Summary of SCADA Cyber Self-Assessment Methods and Tools Survey
2/16/07

Introduction

(*Note*: *in this document, consistent with the group's name and usage, the term "SCADA" is used as a short hand for all types of industrial manufacturing and control systems.)*

In order to find gaps in the requirements met by the existing set of self assessment tools/methodologies, the PCSF SCADA Cyber Self Assessment Working Group is carrying out the following steps:

1. **Identify SCADA-unique characteristics:** Identify the set of SCADA-unique characteristics that one would expect to be addressed by tools or methodologies for cyber self assessment for these types of systems.
2. **Select tools/methodologies:** Define a set of cyber security self-assessment tools/methodologies that we will consider as representative of the "best available."
3. **Identify gaps:** Compare coverage by the tools/methodologies identified in Step 2 to the SCADA unique characteristics in Step 1 to identify gaps.

In this document we summarize results to date in carrying out these steps, and discuss next steps for the working group.

SCADA Unique Characteristics

The group is drawing information from the following resources to create a list of SCADA unique characteristics. The current unique characteristics list is available from the working group library on the PCSF web site, see table in the library document titled "Methodology/Tool Analysis Template." The **Status** column below indicates whether the most recent version of the template covers the issues found in each resource cited.

Table 1 - Sources for SCADA Unique Characteristics

Sector	Sources for SCADA Unique Characteristics	Status
Electric Power	- NERC Critical Infrastructure Protection Standards 002-009 http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection	- Covered
	- Sandia's "Reference Model for Control and Automation Systems in Electric Power" http://www.oe.energy.gov/DocumentsandMedia/Reference_Model_for_Control_and_Auto_Systems_in_Elec_Ind.pdf#search=%22reference%20model%20for%20control%20and%20automation%22	- Covered
	- NERC Top Ten Vulnerabilities of Control Systems and Their Associated Mitigations – 2006 ftp://www.nerc.com/pub/sys/all_updl/cip/Top_10_vuln_2006_16mar2006_ss.pdf	- Covered

Water/Wastewater	Interim Voluntary Security Guidance for Water Utilities, Section 5; http://www.awwa.org/science/wise/#P7_623	- Pending
Chemical	- CIDX Guidance for Addressing Cyber Security in the Chemical Industry Version 2.1 http://www.chemicalcybersecurity.com/cybersecurity_tools/	- Covered
Refining and Petrochemical	- API 1164, Pipeline SCADA Security - main body of standard Available for purchase from Techstreet and other vendors http://www.techstreet.com/cgi-bin/detail?product_id=1175186	- Pending
Cross-sector	- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator http://www.digitalbond.com/dale_peterson/presentations.htm - DOE 21 Steps to Improve Cyber Security of SCADA Networks http://www.tswg.gov/tswg/ip/21_Steps_SCADA.pdf#search=%2221%20Steps%20SCADA%22 - Process Control System Security Technical Risk Assessment: Analysis of Problem Domain www.thei3p.org/about/researchreport3r1.pdf - NIST Special Publication 800-82 Guide to SCADA and Industrial Control System Security, Initial Public Draft http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf - ISA-TR-99 Reports available for purchase at www.isa.org - ISO 17799 Available for purchase at Standards Direct http://www.standardsdirect.org/iso17799.htm - ISA SP-99 Parts I and II drafts available at SP-99 Working Groups 2 and 3 web pages: http://www.isa.org/MSTemplate.cfm?Section=Working_Group_2__Applications_and_Practices&Site=SP99,_Manufacturing_and_Control_Systems_Security1&Template=/ContentManagement/MSHTMLDisplay.cfm&ContentID=55782 http://www.isa.org/MSTemplate.cfm?Section=WG3_SP99_Part_1_Standard&Site=SP99,_Manufacturing_and_Control_Systems_Security1&Template=/ContentManagement/MSHTMLDisplay.cfm&ContentID=55783	- Covered - Covered - Covered - Pending - Pending - Pending - Pending

Tools/Methodologies List

The group identified for evaluation the following tools and methodologies to represent capabilities available or soon to be available. A status of "Draft posted" means a draft of the evaluation is posted to the Working Group library on the PCSF web site.

Table 2 - Tools/Methodologies for Evaluation

Sector	Tools/Methodologies	Evaluation Status
Electric Power	The group reviewed the following resources from this sector, but found that these did not address self assessment for SCADA cyber security. - IT Recovery Plan for Electric Co-ops (NRECA) https://crn.cooperative.com/Resources/SoftwareDownloads/ITRecoveryPlanning.htm - Method(s) from NERC's "Risk Assessment Methodologies for Use in the Electric Utility Industry" http://www.esisac.com/library-assessments.htm The group recently identified a privately developed assessment tool targeting the electricity industry.	-NA -NA -Pending
Water/Wastewater	- RAM-W (Risk Assessment Methodology – Water) - VSAT (Vulnerability Self Assessment Tool)	- Draft posted - Draft posted
Chemical	- CIDX Guidance for Addressing Cyber Security in the Chemical Industry Version 3.0 – Appendix 1 Self Assessment Questions http://www.chemicalcybersecurity.com/cybersecurity_tools/ - PHAWorks	- Draft posted - Draft complete, in review by vendor Primatech
Refining and Petrochemical	- API Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries - API 1164 Appendices A and B self-questionnaires on SCADA security Both available for purchase from www.techstreet.com and other vendors - Methodology/tool of Industry Participant (proprietary)	- Draft posted - Draft posted - Draft complete, in review by Industry Participant
Cross-sector	- DHS NCSD cyber security questionnaire (mid-level) - DHS CS2SAT (Control System Self Assessment Tool, detail level, uncustomized version)	- Draft posted - Draft posted

Overview of Tools/Methodologies

Resources that we labeled as "methodologies" are step by step instructions for either risk or vulnerability assessment. Resources that we labeled as "tools" were either software based tools or paper-based self-assessment questionnaires. Table 3 and the explanatory text that follows it, summarize information gathered to date.

In the "Focus" column, we note that these methodologies and tools have quite different areas of coverage:

- Some focus on prioritizing risks, others on assessing potential vulnerabilities by comparing to known lists or best practices, and some both
- Some focus on both physical and cyber risks and some on cyber only
- Some focus on cyber risks in general but do not address unique SCADA characteristics in particular, even though they may include SCADA systems as part of the assessment scope.

Table 3 - Tools/Methodologies Characteristics

Name	Type	Sector	Focus
RAM-W	Methodology	Water/Wastewater	Risk assessment and management; both physical and cyber risk; not SCADA specific
API Security Vulnerability Analysis Methodology	Methodology	Refining and Petrochemical	Risk assessment and management; both physical and cyber risk; not SCADA specific
VSAT	Software Tool	Water/Wastewater	Risk assessment and management; both physical and cyber risk; includes some high level SCADA specific assets and threats
CS2SAT	Software Tool	Cross-sector	Cyber vulnerability assessment; unique to SCADA systems
DHS NCSD Questionnaire	Questionnaire	Cross-sector	Cyber vulnerability assessment; not SCADA specific
API 1164 Standard Appendices A-B	Questionnaire plus sample Cyber Security Plan (embodying methodology)	Refining and Petrochemical	Cyber risk assessment, management, and cyber vulnerability assessment; includes many SCADA unique elements
Industry Participant	Spreadsheet tool	Refining and Petrochemical	*(Summary pending review by industry participant)*

Name	Type	Sector	Focus
Internal Tool			
CIDX Guidance for Addressing Cyber Security in the Chemical Industry Version 3.0 – Appendix 1 Self Assessment Questions	Questionnaire	Chemical	Cyber vulnerability assessment; some SCADA specific questions
PHAWorks	Software tool with associated documentation for application to industrial and process control cyber security	Chemical	Cyber risk assessment, management, and cyber vulnerability assessment; includes some SCADA unique elements; some coverage of related physical security topics.

As shown in the table, the group evaluated four software-based tools: one focused on the water sector (VSAT), one internal tool from an industry participant in the refining and petrochemical sector, one used in the chemical sector (PHAWorks) and one cross-sector tool (CS2SAT). VSAT was developed with EPA and private funds, is focused on risk assessment and choosing between countermeasures based on risk reduction impact for a water utility. It is not specific to cyber risk or to control systems, but identifies those areas at a high level as part of an overall risk assessment and countermeasure strategy for a water utility. The internal proprietary tool from the refining and petrochemical sector is implemented as a spreadsheet and provides a number of best practices guidelines. The cross-sector CS2SAT software tool under development by DHS/INL supports cyber self-assessment specifically for control systems. Beta versions of this tool customized for the water and electric power sectors have been developed. CS2SAT reviews typical vulnerabilities by focusing on individual components of the control system network, and also supports assessment against sector-specific standards. The PHAWorks tool is a commercial offering originally developed for safety and compliance assessment, but can be used to assess process control cyber security if taken together with guidance from documents on this topic offered by the vendor.

The group evaluated three questionnaires related to cyber security, developed by DHS, CIDX and API respectively. The DHS questionnaire does not address SCADA unique characteristics; rather it covers cyber security at a generic level. The CIDX Appendix questionnaire addresses some SCADA unique characteristics, but does not reflect all

issues that are pointed out in the main body of this same CIDX guidance document. The API questionnaire is specific to SCADA systems, including detailed questions and implied best practice recommendations. It was targeted at small to medium pipeline operators.

The group evaluated the methodologies RAM-W and the American Petroleum Institute (API) Security Vulnerability Analysis Methodology. RAM-W was developed by Sandia National Labs in conjunction with the EPA, and the AWWARF (American Water Works Association Research Foundation). It provides a method for prioritizing all kinds of risks including cyber, by providing a system of categories for threats and consequences and a quantitative formula for risk. The API SVA lays out a qualitative matrix method for assessing consequence and vulnerability. Both methodologies provide guidance on data that needs to be collected (including that for cyber systems) in order to carry out a solid analysis. Neither method is intended to provide guidance on how to assess a company's posture relative to "best practices" related to SCADA cyber security. Assessment of vulnerability is required to carry out these methodologies, but specific cyber security management practices and lists of possible cyber vulnerabilities are outside the scope of these methodologies.

The group recently identified one new tool that addresses cyber security for the electric power sector, but has not yet evaluated this tool. This sector has recently approved standards for control system security, cited in Table 1. A comparison of these NERC standards to the set of control system unique elements in the methodology/tool evaluation template used by the working group can be found in the working group library.

From the above analysis of existing methodologies and tools, the group believes it will be useful to consider how best to architect tools to cover risk management and vulnerability analysis, physical and cyber risk, and SCADA and non-SCADA cyber risk, with goal to be most productive for users.

Identifying Gaps and Next Steps

As of this report, the group is carrying out the process of identifying requirements gaps. Specifically the group is working on a draft document that classifies SCADA unique characteristics as well covered or poorly covered by existing tools/methods over all sectors, and in specific sectors. This draft document contains a spreadsheet matrix of all methods/tools evaluated, against the list of SCADA unique characteristics. Versions of this document are posted to the working group library at https://www.pcsforum.org/groups/68/library/ with the titles "Methodology-Tool-Analysis_Vxx.xls."

At the working group meeting at PCSF Fall 2007, the group will present a view of the gaps identified and prioritize these gaps in terms of the need to develop methodology/tool requirements to fill them. The group will also call for volunteers interested in working on the tool/methodology requirements for these high priority gaps.

At the working group meeting at PCSF Spring 2006, the group had asked the roughly 40 attendees to vote on where they felt the gaps lie – the following topics received more than five votes. The area of risk assessment was an outlier- it received twice this many votes. The group interpreted the vote results not necessarily as an assessment of available methodologies/tools, but most likely a statement of where users feel they need the most help from methodologies/tools. The raw votes can be found in notes from this meeting posted to the working group library on the PCSF web site.

- Prioritizing risk based on threat and business impact
- SCADA specific security policy
- Specific recommendations for employee screening
- Cyber incident response
- SCADA specific vulnerability analysis.

The group will continue to refine the SCADA unique characteristics list incorporating the resources shown as pending in Table 1 above. However, at this point we have found that as we study new resources, most information is already included in the existing list. Therefore we do not expect major additions to the list and are proceeding with the gap analysis.

In addition the group will continue to examine new tools and methodologies as we become aware of them.