U.S. DEPARTMENT OF
ENERGY

PNNL-18031

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Metrics for the National SCADA Test Bed Program

PA Craig, Jr
J Mortensen
JE Dagle

October 2008

Pacific Northwest
NATIONAL LABORATORY

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401, fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847, fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

♻ This document was printed on recycled paper.

(8/00)

PNNL-18031

Metrics for the National SCADA Test Bed Program

PA Craig, Jr
J Mortensen*
JE Dagle

October 2008

Prepared for
U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352

*Energetics, Inc.

ENERGETICS
A Subsidiary of VSE Corporation

Summary

The U.S. Department of Energy-Office of Electricity Delivery and Energy Reliability (DOE-OE) National SCADA (Supervisory Control and Data Acquisition) Test Bed (NSTB) Program is providing valuable inputs into the electric industry by performing topical research and development (R&D) to secure next generation and legacy control systems. In addition, the program conducts vulnerability and risk analysis, develops tools, and performs industry liaison, outreach and awareness activities. These activities will enhance the secure and reliable delivery of energy for the United States. This report will describe metrics that could be utilized to provide feedback to help enhance the effectiveness of the NSTB Program.

Contents

Figures

Tables

Introduction

The National SCADA Test Bed (NSTB) Program is providing valuable inputs into the electric industry by performing topical research and development (R&D) to secure next generation and legacy control systems. In addition, the program conducts vulnerability and risk analysis, develops tools, and performs industry liaison, outreach and awareness activities. These activities will enhance the secure and reliable delivery of energy for the United States.

The following issues share a common set of core drivers that address efficiency, security, and reliability for the U.S. national energy infrastructure.

Efficiency is essential to delivering energy within current demands of rapidly expanding infrastructure where capital cost recovery, operating costs, and future investments drive such costs directly to end users.

Security is no longer limited to the chain link fencing that protects assets from tampering and public interests in health and safety from the dangers of exposure to these assets. Rather, current security postures are rapidly adapting to serious and dynamic threat environments that consider physical and cyber attacks frontrunners that are challenging the operational integrity, resiliency, and economic stability of our Nations' critical energy infrastructure.

Reliability is at the core of public trust that energy will be available for use anytime the demand or desire requires it and plays a role paramount to public health and safety, and economic stability.

To this end, the U.S. Department of Energy - Office of Electricity Delivery and Energy Reliability (DOE-OE) has committed to providing R&D support for enhancing security of control systems associated with the Nation's critical energy infrastructure.[1]

This report will discuss components and attributes of *metrics* that could be utilized to provide feedback to those who manage strategic objectives, provide advisory input, or provide deliverables to the NSTB Program. To accomplish this task, the Pacific Northwest National Laboratory (PNNL) partnered with Energetics Inc. to develop this report. An initial draft report was provided by Energetics that included an approach to *modeling* the design of NSTB Program components, providing metrics for each component within the model, and identifying a data collection method for each component. Following the submission of this draft, PNNL utilized additional internal expertise that included experience in creating security metrics and control system security subject matter experts to develop this final report that incorporates materials from Energetics' report. The PNNL expertise also leveraged participation in an Institute for Information Infrastructure Protection (I3P) effort culminated in the *"Process Control System Security Metrics – State of Practice"*, Research Report No. 1, August 2005 that was submitted under a U.S. Department of Homeland Security, Science and Technology Directorate grant[2].

[1] http://www.oe.energy.gov/controlsecurity.htm

[2] U.S. Department of Homeland Security, Science and Technology Directorate grant number 2003-TK-TX-0003.

Purpose

As with any federal government program, the NSTB Program must have a structured and defensible method for evaluating the effectiveness and success of its investments. At the core of this evaluation is the development and application of logical and reliable metrics that tie program outputs to improvements in control system security in the energy sector. PNNL believes that a hybrid of the Energetics approach with some additional consideration to higher programmatic oversight would give the DOE-OE program management and its associated industry advisory council a better series of overall metrics for determining necessary strategic adjustments as well as benchmark measurements of the NSTB Program deliverables. Key to this goal is achieving the objectives in the control systems roadmap for the energy sector.[1] Therefore, the purpose of this task is to develop a framework in which metrics supporting such a defensible method could be created.

[1] Roadmap to Secure Control Systems in the Energy Sector, sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security, prepared by Energetics Incorporated, Columbia Maryland, January 2006.

Goals, Milestones and Activities

The NSTB Program has been committed to an approach that includes *performance goals, milestones,* and *activities*. To deliver on this approach, an Energy Sector Control Systems Working Group of the Critical Infrastructure Partnership Advisory Council is assigned to coordinating the roadmap research efforts among the *Electric* Sector Coordinating Council (SCC), the *Oil & Natural Gas* SCC, and the Government Coordinating Council (GCC) for Energy.

The NSTB Program, in collaboration with its partners, sets milestones to achieve the roadmap objectives through research and other activities that deliver practical solutions. This approach, while effective at delivering results to achieve the established milestones, does not necessarily deliver a systematic representation of the *effectiveness* of these activities in achieving the roadmap's goals. It should be the desire of the program and its industry advisory council to attain information that supports their strategic decisions during the assignment of roles and responsibilities, priorities, and future efforts. To determine which method would best represent the program's success, there should be a number of pointers to *what* is viewed as success in the eyes of various stakeholders.

The success of the NSTB Program will be realized when the NSTB team completes the necessary activities that support the program goals, and the goals have *effectively* supported the vision of the program. The operative phrases are "*completes the necessary activities*" and "*effectively supported the vision*". How would these two statements be supported? Completing the necessary activities should be a simple exercise in the alignment of deliverables to the desired milestones. The second *success* however, is more difficult to define. The DOE-OE and NSTB advisory council members have predefined success as a vision provided in the roadmap that states, *"In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function."*

This vision is supported by four roadmap goals:

- Measure and Assess Security Posture
- Develop and Integrate Protective Measures
- Detect Intrusion and Implement Response Strategies
- Sustain Security Improvements.

Each goal is represented in more detail in Exhibit 1.5 of the roadmap. *It is important to note that each goal also has identified an achievable date of 2015.* This is important because it identifies that the each goal is being achieved by teams working on parallel activities each with an eye on ensuring the program's vision is met, preferably with commensurate levels of success for each activity.

The following section describes a logic model to identify metrics that could be useful for evaluating the overall impact of the NSTB Program.

Approach and Methodology

A well-documented and widely used approach was utilized to identify metrics for the NSTB Program. This approach followed three steps:

1. Develop a logic model for the program
2. Identify metrics and/or measures for each logic model component
3. Develop a data collection plan for each metric or measure.

A logic model is a graphical depiction showing how program activities lead to intended outcomes or goals. The logic model is a widely-used tool in the program planning and evaluation community for showing how a program is designed, providing a foundation for metrics development, and identifying key evaluation questions. For this project, the logic model is used to confirm the program's design and used the components of the logic to identify potential metrics.

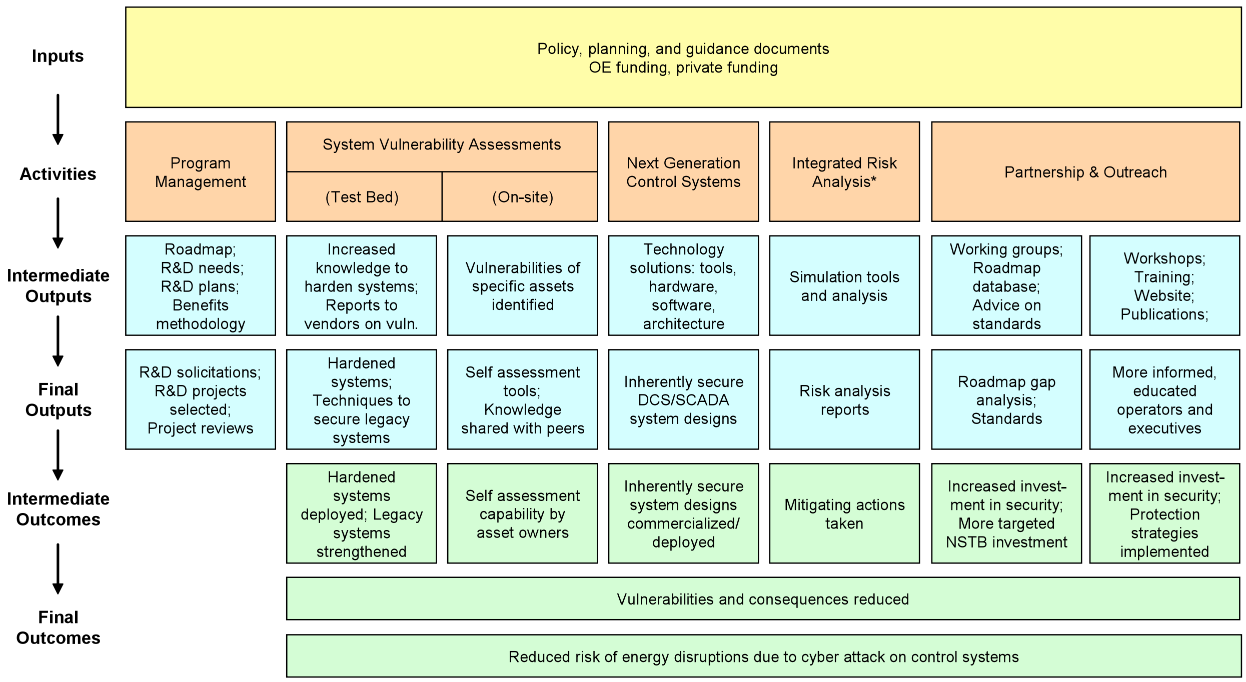
Development of the NSTB Program Logic Model

Inputs into the NSTB Program include policy, planning and guidance documents that DOE-OE and other stakeholders may develop that influence the direction of the program; funding received through the NSTB Program; and private sector funding that may complement the activities the program is undertaking.

NSTB Program activities fall into five categories: Program Management, System Vulnerability Assessments (Test Bed and On-site), Next Generation Control Systems, Integrated Risk Analysis, and Partnership and Outreach. These activities each lead to a number of intermediate and final *outputs*, which are directly produced or influenced by the NSTB Program. These outputs then influence intermediate and final outcomes that align with the goals of the NSTB Program.

The logic model for the NSTB Program (Figure 1) illustrates how the program utilizes its resources to engage in activities that lead to achievement of its goal: *reduced risk of energy disruptions as a result of a cyber attack on the control systems*.

GOAL: Reduce the risk of energy disruptions due to cyber attack on control systems



Inputs	Policy, planning, and guidance documents OE funding, private funding						
Activities	Program Management	System Vulnerability Assessments (Test Bed)	System Vulnerability Assessments (On-site)	Next Generation Control Systems	Integrated Risk Analysis*	Partnership & Outreach	

Intermediate Outputs	Roadmap;
	R&D needs;
	R&D plans;
	Benefits methodology
		Increased knowledge to harden systems;
		Reports to vendors on vuln.
			Vulnerabilities of specific assets identified	Technology solutions: tools, hardware, software, architecture	Simulation tools and analysis	Working groups;
						Roadmap database;
						Advice on standards
							Workshops;
							Training;
							Website;
							Publications;

Final Outputs	R&D solicitations;
	R&D projects selected;
	Project reviews
		Hardened systems;
		Techniques to secure legacy systems
			Self assessment tools;
			Knowledge shared with peers
				Inherently secure DCS/SCADA system designs	Risk analysis reports	Roadmap gap analysis;
						Standards
							More informed, educated operators and executives

Intermediate Outcomes		Hardened systems deployed; Legacy systems strengthened	Self assessment capability by asset owners	Inherently secure system designs commercialized/ deployed	Mitigating actions taken	Increased investment in security; More targeted NSTB investment	Increased investment in security; Protection strategies implemented
Final Outcomes		Vulnerabilities and consequences reduced					
		Reduced risk of energy disruptions due to cyber attack on control systems					

* Risk analysis includes analysis of threats, vulnerabilities, consequences, and interdependencies

Figure 1. National SCADA Test Bed Program Logic Model

Activities and Intermediate/Final Outputs

Each of the program activities intermediate/final outputs is discussed in the following paragraphs as they relate to the logic model in Figure 1.

Program Management

The program management activity develops roadmaps, prioritizes R&D needs for mapping R&D plans, and drafts a methodology for estimating the benefits of the program. Once these foundational activities are completed, the program then releases R&D solicitations, selects R&D projects, conducts project reviews, and ensures resources are allocated in an optimal fashion and R&D activities are properly coordinated. The outcomes of the program management activity are inherent in the four remaining program activities.

System Vulnerability Assessments (Test Bed and On-site)

A key area of the NSTB program is assessing the vulnerabilities of control systems. System vulnerability assessments are conducted either in a laboratory environment or on-site at an energy company's facility. The advantage of the first type of testing is that it is performed in a controlled environment that provides a semi-realistic environment while enabling comprehensive testing without the hazards associated with inadvertent disruptions to infrastructure operations. Control systems are placed in the test bed and subjected to a variety of cyber attacks. The results of the tests are increased knowledge of vulnerabilities and recommended mitigation strategies that are then reported to the control system's vendor. The vendors address the vulnerabilities by creating new "hardened" control systems in the future, or lessons learned and software patches that secure existing legacy systems. The new hardened systems or the strengthened legacy systems are deployed and penetrate the market. This increased use of new and strengthened systems reduces the vulnerabilities, consequences, and risk of energy disruptions as a result of cyber attack on control systems.

The 'on-site' vulnerability assessments are performed at a selected operational facility to evaluate the control systems in a real-world setting. The on-site assessment identifies vulnerabilities specific to a particular asset. The advantage of this testing is that it provides a more realistic assessment of the actual security posture associated with the Nation's critical energy infrastructure. It is important that the knowledge gained through the on-site assessments is appropriately shared with other sites or facilities. An additional benefit of this activity is that it can lead to the development of self-assessment tools. This self-assessment capability will build on the benefits of the NSTB assessment process by empowering industry with proven assessment techniques, further reducing the risk of energy disruptions as a result of cyber attack on control systems.

Next Generation Control Systems

Another approach to reducing the risk of energy disruptions as a result of cyber attack is to develop control systems that are, to the extent possible, inherently secure. The NSTB Program funds R&D on such "next generation" control systems. The R&D produces a variety of technology solutions including tools, hardware, software, and architecture. These tools will be incorporated into future control systems that will be more robust and inherently secure. These system architectures, hardware, and software will then be commercialized, deployed, and will eventually penetrate the market. NSTB's next generation R&D is designed to accelerate this process from initial concept through final commercialization. By speeding the transfer of more secure next generation technologies to market, the NSTB Program enables the energy sector to respond more swiftly and effectively to current and emerging cyber threats, thereby reducing the risk of energy disruptions as a result of cyber attack on control systems.

Integrated Risk Analysis

Risk analyses can be conducted that are more comprehensive than examining the vulnerability of any single system or asset. Integrated risk analysis collectively examines threats, vulnerabilities, consequences, and cross-sector interdependencies using simulation tools or other analytical methods. Data obtained through integrated risk analyses reduce the risk of energy disruptions as a result of cyber attack by helping energy sector stakeholders to prioritize security needs and focus limited resources on the most pressing security issues, enabling more decisive mitigating action. Risk assessment data are also necessary to build a sound business case for investment in creating, procuring, and implementing such cyber security measures.

Partnership and Outreach

The final area in which the NSTB Program works to reduce risk is through partnership and outreach with various stakeholders. The program engages partners in activities such as roadmap implementation and standards development. Combining the expertise and perspectives of all facets of the sector ensures that security needs are being met and anticipated from every angle. Additionally, information and cost sharing minimizes the duplication of technology development efforts and maximizes resources to efficiently achieve effective solutions. Through the newly formed Energy Sector Control Systems Working Group, NSTB's public-private partnership efforts also facilitate R&D gap analysis that helps align public- and private-sector control systems security R&D with roadmap goals and strategies.

For outreach, the program conducts workshops and training, maintains a website, and distributes publications. All of these lead to more informed, educated operators and executives, who then increase investment in security and implement protection strategies. Outreach and educational activities keep industry groups informed and up-to-date regarding effective strategies and technologies to enhance infrastructure security. Engaging energy sector stakeholders through outreach encourages more rapid implementation of new security measures and provides input from the field to help guide future technology development.

Intermediate/Final Outputs

The next descriptions provide the logic model's intermediate/final outcomes that allow metrics to be defined.

Program Management

The metrics for program management area are mostly milestones or deliverables relating to the completion of materials such as roadmaps, R&D needs, R&D plans, benefits methodology, and solicitations. Quantitative metrics that can be tracked over time are the number of projects selected and the percentage of projects reviewed. Both of these metrics will provide information that will be useful for the Office of Management and Budget (OMB) Program Assessment Rating Tool (PART). PART question 3.CO1 asks whether funds are awarded based on a clear competitive process that includes a qualified assessment of merit.

System Vulnerability Assessments (Test Bed and On-site)

Metrics for system vulnerability assessments are divided by whether they are conducted at the test bed or at on-site locations. At the test bed level, the volume of testing could be measured by the number of systems tested. The critical nature of those tests could be measured by the percentage of tested systems affecting critical systems. Once testing is completed, the program could measure initial impacts with the number of hardened systems developed by vendors as a result of the tests, and the number of patches issued for existing systems. Another measure of the reach of the program could be the percentage of new systems on the market that have been tested. The program only has real impact if the systems penetrate the market. Thus, there are also metrics for the percentage of market share of the tested systems and the number of patches downloaded.

For on-site assessments, there is also a metric for the number of systems tested. The reach of the program is measured by the number (or percentage) of utilities participating in on-site testing. The percentage of utilities participating metric needs further examination to determine how the percentage would be calculated (e.g., based on annual power generation). Final outputs could be evaluated by the number of hardened on-site systems developed and the number of self-assessment tools that were developed. The penetration of self-assessment tools could be measured by the percentage of asset owners performing self-assessments.

For both categories above, it is important to determine the characterize the vulnerabilities by the impact they would have, if compromised, to critical functionality of the control systems, the impact that this loss of functionality would have on overall system operation, and any mitigating measures in place that would either limit the impact or enhance the restoration and recover of critical functionality.

Next Generation Control Systems

Developing metrics for the next generation control systems program area is more difficult because measurement of R&D is hard to standardize. Output metrics could include the number of technology solutions developed and the number of technologies transferred to vendors. Once the technologies are in vendors' hands, the market share of those technologies could be measured over time. An important additional consideration is the overall effectiveness of these solutions, and how broadly they are implemented.

Integrated Risk Analysis

The integrated risk analysis program area is also difficult to measure. The outputs of the risk analysis activities could be measured by the number of risk scenarios conducted and the number of critical risk scenarios identified. Once those scenarios are identified, the program could measure the percentage of the critical scenarios that are being addressed. Key concepts that need to be included are thoroughness and representativeness of the scenarios. Adding other measurements to judge the value of the scenarios generated, such as likelihood and impact, will give greater credibility to the risk analysis.

Partnership and Outreach

Outputs of the partnership area of the NSTB Program could be measured by the number and percentage of partners represented in working groups, number of organizations in the roadmap database, and the number of projects in the roadmap database, and the percentage of roadmap priorities addressed. Involvement of partners could ultimately be measured by the partner cost-sharing ratio.

The outreach component could be measured by the number of workshops held, number of people trained, number of downloads of program documents, and number of publications. The effectiveness of the training component could be measured by having trainees taking a test and tracking the average test score of trainees. (These test scores should be normalized to prevent lax training from inflating the scores.) Another common problem with most cyber security training is that it lacks comprehensiveness, or situationally-relevant subject matter tailored to the employees' job duties. A more in-depth evaluation could determine the percentage of trainees taking action as a direct result of the training they received.

Identification of Metrics and Measures

To identify successes that support activities within the NSTB Program, effective measures for the previously discussed metrics need to be developed. While one could apply a specific *measure* to quantify a metric, an understanding of what makes *good* and what makes *bad* measurements should be discussed. Also, one should consider that the successful measurement of a metric might not provide any information or insight into the *effectiveness* of the specific metric, *or* a relationship to any other metric within the model. Rather, the metric simply represents a number (quantifiable value) and that number's relationship to a definable given point (a measurement). With this perspective, some constraints should be identified that provide definition to the metrics' unit of measure. Metrics used for quantifying value (doing the right things) and those used to measure performance (continually doing those things better), are distinctly different if provided as separate metrics within the same logic model. For the purpose of the NSTB activities represented in the logic model, the intent of the metric should be to combine these concepts into a single measurement of "continually doing the *right things* better". This approach is discussed in greater detail in *Security Metrics*, *Replacing Fear, Uncertainty, and Doubt.*[1]

The primary goal of the metrics identified in the model is to "quantify data to facilitate insight". Metrics do this by:

- Helping an analyst diagnose a particular subject area or understand its performance
- Quantifying particular characteristics of the chosen subject area
- Facilitating "before-and-after", "what-if", and "why/why not" inquiries
- Focusing discussion about the metrics themselves on causes, means, and outcomes rather than on methodologies used to derive them.

To provide good data supporting these attributes, the data should be 1) consistently measured, 2) cheap to gather, 3) expressed as a number or percentage, and 4) contextually specific. Conversely, inconsistent, expensive, non-numerical, non-specific data is worthless and makes a bad metric.

The second method employs measures. Measures will provide data for a specific metric (if properly constructed as described above). They are more effective if represented against benchmarked data when a comparative analysis is desired. Benchmarks rely on either baseline (known and/or accepted criteria) or relational (comparative analysis of like environments) data. In the case of the NSTB activities, benchmarks are a luxury when attempting to be deterministic of success related to cyber security implementations. Historically, a benchmark of 'one' event can have serious implications whether to equipment, or to public perception, both of which have lasting impressions on the effectiveness (or lack thereof) of measures, or counter measures employed to protect a control system. For example, in a typical information technology (IT) anti-virus protection appliance thousands of virus attempts may be thwarted each day, which is an illustration that you're getting your money's worth. In a control system, even the exposure to this type of attempt would be considered unacceptable.

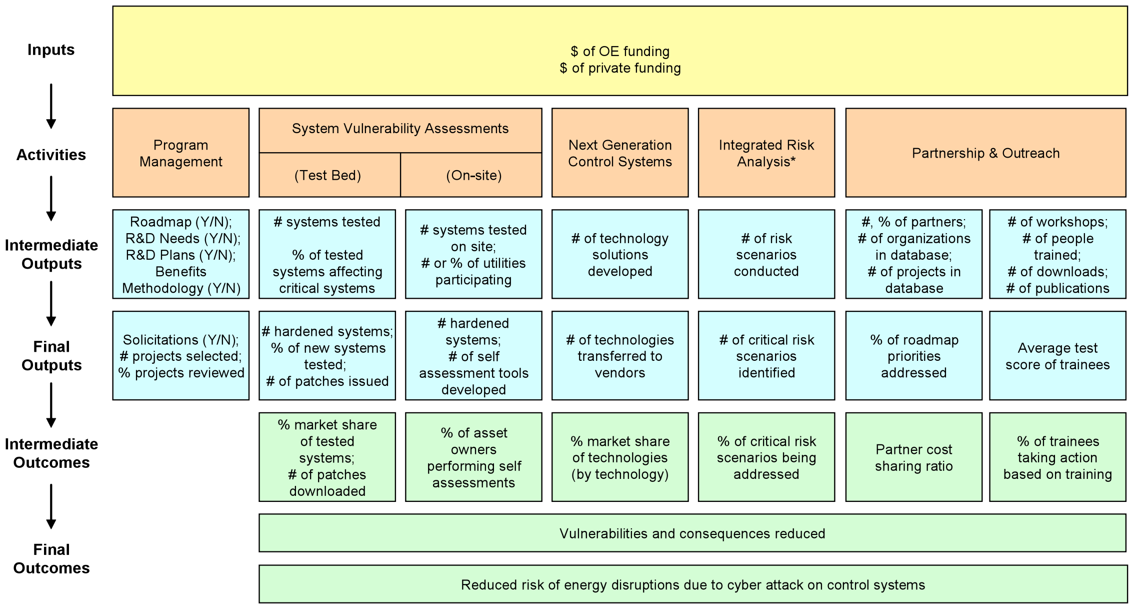
[1] *Security Metrics, Replacing Fear, Uncertainty, and Doubt, Andrew Jaquith, March 2007, Addison-Wesley, New York.*

When determining the metric, and employing the necessary measure to attain a metric value, one should always consider the primary goal of the metrics identified in the model, which is to "quantify data to facilitate insight".

Metrics Supporting the Logic Model

Each activity, output, and outcome box in the logic model represents a *potential measurement area*. Through identification of metrics across the activities, outputs, and outcomes, the NSTB Program can describe how its activities are leading to the realization of final (and desired) outcomes. Initial metrics for the NSTB Program are shown in Figure 2. Not all of the metrics shown can be easily measured. In addition, some may be measured in the near term, while others may represent longer-term measurement opportunities. The metrics shown are intended to *foster discussion (an attribute of a 'good' metric)* among stakeholders on how the NSTB Program might demonstrate progress over time.

GOAL: Reduce the risk of energy disruptions due to cyber attackon control systems



Inputs	$ of OE funding $ of private funding						
Activities	Program Management	System Vulnerability Assessments (Test Bed)	System Vulnerability Assessments (On-site)	Next Generation Control Systems	Integrated Risk Analysis*	Partnership & Outreach	

Intermediate Outputs	Roadmap (Y/N);
	R&D Needs (Y/N);
	R&D Plans (Y/N);
	Benefits Methodology (Y/N)
		# systems tested
		% of tested systems affecting critical systems
			# systems tested on site;
			# or % of utilities participating
				# of technology solutions developed	# of risk scenarios conducted	#, % of partners;
						# of organizations in database;
						# of projects in database
							# of workshops;
							# of people trained;
							# of downloads;
							# of publications

Final Outputs	Solicitations (Y/N);
	# projects selected;
	% projects reviewed
		# hardened systems;
		% of new systems tested;
		# of patches issued
			# hardened systems;
			# of self assessment tools developed
				# of technologies transferred to vendors	# of critical risk scenarios identified	% of roadmap priorities addressed	Average test score of trainees

Intermediate Outcomes		% market share of tested systems; # of patches downloaded	% of asset owners performing self assessments	% market share of technologies (by technology)	% of critical risk scenarios being addressed	Partner cost sharing ratio	% of trainees taking action based on training
Final Outcomes		Vulnerabilities and consequences reduced					
		Reduced risk of energy disruptions due to cyber attack on control systems					

* Risk analysis includes analysis of threats, vulnerabilities, consequences, and interdependencies

Figure 2. Potential National SCADA Test Bed Program Metrics

(Metrics for reduction in vulnerabilities, consequences, and risk were not identified because they were considered beyond the scope of this project and it would be unlikely the program could measure them in the near future.)

NSTB Program Data Collection Plan

The next step was to identify how data on each metric might be collected, when, and how frequently (Table 1). The timetable for the metrics focuses on measuring outputs in the first year or two and then transitioning to measuring outcomes.

Table 1. NSTB Program Data Collection Plan

Program Management			
Metric	**Evaluation Method**	**Frequency**	**Start**
Roadmap (Y/N)	Review of project records	Periodic	2008
R&D Needs (Y/N)	Review of project records	Periodic	2008
R&D Plans (Y/N)	Review of project records	Periodic	2008
Benefits Methodology (Y/N)	Review of project records	Periodic	2008
Solicitations (Y/N)	Review of project records	Periodic	2008
# of projects selected	Review of project records	Annual	2009
% of projects reviewed	Review of project records	Annual	2009
System Vulnerability Assessments (Test Bed - TB, On-site - OS)			
Metric	**Evaluation Method**	**Frequency**	**Start**
# of systems tested (TB)	Review of project records	Annual	2009
% of tested systems affecting critical systems (TB)	Expert review	Periodic	2009
# of hardened systems (TB)	Project records; market analysis	Periodic	2010
% of new systems tested (TB)	Review of project records	Annual	2010
# of patches issued (TB)	Market analysis or vendor survey	Periodic	2010
% market share of tested systems (TB)	Project records; market analysis	Periodic	2012
# of patches downloaded (TB)	Vendor survey	Periodic	2012
# of systems tested on-site (OS)	Review of project records	Annual	2009
# or % of utilities participating (OS)	Review of project records	Annual	2009
# of hardened systems (OS)	Project records; utility survey	Periodic	2010
# of self assessment tools developed (OS)	Review of project records	Annual	2010
% of asset owners performing self assessments (OS)	Survey	Periodic	2011
Next Generation Control Systems			
Metric	**Evaluation Method**	**Frequency**	**Start**
# of technology solutions developed	Review of project records	Annual	2009
# of technologies transferred to vendors	Review of project records	Annual	2010
% market share of technologies (by technology)	Review of project records; market analysis or survey	Periodic	2011
Integrated Risk Analysis			
Metric	**Evaluation Method**	**Frequency**	**Start**
# of risk scenarios conducted	Review of project records	Periodic	2009
# of critical risk scenarios identified	Review of project records	Periodic	2010
% of critical risk scenarios being addressed	Review of project records	Periodic	2011
Partnership & Outreach			
Metric	**Evaluation Method**	**Frequency**	**Start**
#, % of partners	Review of project records	Annual	2009
# of organizations in database	Review of project records	Annual	2009
# of projects in database	Review of project records	Annual	2009
# of workshops	Review of project records	Annual	2009
# of people trained	Review of project records	Annual	2009
# of downloads	Web tracking	Annual	2009
# of publications	Review of project records	Annual	2009
% of roadmap priorities addressed	Expert review	Periodic	2010
Average test score of trainees	Survey of training participants	Annual	2009
Partner cost sharing ratio	Review of project records	Annual	2010
% of trainees taking action based on training	Survey of training participants	Periodic	2010

Conclusions

Some additional discussion and deliberation is required to determine the value that the metrics presented in this report will add to the management of the NSTB Program. A true metric is centered on an analysis of a data set that is bounded by specific measurable criteria. The key issue is “data”. What actual *data* can the program activities provide that would contain measurable substance? Because the NSTB Program encompasses research and development activities, which have little basis for gathering quantifiable data for analysis without significant amounts of judgment, it is difficult to develop quantifiable metrics. Ultimately, there is still the lingering question of whether control system security itself can be effectively quantified as a metric because it may be impractical to envision and fully quantify all possible risks.

Next Steps

Discussion of the logic model and metrics for the NSTB Program should follow a formal submission to the DOE-OE and the NSTB team. These detailed discussions should focus on defining and collecting baseline data supporting the metrics, and evaluating whether effectiveness can actually be determined.

Any metrics that are developed should be provided with updates as activities are completed to the milestones listed in the roadmap. These updates should be submitted to DOE-OE and the advisory council, and should be a factor in annual planning and strategic decisions of the NSTB Program.