

NSTB

National SCADA Test Bed
enhancing control systems security in the energy sector

Security Metrics Taxonomy for Control Systems

Annie McIntyre
Ron Halbgewachs
Blair Becker
Bankim Tejani



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.

Table of Contents

- ◆ **Project Background, Objectives, and Approach**
- ◆ **Metrics as defined in this project**
- ◆ **Metrics from Standards and Best Practices**
- ◆ **Automated Systems Reference Model**
- ◆ **Taxonomy**
- ◆ **Operational use within PCS**
- ◆ **Summary**

Project Background

- 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. The document states that reliable and widely-accepted security metrics are needed to enable security posture measurements – need for “Common metrics available for benchmarking security posture”.
- The Security Metrics for Control Systems Work Package was created to address the needs outlined in the Energy Sector Roadmap. Objectives include research on applicability of metrics to control systems, developing a metrics taxonomy, and addressing the use of metrics to benchmark control systems security.
- 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.

Objectives

- **The Security Metrics for Control Systems Work Package objective is to benefit stakeholders by**
 - Engaging industry feedback
 - Maintaining an operational focus and holistic approach
 - Taking a flexible approach with a model and taxonomy that can mold to industry needs
 - Creating take-away taxonomy product for industry
 - Building upon multiple standards, and timely due to new and evolving standards
- **Meeting stakeholder's use of actionable metrics to**
 - Improve overall security posture
 - Provide situational awareness
 - Assist in procurement decisions
 - Apply resources effectively
 - Define and apply security controls
 - Reduce risk
 - Assist in improving overall operational excellence
- **Reduce cyber consequence and risk by providing situational awareness and allow the stakeholder to be proactive rather than reactive, identifying areas subject to risk.**

Approach

- **Assess the viability of using security metrics for control systems**
 - Determine why metrics are or aren't being employed. What are the barriers?
 - Develop an approach usable for industry, get industry feedback
- **Create a metrics taxonomy**
 - Create a take-away product for oil, gas, and electric industry.
 - Based a taxonomy upon operational areas and where metrics can be utilized.
 - Utilize and revise the ASRM
 - Define the metrics
- **Assess the usage of security metrics for measuring compliance with industry accepted standards and benchmarking security for control systems.**
 - Categorize common metrics in existing standards in areas within the model
 - Address where metrics should be applied, cross-referencing those areas with the standards families
 - Address the applicability of using metrics to measure compliance with various standards
- **Utilize Information sources:**
 - Industry members, Standards bodies, Existing research, Complementary program products, Industry forums
- **Coordination/Cross-pollination**
 - Monitor activities in the area of metrics, coordinate as applicable. These include academic efforts, industry and government projects and events, and other research and development activities.

What are Security Metrics?

Metrics provide useful data that can be analyzed and utilized in technical, operational, and business decisions across the organization. A metric can be qualitative or quantitative, and is 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.

Metrics are categorized into organizational, operational, and technical.

Organizational Metrics

Operational Metrics

Technical Metrics

What are Security Metrics?

- ◆ **Organizational Metrics**

Organizational Metrics apply to people and their interaction with each other and with critical functions.

These metrics apply anywhere personnel exist in operations.



What are Security Metrics?

- ◆ **Operational Metrics**

Operational Metrics include aspects such as physical security, redundancy, and safe operating procedures that ensure secure functions.



What are Security Metrics?

- ◆ **Technical Metrics**

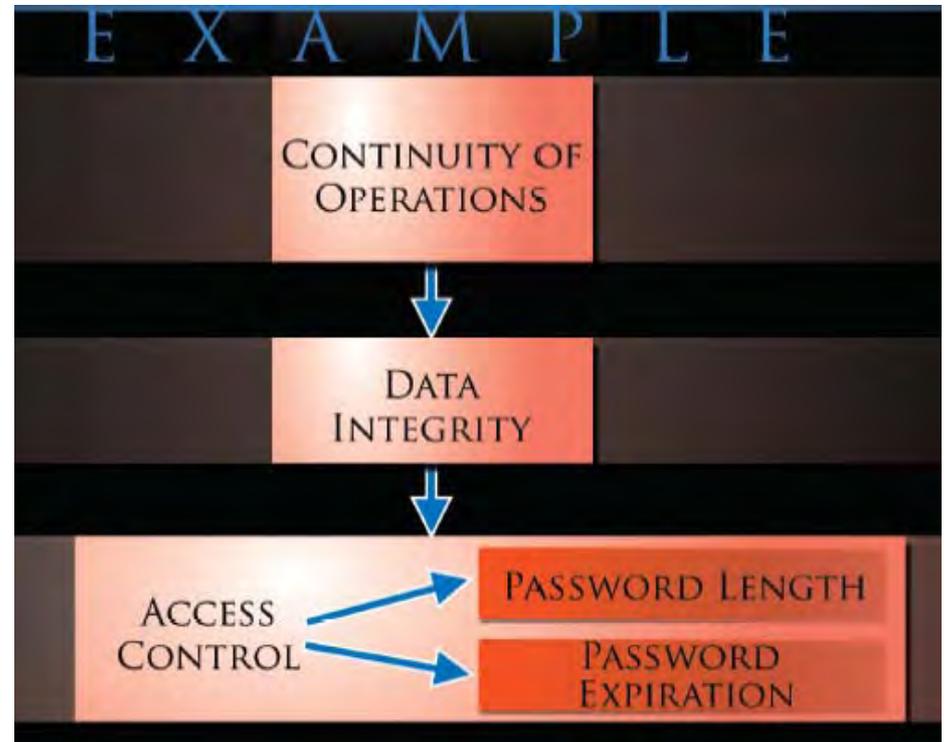
Technical Metrics address technological areas that either require security or produce data used in security decisions.



Structuring Metrics

- ◆ **Metrics should be used to ensure overall mission objectives, such as safety and continuity of operations.**
- ◆ **A process assists in meeting these objectives, whether it is operational, technical, or a personnel function.**
- ◆ **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.**

Structuring Metrics



Metrics from Standards and Best Practices

Metrics can be derived from Standards, Suggested Guidelines, and Best Practices.

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 require 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

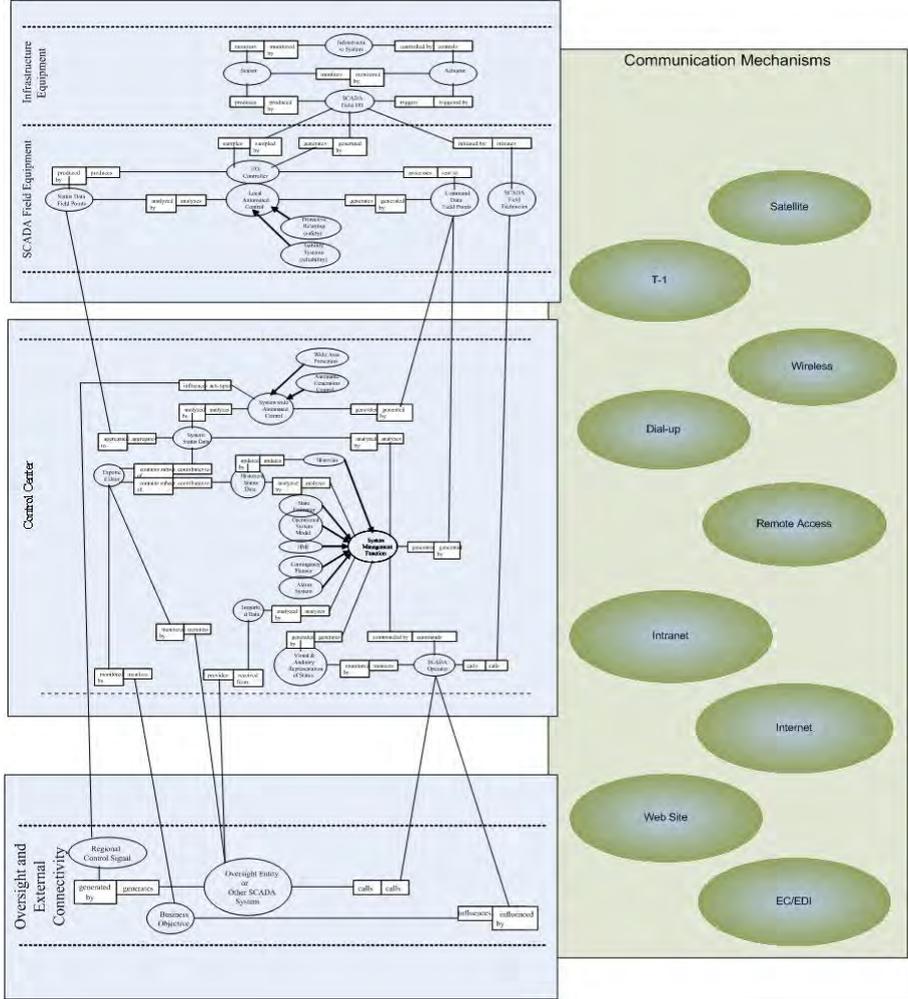
√ 100% Compliant with Best Practice

Why have a Taxonomy?

- ◆ A taxonomy provides an approach for industry to understand why, where, and how metrics can be applied to their operations.
- ◆ This metrics taxonomy is based on operational objectives and mission, rather than standard IT business objectives.
- ◆ An operational approach means a flexible product that can bend to the individual asset owner's architectural needs.
- ◆ Utilizing the Automated Systems Reference Model looks at a standard control network structure but can be customized for each industry member.
- ◆ This provides a take-away map for industry for immediate use.

Operational Structure

The Metrics Taxonomy builds upon operational areas designated in the Automated Systems Reference Model (ASRM) and associated communication mechanisms. Operational, organizational, and technical metrics are applied in each area according to overall mission objectives.



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

Mapped Metrics

- ◆ **Because the ASRM represents a generic architecture, each organization can build on the design to meet their specific topology.**
- ◆ **Organizational, operational, and technical metrics can be applied in each area.**
- ◆ **These metrics take into consideration:**
 - 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
 - Standards or Guidelines the organization has chosen to employ

Mapped Metrics

- ◆ **Interactive Taxonomy (see PDF)**
- ◆ **Taxonomy could easily be customized to meet individual organizational objectives and selected standards**

How to use the Taxonomy

- Asset owners and managers can utilize the taxonomy to identify where and how to apply metrics.
- **Step 1:** Identify your architecture
- **Step 2:** Delineate your primary mission goals
- **Step 3:** Select guidelines, standards, or a set of best practices that best reflects your industry needs
- **Step 4:** Map metrics associated with the best practices in each operational area, keeping in mind technical, operational, and organizational areas. Where does this apply to 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.

Conclusions

- ◆ **The use of metrics has recently received a lot of attention.**
- ◆ **IT metrics cannot be applied to control system architectures. Industry owners with control system architectures have different mission goals!**
- ◆ **Metrics must be addressed with operations in mind.**
- ◆ **Metrics must be applied in a cost-effective manner, meeting goals, reducing risk, and financial feasibility.**
- ◆ **Metrics can reduce overall cyber consequence.**

Summary

- ◆ **The metrics taxonomy is a moldable model that is flexible for industry, rather than a rigid product that may not easily be employed.**
- ◆ **A taxonomy assists asset owners in tailoring their needs and applying metrics to achieve their mission goals.**
- ◆ **The metrics taxonomy based on the ASRM focuses on control systems security, not IT security.**
- ◆ **Addressing metrics as part of the life-cycle can be a cost-effective way to secure operations and achieve overall goals.**

POC Info

Annie McIntyre

505.284.0968

amcinty@sandia.gov

Ron Halbgewachs

505.844.8054

rdhalbg@sandia.gov

Blair Becker

505.844.8877

dbecker@sandia.gov

Bankim Tejani

505.284.9877

bjtejan@sandia.gov

Center for SCADA Security

<http://www.sandia.gov/scada/home.htm>

Sandia – National SCADA Test Bed Program

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



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.