted access control.

3.1.2 Operational Metrics

Operational metrics include aspects such as physical security, redundancy, and safe operating procedures that ensure secure functions. These are metrics associated with the everyday functionality of the site or architecture. Operational metrics might include activation of locked gates or perimeter guards.

3.1.3 Technical Metrics

Technical Metrics address technological areas that either require security or produce data used in security decisions. Technical metrics involve information at rest or in motion that contribute to the overall security of operations. For example, encryption levels between data from field site and the main office is viewed as a technical metric.

In many cases the lines between these categories are blurred, or possibly overlapped. For example, an organizational metric might include the requirement of badges for all employees. These badges may serve as access control for specific site areas, which might be counted as an operational metric. Finally, access control data is logged on a site-wide ingress/egress system, acting as a technical metric. While the exact classification of a metric is not required,

considering the three categories suggested above assists an asset owner in addressing all areas of operations without gaps.

3.2 Structuring Metrics

Applied metrics generally conform to a linear or pyramid structure. Figure 2 illustrates the structure, or components, of a metric. This structure can guide the asset owner in understanding how metrics are applied within an organization.

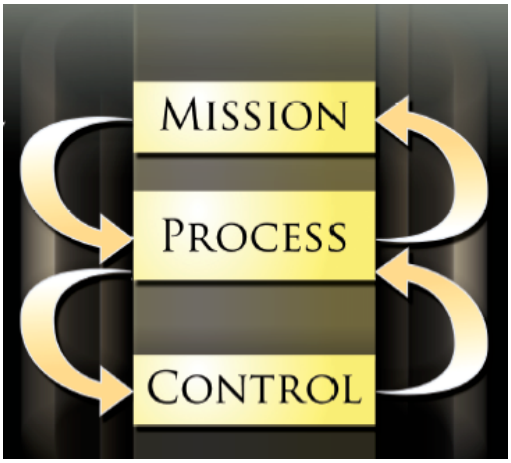


Figure 2. Metrics Structure

Structured into mission, process, and control, metrics can be seen as building blocks to achieve the organization's overall objective. Metrics can measure effects of security solutions, provide cost/benefit data, influence operational changes, and ultimately contribute to the success or accomplishment of mission. Each element is outlined below:

- **Mission -** Metrics should be used to ensure overall mission objectives, such as safety and continuity of operations.
- **Process -** A process assists in meeting these objectives, whether it is operational, technical, or a personnel function.
- **Control -** A control, a specific attribute with a measurable outcome, is put in place as part of the process. Multiple controls support a process and multiple processes achieve overall mission.

An illustration of how these elements work together can be seen in Figure 3.

In this example, we can see that a primary mission or objective of the organization is to maintain continuity of operations. Downtime has been deemed unacceptable to the organization and their customer base. To achieve this overall objective, one valuable process is that of maintaining data integrity. To ensure this process is achieved, several security controls are in place. Two such controls are mandated password expiration and minimum password length. This is one simple illustration of how metrics are applied within an operational set. In most cases, multiple controls support a process and multiple processes are required to achieve an overall mission objective.

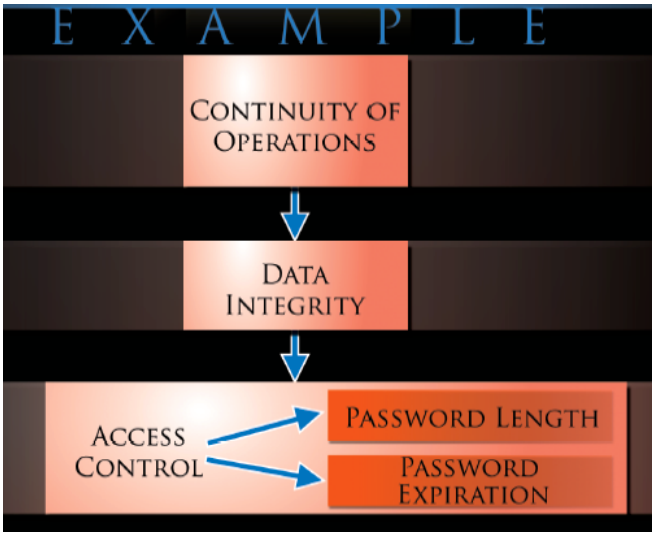


Figure 3. Structured Metrics Example

In addition to supporting overall objectives, many organizations choose to employ controls listed in standards, guidelines, or best practices. These metrics, in the circular pattern illustrated in Figure 2, contribute to the overall mission of the organization. The following is an example of how to employ a metric as part of a recommended security control.

> ***Example Best Practice:***
> Passwords should be at least 8 characters long and contain a mix of letters and numbers.
> ***Example Metric:***
> Do password requirements exist in the user domain that requires minimum length and character mix when passwords are created?
> ***Answer:***
> Yes, technical settings on the server impose these requirements on users when they create or change a password. All 100 users are subject to these requirements.
> **√ 100% Compliant with Best Practice**

3.3 Applicability of Metrics to Process Control Systems

Traditional use of metrics in business applications cannot be considered in control system environments. Metrics are regularly accepted and used in many organizations and sectors such as business, finance, communications, and technology. The use of metrics in information technology or information security aspects of an organization is commonplace. However, operational environments have an entirely different set of requirements and objectives. Primarily, downtime and halting of production are considered unacceptable. Critical infrastructure provides just that, a "critical" product or service. The consumer base depends on this infrastructure to be in place to continue important, everyday functions. Energy availability and reliability is a focus area and can cause serious effects, more so than if an IT system is down at a business or an email server is halted. Understanding the basic differences in objectives and mission between critical infrastructure using operational environments and traditional organizations with business systems is the first step towards

applying suitable metrics. Objectives for asset owners providing critical infrastructure center around availability and safety, both for the public and staff onsite.

Considering mission and objectives, it can then be concluded that traditional metrics used in information technology applications cannot be directly transferred to operational environments. When applying a new metric, especially through a new piece of software, an asset owner must consider all the potential effects including downtime, legacy systems, required resources, etc. Testing obtrusive metrics or tools in a laboratory environment is critical before application into a live environment. Ensuring that metrics applied in the correct areas with minimal or no resulting effect is of particular importance to the asset owner. Understanding potential consequences and the amount of research and planning required to use metrics and tools has often become a deterrent and the potential cost outweighed the benefit. Asset owners are understandably reluctant to use traditional metrics.

The successful use of metrics requires a focus on maintaining operational objectives and achieving mission. Use of metrics within an architecture or operational set must consider the criticality of specific assets, potential consequences, and value of the resulting data. Addressing an architecture by breaking apart specific aspects can assist an asset owner in applying beneficial metrics with minimal impact. Utilizing a metrics taxonomy, as described later in this paper, can assist with this activity and overcome certain barriers.

3.3.1 Barriers

Common barriers include the transition from traditional IT metrics to an operational environment. Cost, return on investment, and cost of implementation are just some of the common obstacles to employing metrics. Using an approach that addresses specific operational areas can break down cost and implementation issues into manageable tasks and provide a more focused approach to meet an organization's objectives for security. The basis for most decisions to employ metrics is often a matter of resources. Costs associated with new software and hardware tools and the staff time to make these implementations can be significant. This supports the decision to use metrics tailored to meet specific objectives.

In addition to immediate resources needed to implement metrics, resources are required to provide subsequent functions. For example, aggregation and analysis of data generated from metrics requires time or computing power. Likewise, interpretation of this data is required to make decisions that could include implementing a new security control, reconfiguration, or process changes to improve overall security posture. These security decisions could be made by a staff member or by an automated process. This process requires time and funding.

3.3.2 Benefits

Given the barriers and the metrics available, it can be said that if implemented correctly, the benefits of metrics outweigh the barriers or cost. Metrics are an integral component in building overall secure operations. The benefits of metrics in information technology environments are well documented and can facilitate day-to-day business while providing the basis for security decisions. From an operational standpoint, security can be mapped to availability and readiness. Significant research has been conducted on industry priorities and determining the relationship between vulnerability, technical consequence, and business impact [6]. Identification and mitigation of vulnerabilities reduces technical consequence and

subsequent business impacts. Metrics are crucial in determining critical areas of an architecture, valuable processes, points of failure, and attractive targets within an operational set. Metrics can be a tool to identify and reduce vulnerability as well as provide valuable data for security decisions. Both situational awareness and life-cycle planning play valuable roles in ensuring availability and safety through increased security.

The benefits of metrics, and even their necessity, have been realized by industry and government. As mentioned in the introduction, this metrics project maps directly to the Roadmap goal to *measure and assess security posture* [1]. The utilization of metrics and resulting data feeds directly to the goal of *developing and integrating protective measures*. A "selected priority" in the Roadmap lists the need to develop consensus on what serves as clear measurement of security posture. Industry recognizes the need for situational awareness and methods to identify vulnerabilities and protective mechanisms. An additional priority, to develop risk assessment tools that include frameworks for prioritizing control measures and cost justification of tools, is also supported by the employment of metrics in control system architectures .

3.3.3 Role of Standards

Industry guidelines and standards play an integral role in the implementation of metrics. The National SCADA Test Bed Standards Report [7] outlines the common industry standards and guidelines in use today. This metrics project utilizes standards and guidelines as examples of how to apply specific metrics. No one standard or best practice is recommended but rather it is suggested that an organization choose guidelines that best match their sector and operational environment. Metrics can then be derived from standards to build a better security posture.

There is a close relationship between metrics and standards as defined by industrial standards groups to be implemented by industry asset owners. Energy sector asset owners need a means of quantifying their success of attempting to meet security and operational goals. Many asset owners rely on standards as a starting place when evaluating their overall security posture. Depending upon the particular area of sector responsibility, some standards implementations might not be as effective as other implementations. Consider the differences between oil and gas pipelines compared to power lines or oil refineries compared to power generation stations. Standards are tailored to each industry just as measures of effectiveness must be. The industry owner must also determine the most rewarding security applications to be implemented based upon a limited amount of available funds. Through metrics, the effectiveness of implementation can be determined.

Standards are defined and developed to provide guidance in the steps to be taken by the industry asset owners in achieving the security necessary and expected, while metrics provide the measures to demonstrate the success attained in the implementation of the standards. Metrics provide an effective means of the evaluation of systems over a period of time as threat conditions change and new capabilities for protection are considered. Many of the standards now being defined that are specific to the security of control systems are still in the state of definition and approval. Accordingly, new vendor applications and enhancements to existing applications are being developed for use by asset owners. Now is the time that

metrics should be employed to provide the evidence of improved security through the implementation of these new standards should also be undergoing definition.

Implementations of new technologies by asset owners are not the only steps to be taken in making security improvements. Processes and changes in operations implemented by companies will also affect the overall security posture of a company. Standards for control systems within the energy sector are now providing definitions of expected management (organizational) responsibilities with respect to security and the processes of implementation and operational security responsibilities within an industry. Hence the need to consider different types of metrics that can be applied at different levels and different segments of the overall control of critical systems.

From a systems perspective, there should be traceability from the highest levels of standards definition and protection down to the lowest levels of actual implementation of elements to deliver the expected protection and security. Standards are usually defined at a fairly high level of requirement, leaving the specific steps of implementation to the organization responsible for assuring the standards have been achieved. Within each standard definition, there may be multiple steps of implementation (often referred to as specifications). At the lowest levels of implementation, stated specifications can often be measured in some units of capability or assurance of meeting the objectives expected by the standards. Metrics provide direct support traceability of operational needs to the control system security design effort.

3.4 A Metrics Taxonomy

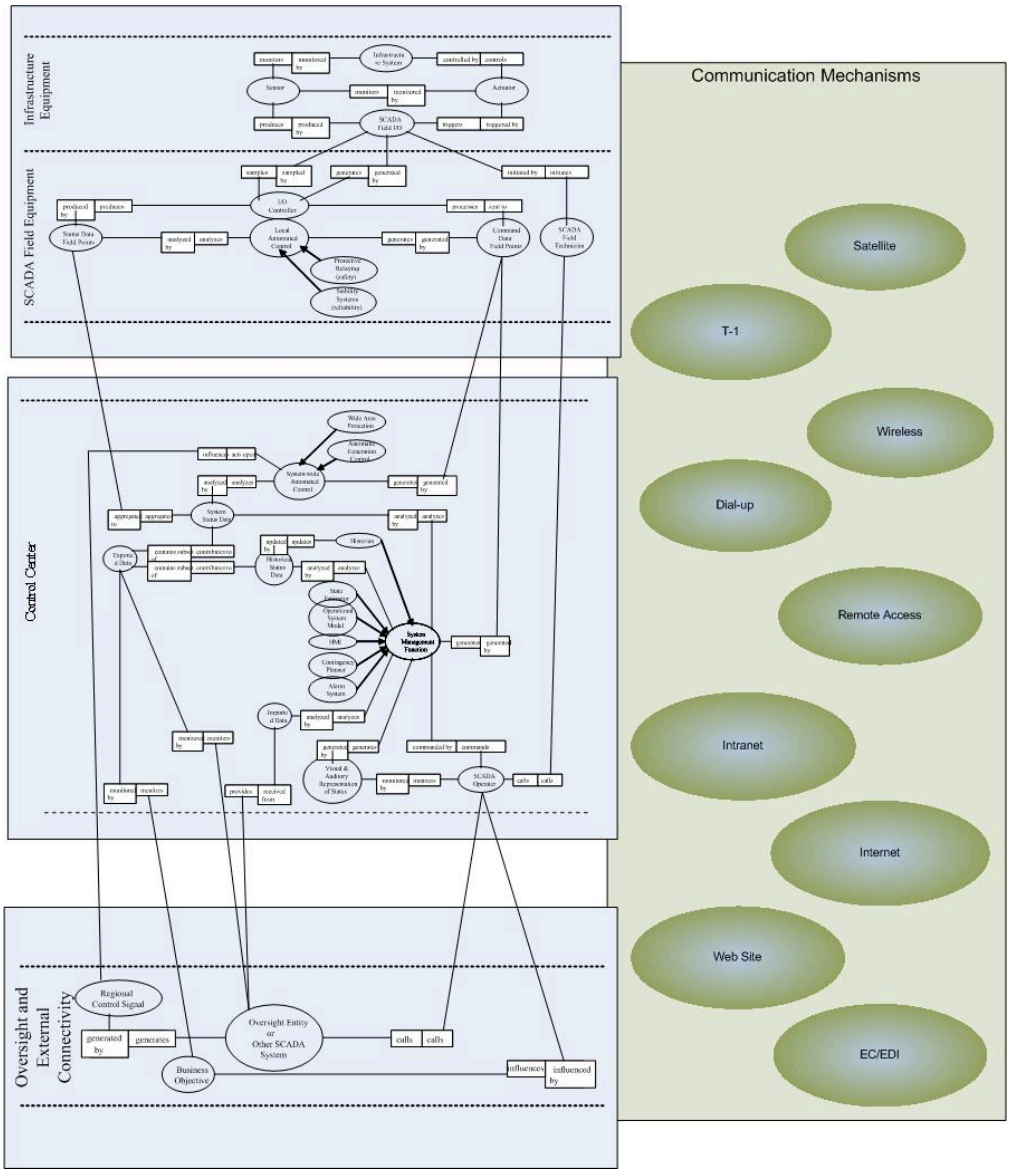
In this project, a metrics taxonomy was created that fostered the organization of security metrics as they relate to an operational environment. Metrics, organized by organizational, technical, and operational categories, were mapped to areas with specific operational missions. This model is based on operational objectives and mission, rather than standard information technology objectives. In this project, a taxonomy provides an approach for industry to understand why, where, and how metrics can be applied in their operations. Feedback from industry commonly echoes the need for flexibility and applicability to the specific architectures. A taxonomy with an operational focus means a flexible product that can bend to meet the individual asset owner's architectural needs. For this research and analysis, a generic operational model was applied as the baseline, or foundation, to assist in applying metrics for control systems. This baseline can then be modified to represent specific architectures that meet an asset owner's needs. The taxonomy provides a take-away map for industry for their immediate use. The interactive taxonomy document can be located at [Taxonomy Document]

3.4.1 Automation Systems Reference Model

The Automation Systems Reference Model (ASRM) [8], created at Sandia National Laboratories, has been vetted with industry and was selected to provide the foundational map for the taxonomy. This model has been slightly modified for this project to represent four functional areas that serve as a map. These areas represent logical, not necessarily physical connectivity. These areas are:

- Field and Infrastructure Equipment – sensors and field equipment that provide data for decision making
- Control Center – central site operations and processing
- External Connectivity – links to billing, business network, or strategic partners
- Communications – methods of moving data either inside or outside the organization

Figure 4 represents the ASRM and the foundation for the metrics taxonomy. This model was created to represent generic operations and can be tailored to a specific sector or site. A complete model can assist asset owners in determining the location of critical assets and processes that are required to meet overall objectives such as availability. This information is critical to selecting and applying security controls in the right locations within the architecture.



Adapted from the Automation Systems Reference Model by Jason Stamp and Michael Berg, Sandia National Laboratories

Figure 4. The Automation Systems Reference Model for the Metrics Taxonomy

3.4.2 Building the Taxonomy

The taxonomy relies on three documents chosen because they provide a comprehensive view of the latest control system security requirements and best practices as described in Section 1.1.4, *Literature Review*. Two of these documents have extensive bibliographies that serve as guides to more detailed documents, allowing an asset owner to determine the level of detail for a control system security plan.

The taxonomy groups categories for the purpose of delegating responsibilities. Organizational metrics more often involve someone in a managerial role, whereas technical metrics are usually addressed by technical staff. Operational metrics are a third group; however, they are represented as a "go-between" in the taxonomy for greater adaptability. Depending on an asset owner's particular situation, some organizational and technical metrics may fit better into an operational metrics group. Operational, organizational, and technical metrics can be applied in each area according to overall mission objectives.

3.4.3 Using the Taxonomy

The taxonomy can be used to help devise a control system security plan by locating specific areas to be considered, or to help refine an existing security plan by determining security levels based on metrics. This general taxonomy can adapt to meet an asset owner's specific needs. Because the ASRM represents a generic architecture, each organization can build on the design to meet their specific topology. The taxonomy is currently structured as an interactive file in portable document format (PDF). The taxonomy currently contains sample metrics from common industry standards to serve as an example of how metrics fit into each functional area of the architecture. Any standard or best practice could be applied in this structure. When determining how organizational, operational, or technical metrics fit within the architecture, an asset owner should consider:

- Overall mission objectives
- Key functions in each area
- Critical assets in each area
- Data and process integrity
- Human involvement in key processes
- Security controls already in place

A simple process can be employed, using the taxonomy as a tool in building inherently secure operations. A high-level breakdown of the process:

Step 1: Identify. Define your control system architecture and operational set.

Step 2: Delineate. Define your primary mission goals; include critical processes and overall business objectives.

Step 3: Select. Determine the guidelines, standards, or a set of best practices that best reflects your industry needs.

Step 4: Map. Determine and plan metrics associated with the best practices in each operational area, keeping in mind technical, operational, and organizational areas. Where does this apply in your architecture?

Step 5: Analyze. Evaluate operations based on the metrics. Do you feel your security level best meets your mission goals? How did you score in critical areas?

Step 6: Apply. Include changes or additions to the architecture, processes, or controls in place to ensure the security meets mission goals, but does not hinder operations or become cost prohibitive.

Figure 5 illustrates sample operational and technical metrics topics in each functional area. The metrics taxonomy maps metrics derived from representative standards into categories and by functional area. An organization can use this as a sample guide to map metrics to their most critical areas of the operational architecture. Typical standards or best practices fall into topic areas such as access control or logging. These areas help guide the asset owner in matching metrics to function, saving time to focus on application within their own specific architecture.

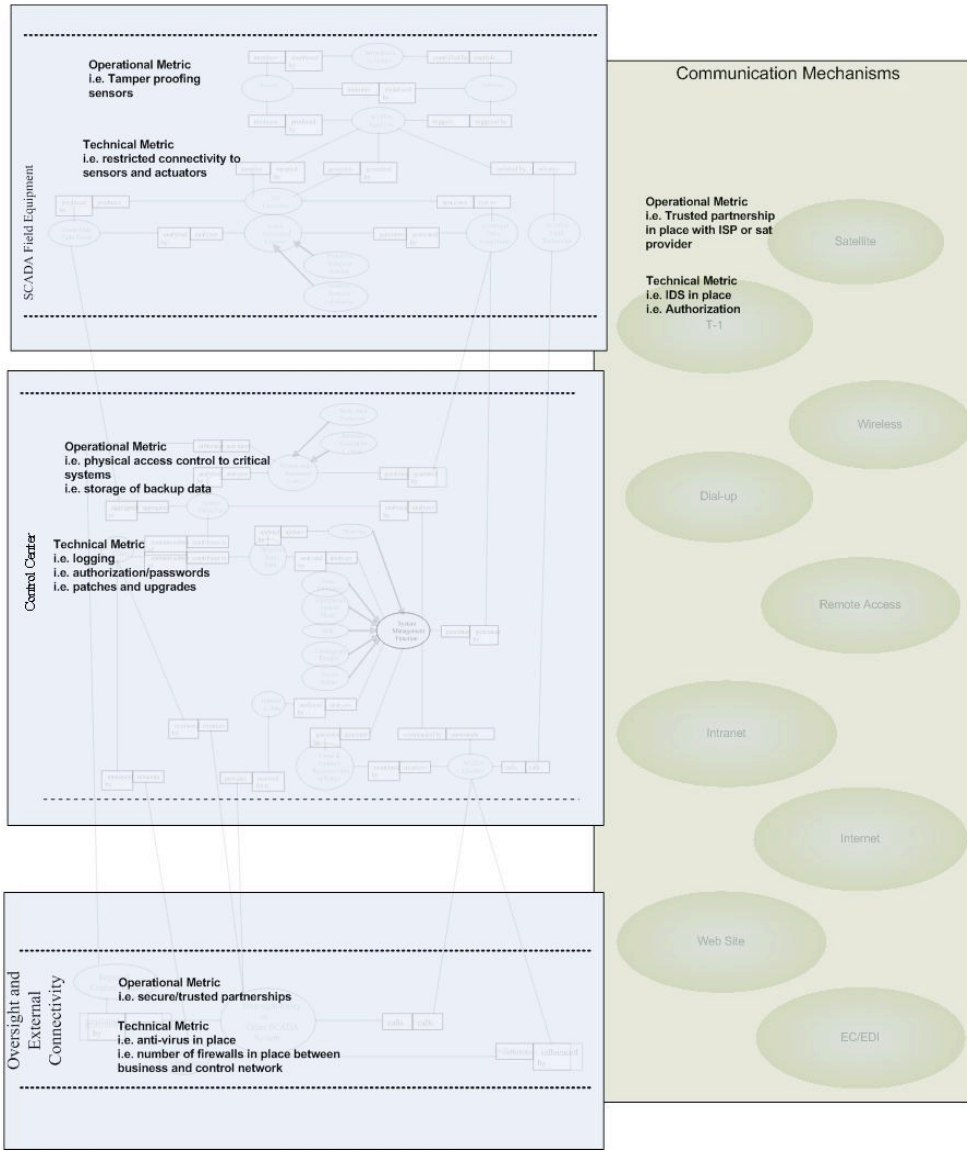


Figure 5 Sample Operational and Technical Metrics Topics

For an asset owner who has put little effort into control system security, the taxonomy provides an ideal starting point for implementing a control system security plan. Beginning with the first Organizational category, Security Policy/Implementation Framework, the user becomes aware of the need for a security policy and a management framework to implement a security program. Figure 6 represents the front, or start-up page of the metrics taxonomy. From there, by simply surveying the taxonomy categories, the user can gain a good overview of what is required for an effective security program. The grouping of the categories within the taxonomy can facilitate the delegation of tasks to begin implementing such a program. Figure 7 illustrates example metrics if an asset owner chooses “Access Control” under the Organizational category.

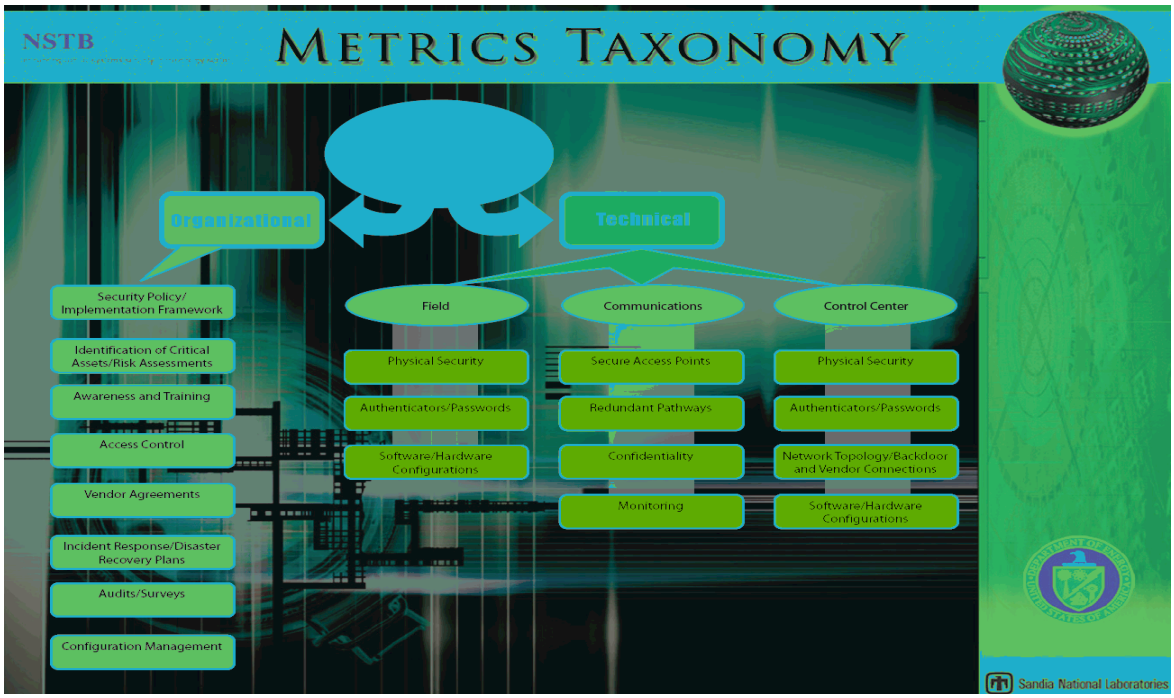


Figure 6. Metrics Taxonomy Front Page

Figure 7. Link from Access Control in Organizational Metrics Category

Refining an existing control system security plan by determining security levels based on metrics, an asset owner assigns various metrics to the taxonomy categories based on importance to the industry's mission. For example, the user may assign a scale of 0 or 1 for Vendor Agreements (1 if security agreements are in place, 0 if they are not) but assign a scale of 0 to 5 for Network Topology/Backdoor and Vendor Connections to assess the security status of firewalls, control system/enterprise network separation, etc. Once metrics have been

assigned to each category, an overall score can be calculated and mapped to various security levels. The user can then gauge whether to refine the existing security plan.

Mapping metrics to functional areas within an architecture can help break down the daunting task of securing operations at a site with a working topology and process set already in place. Determining priorities, identifying critical areas, and mapping appropriate metrics helps to focus security in the most needed areas. This allows for more cost-effective security decisions on applying new technology, redesigning and architecture, or implementing an add-on security control.

3.5 Application and Use of Metrics

One of the common findings from control system security research projects is the need to address security from an operational standpoint. Critical infrastructure environments require different technical and business objectives and have different resulting consequences than other environments that serve as corporate infrastructures. Recognizing these objectives and matching security with critical architectural areas are keys to achieving inherent security and operational excellence.

3.5.1 Operational Motivators

Operational goals typically include continuity and availability, safety, environmental compliance, public confidence, and optimized productivity. Considering current architecture designs, asset owners often recognize critical processes or assets that must function accordingly to ensure the operational goals are met. Other situational awareness and mapping tools are available to assist with this process, such as RiskMAP, developed under I3P [6]. These critical areas are excellent places to begin employing metrics. Utilizing the taxonomy to apply organizational, operational, and technical metrics in these areas can make meeting these goals more manageable. Asset owners may choose to derive metrics from guidelines most applicable to their operations. Recently more industry sector forums are making recommendations on standards or best practices to be followed. For example, the Pipeline Hazardous Materials Safety Administration requires a public awareness program based on an American Petroleum Institute (API) Standard 1164 [9]. It may become commonplace for public agencies to recommend specific industry best practices. The largest example of compliance in critical infrastructure over the past year is the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards and the movement of the bulk power sector towards mandated compliance [4].

3.5.2 Compliance vs. Security

While much discussion has surrounded industry standards and best practices, it can be said that such guidelines assist in applying security in control systems environments. These standards are much more applicable than guidelines development for use within IT environments. As is often discussed by industry, compliance with standards does not definitively provide security. Guidelines provide starting points but an approach to security must include consideration of operational goals and architecture design. Therefore each application of a best practice or standard should consider hardware, software, and communication design, along with overarching objectives such as availability. Although this can require additional staff time and resources, a level of specification or customization is needed to attain secure operations beyond standard compliance.

4 Conclusions

The use of metrics has recently received a great deal of attention from both government agencies and industry. We now recognize that IT metrics cannot be applied to control system architectures. Industry owners with control system architectures have different mission goals and metrics must be addressed from an operational perspective. As suggested in the Roadmap, well-defined metrics can reduce overall cyber consequence while being applied in a cost-effective manner that meets operational goals. A taxonomy assists asset owners in tailoring their needs and applying metrics to achieve their specific operational needs. The metrics taxonomy created in this project is a moldable model that is flexible for industry, rather than a rigid product that may not easily be employed. This metrics taxonomy is based on the Automation Systems Reference Model and it focuses on control systems security rather than IT security. A security plan that involves identification of critical areas within the architecture, the selection of applicable best practices, and the definition and application of relevant metrics in those areas will greatly assist in reaching secure operations.

5 Recommendations

Addressing metrics as part of the life cycle can be a cost-effective way to secure operations, making implementations and upgrades easier. Successfully employing metrics to implement controls across an architecture or operational base can create inherent security while maintaining overall business objectives. As asset owner/operator should consider the following steps in security overall operations:

- Identify operational objectives and motivators;
- Choose guidelines or standards that best fit their industry sector and overall operational goals;
- Utilize the metrics taxonomy to apply requirements and best practices to specific parts of the operational base and/or architecture;
- Ensure all aspects of operations are secure while objectives are met and business goals intact.

Appendix A: References

[1] U.S. Department of Energy and U.S. Department of Homeland Security, *Roadmap to Secure Control Systems in the Energy Sector,* January 2006.

[2] National Institute of Standards Computer Security Resource Center, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, NIST Draft Special Publication 800-82. 2006. http://csrc.nist.gov/publications/drafts.html

[3] U.S. Department of Homeland Security, *Catalog of Control System Security: Recommendations for Standards Developers*, awaiting release date.

[4] North American Electric Reliability Corporation, *NERC Standards CIP-002-1 through CIP-009-1*. 2005. http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

[5] Clark, Richard, *Wonderware Security Guidance Manual (Draft)*, Revision 1.0, Invensys, 2006.

[6] A. McIntyre, J. Stamp and A. Lanzone, *I3P Preliminary Risk Characterization Report*, I3P Research Report. May 2006.

[7] Halbgewachs, Ronald, *Control Systems Security Standards Accomplishments & Impacts,* NSTB Research Report, SAND2007-xxxx, September 2007.

[8] J. Stamp, M. Berg, and M. Baca, *Reference Model for Control in Automation Systems in Electrical Power*, 2005. SAND2005-6286P.

[9] American Petroleum Institute, "2007 Pipeline Conference Preliminary Program," 2007. http://www.api.org/meetings/topics/pipeline/upload/2007_Pipeline_Preliminary_Program-4.pdf

Appendix B: Acronyms

API	American Pipeline Institute
ASRM	Automation Systems Reference Model
CIP	Critical Infrastructure Protection
IT	Information Technology
NERC	North American Electric Reliability Corporation
NSTB	National SCADA Test Bed
PDF	Portable Document Format
SCADA	Supervisory Control and Data Acquisition

Appendix C: Outreach Activities

2006-2007 Activities:

- Attended the NSTB Standards meeting, La Jolla (June 2006)
- Circulated questionnaire (August 2006)
- Briefed John Tichotsky, Alaska Energy Consultant on Project Goals, Albuquerque (August 2006)
- Representative from API reviewed the Taxonomy and Project Approach, Albuquerque (Sept 2006)
- Representative from Western Refining reviewed the Taxonomy and Project Approach, El Paso (Sept 2006)
- Participation at the SANS SCADA Summit, Metrics Factsheet presented at NSTB booth, Las Vegas (Sept 2006)
- Discussed Taxonomy and Project Goals with Perry Pederson at a SANS breakout session (Sept 2006)
- Presented Peer Review Briefing, Washington (October 2006)
- Briefed UIUC on Taxonomy and Project Approach, Houston (Feb 2007)
- Presented Project Accomplishments and Goals at Process Control Systems Forum, Atlanta (March 2007)
- Request from industry members to obtain the Taxonomy and Final Report (March 2007)
- Briefed Alyeska representatives on NSTB and the Metrics Project Goals (March 2007)
- Brief NSTB Project as part of a presentation at the API Pipeline Conference, Albuquerque (April 2007)
- Advertise the Taxonomy and Factsheets at the booth at SPE Digital Energy Conference, Houston (April 2007)
- Circulate report for final comment (April 2007)

Appendix D: For More Information

Websites:

http://www.sandia.gov/scada

http://www.sandia.gov/scada/National_Testbed.htm

http://www.oe.energy.gov/randd/487.htm

Points of Contact:

Annie McIntyre
Sandia National Laboratories
505.284.0869

Blair Becker
Sandia National Laboratories
505.844.8877

Ron Halbgewachs
Sandia National Laboratories
505.844.8054