Process Control Systems
Industry Conference

Summary of

SCADA Cyber Self-Assessment Working Group

Results

August 2008

Executive Summary

During 2005-2008, the SCADA Cyber Self Assessment Working Group (SCySAG) carried out its charter to identify requirements unique to control systems that should be met by cyber self assessment tools and methods, and to analyze the requirements to identify gaps not met by available tools and methods.

The major conclusions from the SCySAG work were:

- Roughly a third of the requirements identified were adequately covered by existing tools and methods. These were high level topics with good correlation between control system and non-control system applications.
- The highest priority requirement areas with the weakest coverage by existing tools and methods were *identifying vulnerabilities, risk identification and assessment, access control* and *training*.
- Methods and tools vary widely in scope of coverage. It will be useful to consider how best to architect and integrate tools to cover risk management and vulnerability analysis, physical and cyber risk, and control system and non-control system cyber risk, with goal to be most productive for users.

The cross sector CS2SAT effort is well positioned to continue to strengthen identification of vulnerabilities, and access control self assessment. The weak tool coverage of the cyber risk topic is at least partially due to the lack of community consensus on how to treat cyber security risk in general, and for control systems in particular. The lack of coverage for training-related self assessment is at least partially due to the orientation of many tools and methods toward system technology issues that impact cyber security, rather than those related to personnel. The training requirements gap appears to be more straightforward to address than the risk gap area.

To reach the above conclusions, SCySAG developed a list of 19 self assessment method/tool requirements categories and control system-specific requirements areas under these categories, analyzed 9 existing methods and tools against these requirements areas, and worked with end users and other industry representatives in a workshop setting to prioritize gap areas, at the PCSF 2007 Meeting. Details of the SCySAG approach and written outputs from these efforts (for which the body of this report provides references) are available in electronic form from the SCySAG working group area of the PCSF website and also as part of the 2008 Process Control Systems Industry Conference (PCSIC) participant materials. It is SCySAG's intention that these intermediate outputs serve the community, for example as follows:

- The SCySAG requirements area list serves as a checklist for end users contemplating self assessment programs.
- The SCySAG requirements list serves as a feature candidate list for self assessment tool/method developers.
- SCySAG assessments of specific tools provide information and approaches to end users for the process of tool and method selection.
- SCySAG assessments of specific tools and methods provide a third party coverage perspective to the developers of these tools and methods.

To conclude its working group activities, SCySAG will host a panel discussion at the 2008 PCSIC to address the requirements areas of risk assessment and training. The working group will post an update of this report including outcomes from this panel. A second topic of this session will be potential transition for the methods and kind of activity carried out by SCySAG to other organizations.

Introduction

(*Note*: *The working group name retained the term "SCADA" for continuity, even though its work addressed all types of industrial control and automation systems.)*

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

1. **Identify control system-unique characteristics:** Identify the set of control-system 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 considered as representative of the "best available."
3. **Identify gaps:** Compare coverage by the tools/methodologies identified in Step 2 to the unique characteristics in Step 1 to identify gaps.

In this document we summarize results to date in carrying out these steps. The working group began by creating a list of relevant resources to consider. This list is captured in the document *VA_Tool_v4.0.xls*, which also shows the group's initial judgment of priority with respect to their effort.

Control System Unique Characteristics

The group considered and extracted information from the resources shown in Table 1, for creating its list of control system unique characteristics. The current unique characteristics list is available in a document titled "Methodology/Tool Analysis Template" (filename *Tool_evaluation_template_v3.0.doc*). A "Yes" in the **Covered** column below indicates that the source was reviewed in detail by the group, and its contents explicitly incorporated into SCySAG's 19 requirements categories in the template. After covering the documents indicated, the group judged that sufficient work had been done to create a useful characteristics list when duplicate information began turning up. The documents shown in this list as not covered were felt to provide valuable inputs that could be studied in detail to potentially uncover additional requirements insights. Note that since group members were also on the SP-99 committee, those standards documents are in all likelihood implicitly covered by the group's work.

Table 1 – Sources for Control System Unique Characteristics

Sector	Sources for Control System Unique Characteristics	Covered
Electric Power	• NERC Critical Infrastructure Protection Standards 002-009 *http://www.nerc.com/page.php?cid=2|20*	Yes
	• 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*	Yes
	• 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*	Yes
Water/Wastewater	Interim Voluntary Security Guidance for Water Utilities, Section 5; *http://www.awwa.org/science/wise/#P7_623*	No
Chemical	CIDX Guidance for Addressing Cyber Security in the Chemical Industry Version 2.1 *http://www.chemicalcybersecurity.com/cybersecurity_tools/*	Yes
Refining and Petrochemical	API 1164, Pipeline SCADA Security - main body of standard	No

Sector	Sources for Control System Unique Characteristics	Covered
	Available for purchase from Techstreet and other vendors *http://www.techstreet.com/cgi-bin/detail?product_id=1175186*	
Cross-sector	• Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator *http://www.digitalbond.com/dale_peterson/presentations.htm*	Yes
	• 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*	Yes
	• Process Control System Security Technical Risk Assessment: Analysis of Problem Domain *www.thei3p.org/about/researchreport3r1.pdf*	Yes
	• 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*	No
	• ISA-TR-99 Reports available for purchase at *www.isa.org*	No
	• ISO 17799 Available for purchase at Standards Direct *http://www.standardsdirect.org/iso17799.htm*	No
	• 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*	No

Tools/Methodologies List and Evaluation Template

The group identified and evaluated the tools and methodologies in Table 2 below, to represent capabilities available or soon to be available, on a per sector basis. In the right column of the table is the name of the Word file that contains the review that SCySAG carried out against its standard evaluation template. In addition to review against the 19 technical requirements categories as discussed previous section, the evaluation template included a tool or methodology overview and other information about the applicability, assessment process features and deployment considerations for the tool or methodology. Applicability aspects discussed were target organization, scope of assessment, level of coverage for cyber security, and target audience for results. Assessment process features discussed were data collection approach, detailed operator guidance, form of results, and support for an ongoing assessment program. Deployment considerations discussed were learning curve, cost, schedule, installed base, and vendor support.

A notation of “Reviewed” in the Evaluation File column means that the evaluation output was reviewed by the developer of the tool or method. The content of evaluations that were not reviewed represents the opinion of the SCySAG working group members who performed the evaluation work, based on available information at the time the evaluation took place. For the CS2SAT tool, the working group provided feedback to the CS2SAT team, and the file containing that feedback is also referenced in the table.

Table 2 – Tools/Methodologies for Evaluation

Sector	Tools/Methodologies	Evaluation Filename
Electric Power	Although NERC CIP 002-009 itself is neither a tool nor a methodology, the group reviewed it using the methodology/tool template (and incorporated information from it into the template during this process as noted above). The group did see a demonstration from a questionnaire framework vendor who had worked with a major process control vendor to incorporate the NERC CIP content into their framework to create a self assessment tool. Likewise, NERC CIP content has been incorporated into the CS2SAT tool. These standards are found at: *http://www.nerc.com/page.php?cid=2|20*	*NERC_CIP_ 002-009_ Assessment.doc*
	The group reviewed the following resources from this sector, but found that these did not address self assessment for control system cyber security.	
	• IT Recovery Plan for Electric Co-ops (NRECA) *https://crn.cooperative.com/Resources/SoftwareDownloads/ITRecoveryPlanning.htm*	NA
	• Method(s) from NERC's "Risk Assessment Methodologies for Use in the Electric Utility Industry" *http://www.esisac.com/library-assessments.htm*	NA
Water/Wastewater	• RAM-W (Risk Assessment Methodology – Water) *http://www.sandia.gov/ram/RAMW.htm*	*RAM-W_ v2.0.doc*
	• VSAT (Vulnerability Self Assessment Tool) *http://www.vsatusers.net/index.html*	*VSAT_assessment_v2.0.doc*
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/*	*CIDX_Assessment_v2.0.doc*
	• PHAWorks (product of Primatech) *http://www.primatech.com/software/phaworks5.htm*	*PHAWorks_Summary_v1.0.doc (Reviewed)*
Refining and Petrochemical	• API Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries	*API_SVA_Assessment_v2.0.doc*
	• API 1164 Appendices A and B self-questionnaires on SCADA security Both available for purchase from *www.techstreet.com* and other vendors	*API1164_060802.doc*
	• Methodology/tool of Industry Participant (proprietary)	*IndustryTool_evaluation_v03.doc*
Cross-sector	• DHS NCSD cyber security questionnaire (mid-level)	*NCSD_Cyber_VA_Questionnaire_summary_v2.0.doc*
	• DHS CS2SAT (Control System Self Assessment Tool, detail level, uncustomized version) *http://www.loftyperch.com/cs2sat.html*	*CS2SAT-Summary_V05.doc* *CS2SAT_feedback_v04.doc*

Overview of Tools/Methodologies

In this section we summarize the results of the tool and method evaluations.

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 about these resources.

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 control system characteristics in particular, even though they may include control systems as part of the assessment scope.

Table 3 – Tools/Methodologies Overview

Name	Type	Sector	Focus
RAM-W	Methodology	Water/Wastewater	Risk assessment and management; both physical and cyber risk; not control system specific
API Security Vulnerability Analysis Methodology	Methodology	Refining and Petrochemical	Risk assessment and management; both physical and cyber risk; not control system specific
VSAT	Software Tool	Water/Wastewater	Risk assessment and management; both physical and cyber risk; includes some high level control system specific assets and threats
CS2SAT	Software Tool	Cross-sector	Cyber vulnerability assessment; unique to control systems
DHS NCSD Questionnaire	Questionnaire	Cross-sector	Cyber vulnerability assessment; not control system 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 control system unique elements
Industry Participant Internal Tool	Spreadsheet tool	Refining and Petrochemical	Cyber vulnerability assessment; unique to control systems
CIDX Guidance for Addressing Cyber Security in the Chemical Industry Version 3.0 – Appendix 1 Self Assessment Questions	Questionnaire	Chemical	Cyber vulnerability assessment; some control system 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 control system 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. An area of particular clarity offered by this tool was its in-depth coverage and security policy related to modems for remote sites. The cross-sector CS2SAT software tool developed by DHS/INL supports cyber self-assessment specifically for control systems. Versions of this tool customized for the water and electric power sectors have also 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 the American Petroleum Institute (API) respectively. The DHS questionnaire does not address control system unique characteristics; rather it covers cyber security at a generic level. The CIDX Appendix questionnaire addresses some control system 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 control 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 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 control system 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.

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

Identifying Gaps

After the group carried out its evaluations of individual methodologies and tools, it next used these evaluations as the input data to classify control system unique characteristics as well covered or poorly covered by these existing tools/methods in specific sectors, and over all sectors. This was accomplished using a spreadsheet matrix showing all methods/tools evaluated, against the list of control system unique characteristics. The filename for this document is *Methodology-Tools_Analysis_v07.xls*.

This analysis showed that control system unique requirements in the following areas were generally well covered by methods and tools, for all sectors analyzed (Oil and Gas, Chemical, Electric Power, and Water/Wastewater):

- Importance of Cyber Security in Business
- Scope of the Cyber Security Management System
- Security Policy
- Personnel Security
- Organizational Security
- Compliance

The following areas had good coverage for a few sectors:

- Physical and Environmental Security
- Access Control
- Information and Document Management

The following were not well covered for any sector:

- Identifying Vulnerabilities
- Risk Identification, Classification and Assessment
- Risk Management and Implementation
- Incident Planning and Response
- Infrastructure-Related Operations and Change Management
- Staff Training and Security Awareness
- System Development and Maintenance
- Monitoring and Reviewing the Cyber Security Management System
- Maintaining and Implementing Improvements

Prioritizing Gaps

At the working group meeting at PCSF Spring 2007, the group presented a view of the gaps identified based on the spreadsheet analysis just described, and requested attendees at the session to prioritize these gaps in terms of the need to develop methodology/tool requirements and implementations of these requirements to fill them. A detailed report from this session can be found in the document *Atlanta_notes_030607_v04.doc*. An unanticipated result of this event was that even though attendees worked individually in teams by sector and were asked to create priorities in this light, *all sectors* had the following three requirements areas in their top five list:

- Identifying Vulnerabilities
- Risk Identification, Classification and Assessment
- Staff Training and Security Awareness

Further, Access Control appeared in the top five for three out of four of the sector teams. The working group felt that the CS2SAT tool evolution would naturally address Identifying Vulnerabilities and Access Control. In light of this view, SCySAG provided feedback to the CS2SAT team concerning gaps in these two areas (see the document *CS2SAT_feedback_v04.doc*). The working group then decided to focus its final efforts on the Risk Identification and Assessment, and Staff Training and Security Awareness.

At an earlier working group meeting at PCSF Spring 2006, before the working group had completed their detailed gap analysis matrix, the group had asked the roughly 40 attendees to vote on where they felt the gaps lie – and 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 the document *Spring_workshop_notes_v2.0.doc*.

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

Next Steps

To conclude its working group activities, SCySAG will host a panel discussion at the 2008 PCSIC to address the requirements areas of risk assessment and training. The purpose of the panel is validate these unmet needs, discuss what steps should be taken to address them, and consider who within the community is best positioned to take these steps.

This session will also consider whether there would be potential for a useful transition of SCySAG techniques and activity to other organization(s). This would support ongoing evaluation of available process control cyber self assessment methodologies and tools, toward one or more of the goals defined by SCySAG.

APPENDIX A

Working Group Notes and Analysis Outputs

Atlanta Workshop Notes and Results *(Atlanta_notes_030607_v04.doc)* **A-2**

Cyber Self Assessment Resource List *(VA_Tool_list_v4.0.xls)* **A-7**

Methodology and Tools Analysis *(Methodology-Tools_analysis_V07.xls)* **A-20**

Spring 2006 Workshop Notes *(Spring_workshop_notes_v2.0.doc)* **A-36**

Spring 2006 Workshop Votes *(VAT_template_table_votes_v2.0.doc)* **A-38**

Tool Evaluation Template *(Tool_evaluation_template_v3.0.doc)* **A-48**

Summary:
Approximately 50 people attended the SCySAG Workshop at the PCSF meeting in Atlanta March 6 2007, to prioritize unmet cyber security self assessment requirement needs. The attendees had a diverse background from industrial control end-users, IT, control system vendors, consultants/service providers, and cyber security researchers. The workshop attendees were very engaged and provided excellent discussion and feedback.

The objective of the workshop was to identify the 3 to 5 highest priority cyber security assessment requirement gaps for each sector. The attendees documented the reasoning behind the prioritization. SCySAG will use the results to identify and prioritize next steps. The sectors considered were:

- Water and wastewater
- Oil & gas, refining, chemicals
- Electric power
- Cross-sector

The attendees were asked to prioritize the categories in the document posted in the SCySAG working group library called "Methodology and Tools Evaluation Template," specifically those 11 among the full set of 18 that the working group indicated to the attendees were not fully covered by existing tools and methodologies for all sectors. The seven items indicated as fully covered in all sectors were "Importance of Cyber Security in Business," "Scope of Cyber Security Management System," "Security Policy," "Organizational Security," "Personnel Security," and "Compliance."

There was a remarkable consistency across the sectors with regards to the requirements and their priorities as shown in Table 1. (Note that the electricity sector group provided its top four categories but did not explicitly prioritize these with respect to each other.) Table 2 documents each sector's rationale for its prioritization. The working group noted a clear focus since three categories appeared in all four sector lists, and two categories appeared in three of the four sector lists, as shown in bold in Table 1.

SCySAG's next steps will be to focus on the top four categories, (19.1, 11.2, 7.2, & 14.2) that are, per the attendees, both high value and need additional work. (10.2, Infrastructure-Related Operations and Change Management was also a focus, but was prioritized lower than Access Control by the two sectors who selected both.) The SCySAG team later discussed and concluded that the top four categories are split into 2 groups. The first group (19.1 & 11.2) may well be covered with current version of CS^2SAT. SCySAG will review CS^2SAT coverage and provide feedback to the CS^2SAT development team on ways to strengthen the tool. The second group (7.2 & 14.2) was felt to be only partially covered by existing tools. For this group, SCySAG will review related documents including the draft ISO 19791 and then identify what is needed. A potential approach for defining the unmet tool/methodology requirements includes proposing a workshop with subject experts and end-users to define these requirements.

Results:

Sector Priority	Water/ Waste Water	Electric Power	Oil & Gas	Cross Sector
1	19.1 Identifying Vulnerabilities	19.1 Identifying Vulnerabilities	19.1 Identifying Vulnerabilities 7.2 Risk Identification, Classification, and Assessment	19.1 Identifying Vulnerabilities
2	11.2 Access Control	11.2 Access Control	11.2 Access Control	7.2 Risk Identification, Classification, and Assessment
3	7.2 Risk Identification, Classification, and Assessment	7.2 Risk Identification, Classification, and Assessment	10.2 Infrastructure-Related Operations & Change Management	10.2 Infrastructure-Related Operations & Change Management
4	14.2 Staff Training & Security Awareness	14.2 Staff Training & Security Awareness	14.2 Staff Training & Security Awareness	9.2 Incident Planning & Response
5	10.2 Infrastructure-Related Operations & Change Management		13.2 System Development & Maintenance	14.2 Staff Training & Security Awareness

Table 1: Category Priority for Each Sector

Reasoning behind the prioritization:

Sector	Prioritization Rationale
Water/Wastewater	
19.1	1. Data security, accessibility, availability & integrity for operations and business decision-making are critical. 2. The core of your business is exposed to a variety of threats.
11.2	1. Authorization & authentication of users is the second line of defense for critical operation. 2. Because a high percentage of threats are internal.
7.2	1. Without understanding overall risk, it is impossible to apply effective prevention & migration policies & actions. 2. Guidance on prioritization of assets needed by utilities. 3. Defining criticality of parameters – i.e., business continuity.
14.2	1. People are the weakest link. 2. Organizational change is difficult & often overlooked. 3. No method in place to transfer knowledge to those who work with/operate the control systems/SCADA.
10.2	1. Need stress live system versus mock/test system. 2. Change management procedures are needed.

Sector	Prioritization Rationale
	3. Ensuring system stability.
Electric Power	
19.1	1. Tool can maintain a large list of vulnerabilities, difficult for an individual entity to track. 2. Urgency because of NERC CIP standards requirement for vulnerability assessment.
11.2	1. Access control – has many piece parts, procedural as well as technical, very important, heart of security. 2. Access control requirements are called out by NERC standard.
7.2	1. Risk is foundational to all other efforts regarding cyber security. 2. Risk based assessment called out by NERC standard.
14.2	1. The best procedures will not be effective if not trained properly at all levels. 2. Need methods to track training, what to train, how to encapsulate information for training, how to determine whether training has been effective. 3. Training requirement is part of NERC standard.
Oil & Gas	
19.1 & 7.2	1. Topology of Network – How does it affect vulnerabilities? Securing one area, but opening up another 2. Probability of risk and how to assess 3. Open systems/IP not secure/wireless access is problematic. 4. Safety issues in general not addressed, especially in retrofits – see 13.2
11.2	1. Identity management (separate from authentication and authorization). 2. Third part access (process management) How do we manage contractor access (including modems, LAN, etc.)
10.2	1. Virus updates and scan schedule. 2. Patch management & process of managing it 3. Test environment for testing of patches, etc. 4. Vendor requirements for patches and virus updates
14.2	1. Training 2. Awareness program – for items such as social engineering. Make security more second nature. Business security has had this type of programs.
13.2	1. Technology risk assessment 2. Safety analysis or re-analysis When or at what point do you do a re-assessment. How big a change before a safety audit or review? 3. Possibly add a new section – Safety Section
Cross Sector	
19.1	1. You need to know your vulnerabilities & weaknesses 2. HAZOP for system!
7.2	1. Identification of what you want to protect (asset)

Sector	Prioritization Rationale
	2. Prioritization of mitigation against possible consequence.
10.2	1. You need to know who is doing what, where, & the possible impact. 2. Not forgotten or degrades 3. Continuity of ops overlap: recovery point 4. Consistency for management & verification
9.2	1. Have a plan and stick to the plan 2. Slow to react to incident 3. Going to cost money or HSE
14.2	With out security awareness the other process like change management & incident management aren't going to be successful.

Table 2: Reasoning Underlying the Prioritization

SCySAG Team Attendees:

- Brian Isle
- Carol Muehrcke
- Candace Sands
- Mark Morgen
- Ron Melton

Workshop process

- Started with five tables: water and waste water; power/electric; chemicals, refining & petrochemical; oil & gas; and cross-sector. (The chemical sector had few representatives and so merged with the cross-sector table.)
- Each table has:
    - Facilitator
    - Copies of the matrix with white, gray, and green spaces denoted
    - Large colored "stickies"
    - Black markers
- Each table will:
    - Discuss and prioritize the un-met requirements for their sector
    - Capture the reasoning behind the prioritization
- Summarize the results
    - A spokes person for each table will:
        - Briefly describe the priorities
        - Briefly describe reasoning for prioritization
        - Update the master chart with priorities

SCySAG Next Steps:

- Summarize workshop and post to the working group library.
- Focus on the top four categories, (19.1, 11.2, 7.2, & 14.2)
- Review CS^2SAT coverage and provide feedback to the CS^2SAT development team related to requirements for self assessment of vulnerabilities and access control

- Review related documents including the draft ISO 19791TR "Security Assessment of Operational Systems" and then identify what is needed. Initiate discussion with PCSF about the possibility of them funding a workshop with subject experts and end-users to define possible user requirements for self assessment in the areas of risk and training. Develop concept for such a workshop.

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
1	API 1164 Guideline	Security Guidelines for the Petroleum Industry	API	Oil & Gas	Report	Guideline	http://api-ec.api.org/filelibrary/Security_Guidance2003.pdf
1	API 1164 Pipeline SCADA Security	Pipeline SCADA Security Standard	API	Oil & Gas	Controls	Standard	http://www.techstreet.com/cgi-bin/detail?product_id=1175186
1	Assessment Primer	Cyber Security: Business and Control Systems Assessment Primer	NCSD		Controls	Report	
1	AuditWorks	AUDITWorks project with (CYBER.APW) using a simple cyber security checklist	PrimaTech	Chemical	Controls	VA	http://www.primatech.com/index.html
1	CIP Comparison	Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator	Digital Bond		Controls	Report	www.digitalbond.com/dale_peterson/presentations.htm
1	CS2SAT	The software supporting the “Self-Assessment Tool” is designed for a desktop or laptop application and will be disseminated via compact disc to the control system community after the current pilot testing efforts are completed near the end of 2006. The tool guides the user through a questionnaire (based on the topology of the control system network) and generates a report highlighting areas for recommended improvement and/or change in cyber security practices. The questionnaire is based on industry standards, guidance, and requirements for securing control systems against cyber attacks.	INL	critical infrastructure	Controls	VA	
1	DOE 21 Steps	Very simple but a great start.	DOE	Power	Controls	Report	http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
1	Guidance for Addressing Cybersecurity in the Chemical Sector Version 2.1	Guidance for Addressing Cybersecurity in the Chemical Sector Version 2.1	CIDX	Chemical	Controls	Report	http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm
1	ISA 99.00.02	Establishing a Manufacturing and Control Systems Security Program. Gives practical guidance and direction on how to establish the business case for a security program and how to design the program to meet business needs.	ISA	Manufacturing & Control Systems	Controls	Standard	http://www.isa.org/template.cfm?template=customsource/isa/sp99/manufacturing.cfm
1	ISA 99.00.03	Operating a Manufacturing and Control Systems Security Program. Describes how a security program is operated after it is designed and implemented.	ISA	Manufacturing & Control Systems	Controls	Standard	http://www.isa.org/template.cfm?template=customsource/isa/sp99/manufacturing.cfm
1	ISA 99.00.04	Specific Security Requirements for Manufacturing and Control Systems. Defines the characteristics of Manufacturing and Control Systems that differentiate them from other Information Technology systems from a security point of view. Based on these characteristics, establishes the security requirements that are unique to this class of system.	ISA	Manufacturing & Control Systems	Controls	Standard	http://www.isa.org/template.cfm?template=customsource/isa/sp99/manufacturing.cfm
1	ISA-99.00.01	Manufacturing and Control Systems Security Part 1: Concepts, Models and Terminology	ISA	Manufacturing & Control Systems	Controls	Standard	http://www.isa.org/template.cfm?template=customsource/isa/sp99/manufacturing.cfm
1	ISA-TR99.00.02-2004		Instrumentation Systems and Automation Society	Chemical	Controls	Standard	http://www.isa.org/Template.cfm?Section=Find_Standards&template=/Ecommerce/ProductDisplay.cfm&ProductID=7380

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
1	ISO 15408	Common Criteria for Information Technology Security Evaluation	ISO	IT	IT		http://www.iso15408.net/
1	ISO 17799	ISO security standard for IT	ISO	IT	IT	Standard	http://www.computersecuritynow.com/presentation/ http://webstore.ansi.org/ansidocstore/product.asp?sku=ISO%2FIEC+17799%3A2005&source=google&adgroup=17799&keyword=iso%2017799&gclid=COja-cOx3IMCFRaBOAodoVeI_A
1	NERC 1300 CIP 002 - 009	Cyber Security Power Generation and Transmission	NERC	Power	Controls	Standard	
1	PHAWorks	PHAWorks with (CSVA SB TEMPLATE.wpw) to conduct a Cyber Security Vulnerability Analysis (SVA) using PrimaTech scenario-based method	PrimaTech	Chemical	Controls	VA	http://www.primatech.com/index.html
1	RAM-W	Risk Assessment Methodology for Water	Sandia/ AwwaRF, EPA	Dams	Physical	VA	http://www.sandia.gov/ram/index.htm
1	Reference Architecture	A Reference Model for Control and Automation Systems in Electric Power	Sandia	Controls	Controls	Report	
1	Report on the Evaluation of Cybersecurity Self-assessment Tools and Methods Version 1.0	Report on the Evaluation of Cybersecurity Self-assessment Tools and Methods Version 1.0	CIDX	Chemical	Controls	Report	http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm
1	System Protection Profile	This SPP has been developed as part of the Process Control Security Requirements Forum (PCSRF) sponsored by the National Institute of Standards and Technology (NIST).	NIST	Cyber	Controls	Report	http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.doc

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
1	VSAT	The Vulnerability Self Assessment Tool (VSAT™) software was developed to support water and wastewater utility vulnerability assessments using a qualitative risk assessment methodology. VSAT™ software is available, free of charge, for wastewater utilities (VSATwastewater™), drinking water utilities (VSATwater™), and for utilities providing both services (VSATwater/wastewater™).	Scientech	Water/Waste Water	Controls	va	http://www.vsatusers.net/
2	AGA Report No. 12	Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan	American Gas Association	Gas	Controls	Report	http://www.aga.org/
2	API RP 70	Security for Offshore Oil and Natural Gas Operations	API	Oil & Gas	Controls	Report	http://www.techstreet.com/cgi-bin/detail?product_id=1085161
2	API SVA-2004	Security Vulnerability Assessment Methodology for Petroleum and Petrochemical Industry	API	Petroleum/ Petrochem	Controls	VA	http://api-ec.api.org/filelibrary/SVA_2003.pdf http://www.techstreet.com/cgi-bin/detail?product_id=1183425
2	Connectivity	Security Guidelines for the Electricity Sector: Control System — Business Network Electronic Connectivity	NERC	Power	Controls	Report	http://www.esisac.com/publicdocs/Guides/SecGuide_ElectronicSec_BOTapprvd3may05.pdf
2	Cybersecurity Vulnerability Assessment, Version 2.0	Cybersecurity Vulnerability Assessment, Version 2.0	CIDX	Chemical	Controls	Report	http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm
2	INEEL/EXT-04-02428	A comparison of electrical sector cyber security standards	US-CERT		Controls	Report	http://www.us-cert.gov/control_systems/pdf/electrical_comp1004.pdf
2	INEEL/EXT-04-02462	A comparison of cyber security standards devloped by the oil and gas segment	US-CERT		Controls	Report	www.us-cert.gov/control_systems/pdf/oil_ga

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
2	INL/EXT-06-11464	Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research	TSWG/INL	Critical infrastructure	Physical	Report	www.pcsforum.org/library/files/1159904563
2	ISO 27001	Information technology - Security techniques - Information security management systems - Requirements	ISO	IT	IT	Report	http://webstore.ansi.org/ansidocstore/product.asp?sku=ISO%2FIEC+27001%3A2005 http://www.27000.org/
2	IT Recovery Plan for Electric Co-ops	CD-based tool developed by NRECA and CRN for the Electric Co-op IT and E&O staff. The tool contains a full suite of templates to build the IT recovery plan.	NRECA and CRN	Power	IT	VA	https://crn.cooperative.com/Resources/SoftwareDownloads/ITRecoveryPlanning.htm
2	NERC 1200	Urgent Action Standard	NERC	Power	Controls	Standard	http://www.esisac.com/publicdocs/Workshop_CybSecStd/CybSecStdWS_ExecBrief_WJ.ppt#398,4,NERC Compliance Enforcement Program http://www.esisac.com/publicdocs/Workshop_CybSecStd/CybSecStdWS_Access-red_LN.ppt
2	NIST 800-12	An Introduction to Computer Security:The NIST Handbook	NIST	IT	IT	Report	http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
2	NIST 800-13	Telecommunication Security Guidelines for TMN (Telecommunication Management Network)	NIST	Telecommunication	Network Management	Report	http://csrc.nist.gov/publications/nistpubs/800-13/800-13.wpd
2	NIST 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems	NIST	IT	IT	Report	http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
2	NIST 800-18	Guide for Developing Security Plans for Information Technology Systems	NIST	IT	IT	Report	http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
2	Nist 800-82	Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security	NIST	Industrial control systems	Controls	Report	http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf
2	NIST SP 800-53	Recommended Security Controls for Federal Information Systems	NIST	Federal Information Systems	IT	Report	http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf
2	NIST SP 800-53	Annex 1: Consolidated Security Controls-Low Baseline (.pdf) (includes updates through 6/17/05)	NIST	Federal Information Systems	IT	Report	http://csrc.nist.gov/publications/nistpubs/800-53/800-53-annex1.pdf
2	NIST SP 800-53	Annex 2: Consolidated Security Controls-Moderate Baseline (.pdf) (includes updates through 6/17/05)	NIST	Federal Information Systems	IT	Report	http://csrc.nist.gov/publications/nistpubs/800-53/800-53-annex2.pdf
2	NIST SP 800-53	Annex 3: Consolidated Security Controls-High Baseline (.pdf) (includes updates through 6/17/05)	NIST	Federal Information Systems	IT	Report	http://csrc.nist.gov/publications/nistpubs/800-53/800-53-annex3.pdf
2	NIST SP-800-30	Risk Management Guide for Information Technology Systems	NIST	IT	IT	Guideline	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
2	Patch Management	Security Guidelines for the Electricity Sector: Patch Management for Control Systems	NERC	Power	Controls	Report	
2	RAMCAP	Select questions (~21) are used by owners/operators to assess the fundamental cyber vulnerabilities of their facility. Collaborating with the Chemical, LNG, and Oil/Petro/Gas Sectors to integrate cyber concepts and portions of the cyber VA questionnaire into their respective RAMCAP SVAs	ASME	control related sectors	Controls	VA	http://www.bfrl.nist.gov/PSSIWG/presentations/NSTCPresentation_0917041.pdf
2	SCADA Security Survey Instrument		NISCC		Controls	VA	http://www.niscc.gov.uk/niscc/index-en.html

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
2	Study of Vulnerability Assessments”	Vulnerability Assessment Methodologies Report	DHS Office for Domestic Preparedness	Critical infrastructure	Physical	Report	www.ojp.usdoj.gov/odp/docs/vam**report**.pd
2	Summary of Control System Security Standards	A Summary of Control System Security Standards Activities in the Energy Sector	DOE	Power	Controls	Report	www.inl.gov/scada/publications/d/a_summary_of_control_system_security_standards_activities_in_the_energy_sector.pdf
3	@Risk		Palisade Corp.	Chemical	Controls	VA	
3	Assessment and Remediation of Vulnerabilities in SCADA and Process Control Systems	Assessment and Remediation of Vulnerabilities in SCADA and Process Control Systems	ISI	Power	Controls	VA	
3	Buddy System		Countermeasures Corp.	Chemical	Controls	VA	
3	CARVER	Criticality Accessibility Recuperability Vulnerability Effect Recognizability	Special Operations Forces	Military	Physical	VA	
3	CARVER2	CARVER2 infrastructure analysis system gives those people responsible for the identification and analysis of critical infrastructure (CI) a method of comparing dissimilar types of CI using the same standards.	National Infrastructure Institute	critical infrastructure	Physical	VA	http://www.ni2cie.org/CARVER2.asp
3	Common Vulnerability Scoring System	The NIAC commissioned this project to propose an open and universal vulnerability scoring system to address and solve these shortcomings, with the ultimate goal of promoting a common understanding of vulnerabilities and their impact.	National Infrastructure Advisory Council	Critical Infrastructure	All	Report	www.first.org/cvss/

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
3	CORAS		European Union funded	Chemical	Controls	VA	
3	CR	Complete questionnaire is used by the Federal CR Team to assess a facility's cyber security posture and provide guidance on protective measures. Working with the Risk Management Division and the Chemical Sector to develop and integrate entire questionnaire into the CR process	FEMA	community relations	Physical	VA	http://www.floridadisaster.org/BRM/SOPs/crsop.pdf
3	CRAMM		Insight Engineering	Chemical	Controls	VA	
3	Crystal Ball		Decisioneering	Chemical	Controls	VA	
3	CS SESAT	Control System Security Exposure Self Assessment Tool	WERF/AwwaRF	Water	Controls	VA	
3	CVAM	Community Vulnerability Analysis Methodology Community Characterization	Sandia	Community	Physical	VA	
3	CVAT	NOAA Community Vulnerability Assessment Tool (CVAT)	NOAA	Community	Physical	VA	
3	D(M)SHARPP	Mission demographics symbolism history accessibility recognizability population proximity	United States Air Force	Military	Physical	VA	
3	DATA Interactive		TreeAge Software, Inc.	Chemical	Controls	VA	
3	DecisionPro		Vanguard Software Corporation	Chemical	Controls	VA	
3	Enterprise Risk Assessor		Methodware Ltd.	Chemical	Controls	VA	
3	Firewall Deployment	Good Practice Guide on Firewall Deployment for SCADA and Process Control	NISCC		Controls	Report	http://www.niscc.gov.uk/niscc/docs/re-20050223-00157.pdf

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
3	FSIVA	Full Spectrum Integrated Vulnerability Assessment	US National Guard	Industrial	Physical	VA	
3	Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites	Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites	American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS®)	Petrochem	Physical	Guideline	http://www.amazon.com/gp/product/081690877X/102-1907016-3154533?v=glance&n=283155 http://www.isa.org/PrinterTemplate.cfm?Section=View_by_Title2&Template=/Ecommerce/ProductDisplay.cfm&ProductID=7546
3	IEC 60870-6	Telecontrol Equipment and Systems Part 6: Telecontrol protocols compatible with ISO standards and ITU-T recommendations, (Also referred to as IEC standard TASE.2)					
3	IEC 61850-SER,	Communication Networks and Systems in Substations					
3	IEC 62351-1	Data and Communications Security, Introduction, DRAFT					
3	IEC 62443	Security for Industrial Process Measurement and Control, DRAFT					
3	IEC TC57 WG15, draft standard 62351	- develop recommendations for a develop recommendations for a comprehensive security process	IEC		Controls	Standard	
3	IEC TR 62210	Power system control and associated communications - Data and communication security, May 2003					
3	IEEE Std 1402-2000	IEEE Guide for Electric Power Substation Physical and Electronic Security, January 30, 2000					
3	Info Security Governance - A Call to Action	appendix D has a nice assessment tool		IT	IT	VA	http://www.cyberpartnership.org/InfoSecGov4_04.pdf

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
3	JSIVA	Joint Staff Integrated Vulnerability Assessments	JSIVA, DoD Joint Staff	Military	Physical	VA	
3	MARION		Coopers & Lybrand {U.K.}	Chemical	Controls	VA	
3	MI CIP Assessment						
3	MORDA	Mission Oriented Risk and Design Analysis	United States National Security Agency	IT	IT	VA	
3	MS-ISAC Assessment						
3	NIAC_CVSS_FinalRpt_12-2-04	NIAC Common Vulnerability Scoring System	NIAC		IT	Report	http://www.dhs.gov/interweb/assetlibrary/NIAC_CVSS_FinalRpt_12-2-04.pdf
3	NISCC	SCADA Security Survey Instrument			Controls	VA	http://www.niscc.gov.uk/niscc/index-en.html
3	NIST Security Consensus Operational Readiness Evaluation (SCORE)	IT but a nice start for developing OS hardening checklists.	NIST	IT	IT	VA	http://www.sans.org/score/
3	NSA IAM						
3	PAIR-PM	Pxxx_Assessment Infrastructure Risk - Program Management	Setracon, Inc.	Comunity	Physical	VA	

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
3	PIVA	Port Integrated Vulnerability Assessment	US Navy	Military	Physical	VA	
3	Process Control System Security Technical Risk Assessment: Analysis of Problem Domain	This research report describes an initial approach to PCS technical security risk assessment,	I3P	Oil & Gas	Controls	Report	http://www.thei3p.org/about/researchreport3r1.pdf
3	RAM-C	Risk Assessment Methodology for Communities	Sandia	Communities	Physical	VA	http://www.sandia.gov/ram/index.htm
3	RAMCAP	Risk Analysis and Management for Critical Asset Protection	American Society of Mechanical Engineers	Industry	Physical	VA	
3	RAM-CF	Risk Assessment Methodology for Chemicals	Sandia, DOE, EPA, Chem stakeholders	Chemical facilities	Physical	VA	http://www.sandia.gov/ram/index.htm
3	RAM-D	Risk Assessment Methodology for Dams	Sandia	Dams	Physical	VA	http://www.sandia.gov/ram/index.htm
3	RAM-E	Risk Assessment Methodology for pipelines, electric powr generation, in development	Sandia, DOE, Gas associations	Power, Oil & Gas	Physical	VA	http://www.sandia.gov/ram/index.htm

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
3	RAM-P	Risk Assessment Methodology for Prisons	Sandia, DoJ	Prisons	Physical	VA	http://www.sandia.gov/ram/index.htm
3	RAM-T	Risk Assessment Methodology for [electric] Transmission	Sandia	Power Transmission	Physical	VA	http://www.sandia.gov/ram/index.htm
3	Roadmap	Roadmap to Secure Control Systems in the Energy Sector	DOE	Power	Controls	Report	http://www.controlsystemsroadmap.net/pdfs/roadmap.pdf
3	SAS 70						
3	Security Capabilities Profile for Industrial Control Systems	NIST PCSRF – "Security Capabilities Profile for Industrial Control Systems"	NIST		Controls	Report	
3	SOCMA Model	**SOCMA Chemical Site SVA Model & Manual**	SOCMA	Chemical	Controls	VA	http://www.socma.org/Products/VulnerabilityAnalysis.htm
3	SVA methodology and model		Synthetic Organic Chemical Manufacturers	Chemical	Controls	VA	

Priority	Method/Tool/Stnd	Description	Organization	Primary Domain	Main Focus	Type	URL
3	VA	Vulnerability Assessment Methodology Electric Power Industry	DOE	Power	Physical	VA	http://www.esisac.com/publicdocs/assessment_methods/VA.pdf
3	VFA	Vulnerability Function Allocation	Honeywell	Regions	Physical	VA	
3	ViSAT	Complete questionnaire is used by owners/operators to assess their facility's cyber security posture. Developed by the Transportation Security Administration to assist	TSA	Transportation	Physical	VA	http://www.tsa.gov/public/interapp/tsa_policy/tsa_policy_0045.xml

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
1.0 Importance of Cyber Security in Business													
1.1 General	Critical business processes (CBP) and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed						CBP addressed in the user guide as scenarios. Business processes or high level policies are not covered in the tool. Questions are asked as to whether the policies exist, but make no judgement as to the accuracy, completeness, or effectiveness of the policy	General questions related to dependencies and adequate redunancy are included. Questions related to consequence characterisztion are included in the questionaire.	Partial: -Appendix B calls for acceptance of residual risk and for analysis of consequences if SCADA system is completely taken over -System used in this standard divides applications into consequence categories and applies different controls to each. Hence there is an implicit "acceptance" of the risk of certain consequences.	This is where most of the questions are targeted. Consequences, etc. are not specifically addressed.	Partial:No general discussion of this, however, it is implicit in the requirement to meet this standard and in requirement for risk-based identification of critical cyber assets in (002).	The critical business process (CBP) is defined by the utility as a primary mission. The RAM-W does allow for consequence prioritization and it documents a fault tree of possible breaches and outcomes. However, the interdependencies between CBPand IT systems are not covered. RAM-W is a methodology.	Yes, in the sense that use of this tool will achieve this – so the tool does not ask the user whether they already have it.
1.2 SCADA Specific	-Model lists of typical critical control system assets for entities in specific sector -Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage -Guidance on assessing consequences of incidents typical in a particular sector					Determine if the CS2SAT, 1164, and NERC coverage is applicable to other sectors Assignment: ???	Very extensive coverage of components in a control system down to the field device level. Initial questions deal with consequences of injury, death, damage to the environment and infrastructure and are used to assess the assurance level of the site or plant. No sector specific guidance on assessing consequences. The generic version does not identify incidents.	SCADA specific issues are not addressed in the questionaire.	Yes: -Divides applications into categories depending upon specific consequences of their malfunction, and requirements are levied by category of application -Specific dollar amounts for financial loss, loss of human life, environmental impact inconvenience (odor) are part of categorization	There is no specific coverage of SCADA.	Partial: Yes, gives examples to consider in determining assets critical to bulk power system and defines critical cyber assets as those essential to these critical assets. Also gives examples and other criteria that define critical cyber assets. Yes, Consequence of interest is lack of reliability of the bulk power system. No, does not give numerical targets but requires risk-based determination of critical assets. (all 002) Also requires that electronic security perimeter protection cyber assets be protected (005)	Very Limited - for Water Sector only. Helps identify lists of critical assets – fault tree diagrams include facility assets siuch as plant and pump station control systems. Has model definitions of criticality including level of consequence and incorporating types of consequences, by asset category.	Limited - for Water Sector only. Has model lists of critical assets – mentions plant and pump station control systems. Has model definitions of criticality including level of consequence and incorporating types of consequences, by asset category. Does not have guidance on making a particular consequence level assignment.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
2.0 Scope of the Cyber Security Management System (CSMS)													
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered						Scope is set by the standard set(s) selected by the team to base the assessment. Currently, in the generic cross-sector version, NERC, NIST, and ISO standards are included and overlap in some areas. Some processes/areas may not be covered by one or more of the included standards. For the most complete coverage and scope, select and use all available standards. Some overlap will occur, but more complete coverage will result.	Questions specific to the statement of the scope of the cyber security management system is not addressed in the questionaire.	Partial: -Scope is not explicitly stated, but applications, interfaces and equipment involved is required to be enumerated in Appendix B	This is covered generally.	Yes, Standard applies to critical cyber assets, and entity must list what they are (002).	Limited: Some Cyber Security elements are addressed in section 4.6: Cyber-Threat.	Limited: The tool does not specifically address processes and organizations covered. The scope of the analysis of the tool is determined by the assets and threats selected for analysis.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
2.2 SCADA Specific	• Guidance on list of systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on list of interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.						Covers all aspects of a control system - from the Internet/Firewall/Router level to field devices. Limited coverage on non-control system and generic or business IT components. Yes, there is guidence on devices that span to the business or Internet level, including vendors, contractors, and/or remote users.	SCADA specific issues are not addressed in the questionaire.	Yes: -SCADA unique components and interfaces are listed in the Appendix B template security plan	No specific coverage of SCADA or process control systems.	Partial, gives examples of critical cyber assets unique to this sector (002) and calls out dial-up access to electronic security perimeter. (005)	Limited. RAM-W does include a separate SCADA VA section.	Partial: Since has default modifiable model list of critical assets under control systems, including Server, PLCs, RDUs, CRTs and instrumentation interface. Does not detail potential interfaces.
3.0 Security Policy													
3.1 General	Existence of documented security policy						Choice of several standards: NERC CIP-002 thru CIP 009, NIST SP800-53, and ISO/IEC 15408 v3.1 Assurance Rqmts.	General questions related to security policy documentation are included.	Main standard calls for documented security policy but this is not mentioned in this manner in the Appendices.	General coverage	Yes(003)	The RAM-W requires a thorough review of all security policies in existence with the utility.	No Not intended to audit cyber security management system, but rather to assess risk
3.2 SCADA Specific	-Areas of policy that may differ for IT systems and control systems -Elements needed in control system policy					Determine if CS2SAT's underlying security policy is adequate. Assignment: ???	Designed specifially for control system / SCADA assessments.	SCADA specific issues are not addressed in the questionaire.	Yes: - The Appendix A checklist itself could function as a security policy. It is quite specific. -Appendix B has template security plan	No specific coverage	Partial, states policy must address requirements of this standard (003)	The review of documentation covers all technology-related policies, for both IT and SCADA.	Limited: focuses on countermeasures rather than policy.
4.0 Organizational Security													

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber						Assumes there is an entity within the organization that sets policys for the network and control system. Depending on standard selected, several questions address the organizational security policies.	Questions related specifically to the overall security of organization are not addressed in the questionaire.	No	General coverage	Yes	There is a statement of importance regarding organization security, but no specific guildelines.	No. Not intended to audit cyber security management system, but rather to assess risk
4.2 SCADA Specific	- Individual exists with clear definition of responsibility for control system cyber security -Clear coordination point between business side IT cyber security and control system security -Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security					Need to review the NERC & 1164 to determine the depth of coverage and if the requirnments can be applied to the other sectors. Assignment: ???	Focusses on SCADA systems. Deals with interfaces or links between business and SCADA. Several questions focus on the policies and procedures in place for responsibilities.	SCADA specific issues are not addressed in the questionaire.	Partial: - Sample security plan Appendix B states that there will be a SCADA cyber security manager, lists responsibilities of this individual, and suggests they meet Cyber Security Team across the organization - IT is considered untrusted, coordination not covered - Not necessarily specific point of responsibility for physical/cyber, however many requirements in appendices touch both areas	No specific coverage	Partial: Senior manager must be designated to insure compliance with standard (which includes physical and cyber aspects) and approve exceptions to policy (003)	NOT COVERED.	No. Although it should be noted that the tool allows physical countermeasures to be applied to cyber threats.
5.0 Personnel Security													
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.						Yes - These topics are addressed depending on the security standards selected.	General questions related to personnel screening and personnel security responsibilities are included.		General coverage	Partial, requires personnel risk assessment (004). Does not require in general that job responsibilites for security be clearly defined, other than at executive level in (003)		Partial. Library does contain employee and vendor screening countermeasures. Job responsibilities not addressed.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
5.2 SCADA Specific	- Guidance on defining job criticality for control system personnel - Guidance on security responsibilities of control room and other control system personnel. - Third party contracts related to control room have provisions for cyber security.					Need to determine depth of coverage in CS2SAT. Determine applicability to other sectors. Assignment: ???	These topics are addressed depending on the security standards selected as basis for assessment.	SCADA specific issues are not addressed in the questionaire.	Partial: -States that responsibilities of information owner should be documented, several of these are noted in Apendix A -Appendix B calls out users, managers and administrators as jobs for which cyber security responsibilities should be defined -Appendix B covers responsibilities of cyber security manager -Third parties – Appendix A covers contracts but not background screening – however, main standard says to consider screening for third parties with access to confidential and restricted information, or physical access to computer rooms,	No specific coverage	Partial, Personnel risk assessment required for those with cyber access or unescorted physical access to critical cyber assets. Some guidance given on what type of screening to do. Does not discuss cyber responsibilities of personnel, or mention contracts, but does require risk assessment for service contractors and vendors. (004)	Very limited guidance provided.	Not specific to SCADA, however screening countermeasures noted above could be applied by the user to address a SCADA threat.
6.0 Physical and Environmental Security													
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage						Most devices have questions dealing with these types of issues.	Some general questions related to physical threats are included. Questions related to a power outage threat are not included.	Yes	General coverage	Yes: Does not call out speciic threats but requires physical security perimeter around critical cyber assets. (006) Requires procedures for disposing of critical cyber assets (007)	The RAM-W has two sections (6 & 7) that address physical protection (PPS) and operational security. Common PPS hardware items are provided for consideration.	Partial: Threat library includes theft of documents, employee cutting power. Note that there is a physical access countermeasure in the library related to IT. Not completely covered, focus is on IT threats to IT systems and physical threats to physical systems.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
6.2 SCADA Specific	Considers trade-offs between safety and security (e.g. safety implications of locking up control system elements vs. 24 X 7 guard)					Determine if the requirnments in 1164 are applicable to other sectors. Assignment: ???	Contains questions related to physical security of devices, but no outside the device type security such as guards.	SCADA specific issues are not addressed in the questionaire.	Yes: - Provides specific guidelines for physical security of systems based on criticality - Appendix B calls for physical security audit of remote sites that may have access to SCADA network	No	Partial:Requires 24X7 control of physical security perimeter, lists choice of protection methods. Requires notification on failed access, logging of accesses and testing of system. (007) Template could add "guidance on level of physical protection required for cyber assets"	Hardware for phyiscal protection is discussed (i.e., door locks) but no specific considerations of safety vs. security is contained in the methodology.	No. The "Disadvantages" information given for the IT physical access countermeasure would be a good place to discuss this topic. This was not discussed in the library version reviewed.
7.0 Risk Identification, Classification, and Assessment													
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified						Questions assess the organizations policies and procedures on how often Risks are evaluated and assessed. Does not deal with specific threat profiles.	General questions related to identification of threats, vulnerabilities and consequences are included. Questions related to probability of occurance are not covered.	Yes	Very general coverage, no specific approach provided	YesCalls out in general for a risk based assessment to determine cyber assets (002) Requires vulnerability analysis (005)	Yes. The methodology guides the assessment team in defining mission objectives, priorities, priority facilities and assets, identifying threats, system effectiveness, and consequences to determine risks/ vulnerabilities. Basic design basis threat are identified.	Yes Has built in template threat heirarchy of specific threats and categories of threats, which is customizable. There are 30 IT threats included. Does not specifically look at vulnerabilities as an item in and of themselves, but rather looks at level of vulnerability to a specific threat given the existing countermeasures, in what is called the "baseline analysis." Probability of occurance of attempt is a user input.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
7.2 SCADA Specific	- Topology? Both physical and schematic of control system network - Guidance for enumerating critical assets - Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) - Guidance for assessing probability of control system security incidents - Guidance on assessing consequences - Consider: interdependencies and cascading effects - Identify critical cyber assets (Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able					Determine the depth of coverage in 1164, NERC and water. Is the requirnments applicable to Chem? Assignment: ???	Allows users to create and edit to system/component diagram to baseassessment. Provides several templates. Does not specifically enumerate threats or the probablility of one incident vs. another. Initial questions direct the user to state the consequences of a "worse-case" scenario due to a compromised control system. The tool does not address specific threat assessment. Users must define their worse case scenario and assign consequences to define the Security Assurance Level required.	SCADA specific issues are not addressed in the questionaire.	Partial: - Required to document all applications in some categories and their location - Requires all connections into network be documented - Topology required under Appendix B template security plan, gives details of what exactly to document and lists of interfaces and components - Provides categories of application by defining levels of consequence, but does not cover how to determine consequences - Appendix B gives example of how to rank interfaces and equipment types by "value." It also suggests to rank these by impact and susceptibility. It also	No coverage	Partial, Guidance on defining critical cyber assets (002)	Importance of having network documentation / diagrams is repeatedly emphasized. A basic list of network and control system hardware is needed to applied the methodology. The utility is encouraged to complete the list with any site-specific hardware. Cost assignment is done, and a pair-wise relationship for both threat matrices: the "benefit to threat" matrix and the "degree of vulnerability" matrix.	Partial Has model list of SCADA system critical assets. Does consider temporal aspect of criticality in default definitions for levels of criticality – how long will be out of service. If network diagrams or characteristics of adversaries are used to set the factors that determine vulnerability or criticality, this would be done outside of the tool.
8.0 Risk Management and Implementation													
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.						Questions assess whether these types of strategies are evaluated and reviewed. Most consquences are quanitified in dollar amounts, loss of life or injury, or other impacts.	Questions specific to risk mitigation strategies are not addressed in the questionaire.	Yes	Very general coverage, no specific approach provided	No, Not a general requirement, but see next line.	A risk equation is provided. A process to determine the values to determine relative risk is well defined. The methodology also provides a process to evaluate and select mitigation strategies for identified risks, based on cost and consequences, and to accept residual risk.	Yes, in the sense that the tool itself supports a process to trade off annual cost with risk reduction units, examining various scenarios for adding countermeasures.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
8.2 SCADA Specific	Process in place for management to select mitigation strategies and accept residual risks related to control systems					Determine the depth of coverage in 1164, NERC and water. Is the requirnments applicable to Chem? Assignment: ???	Tool does identify these issues and has questions relating to strategies.	SCADA specific issues are not addressed in the questionaire.	Partial: -Process mentioned specifically in Appendix B but not elaborated upon - process covered in API SVA -Some specific strategies are suggested in Appendix B as follows. -Appendix B calls for physical backups to mitigate some specific consequences in the event of unauthorized control of the SCADA system -Appendix B calls for consideration of removal of interfaces, hardening of components, based on risk level	No coverage	Partial, not a general requirement, but in many specific areas calls out the fact that some technical controls may not be feasible, and requires acceptance of risk and mitigations. (e.g. shutting down ports, use of strong passwords, applying antivirus etc.)	There is some guidance for determining the criticality of each SCADA components and related hardware and a method to evaluate critical assets in a pairwise matrix.	Yes, in the sense that SCADA systems are one type of asset being considered by this tool, and see remarks above.
9.0 Incident Planning and Response													
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.						These topics are addressed depending on the security standards selected.	General questions related to monitoring and incident response are included.	Yes	Very general coverage	Yes(008)	A method for threat identification is provided. It does not provide procedures to develop a system for tracking and documenting incidents. Templates (2) are provided for risk assessment of an insider and outside threats.	The tool focuses on countermeasures in response specifically to water crisis such as boil water alerts, announcements, not cyber events specifically.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
9.2 SCADA Specific	-Integration with organization's existing crisis management processes -Possibly unique reporting requirements for control system incidents -Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?					Determine the depth of coverage in 1164 & NERC. Is the requirnments applicable to Chem and water? Assignment: ???	Yes - These topics are addressed depending on the security standards selected	SCADA specific issues are not addressed in the questionaire.	Partial: -Integration not discussed, not normally related -Refers to company incident reporting standards -States that information owners must determine how long their data can be unavailable in backup/recovery procedure -Regulations require backup system and backup control center, so not covered here	Process control system is mentioned but only in the context of reporting incidents.	Partial, requires procedure for reporting to the Electric Sector ISAC	NOT COVERED.	NOT COVERED.
10.0 Infrastructure-Related Operations and Change Management													
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application						Yes - These topics are addressed depending on the security standards selected.	General questions related to configuration management of cyber systems are included.	Yes	Very general coverage	Yes: Change management system required (003) Requires access points to electronic security perimeter to have minimum ports and services open. (005) Requires that ports on hosts to have only necessarily services and ports open. (007) Requires patch management program (007) Requires anti-virus (007) Requires backup/restore process and testing (009)	NOT COVERED.	Partial Antivirus and configuration management are mentioned as countermeasures

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
10.2 SCADA Specific	-Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes -Consider that servers running control system components may have different profile of required services than business servers -Periodic testing of security controls for high risk control environments					Determine the depth of coverage in 1164 & NERC. Is the requirnments applicable to Chem and water? Assignment: ???	Yes - Depending on the security standards selected, H43these topics are addressed . Some support of this in the ISO/IEC questions. Questions relate to independent testing and verification. NERC standards contain items like patch management and avti virus updates and need for testing.	SCADA specific issues are not addressed in the questionaire.	Partial: -States that backup/restore tests not be done in production environment -Appendix B gives examples of functions that may be removed from computers in the SCADA system -Specifically prohibits "leaving in" emergency changes that circumvented normal procedures -Requires documentation of emergency changes -Calls for separation of roles of programmer and implementer – or mitigating controls as exception -Patching called out -Antivirus called out in Appendix B, specific systems to consider called out in main standard -Backup/test already regulated in other		Partial, points out that testing should minimize impact on production environment (007) Points out that may not be technically feasible to close some unused ports, apply patches or use antivirus, and requests acceptance of risk and mitigating controls (007)	NOT COVERED.	NOT COVERED.
11.0 Access Control													
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties						Assessment questions seem to target this type of policy. There are many questions relating to accounts, authentication, and authorization.	General questions related to identification, authentication and logical access control are included.	Yes	Detailed procedure and policy questions	Yes, requires close management of access to critical cyber assets (004, 007), mentions "need to know" (007)	NOT COVERED. There is a general emphasis on reviewing all existing IT policies and procedures.	NOT COVERED.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
11.2 SCADA Specific	Consideration of: -Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service -Different policies for administrative vs. control access to control system elements -Different policies for access to critical operator functions and platforms hosting critical components -Use of stronger authentication for remote access -Use of team passwords -Common instances in which “weaker” cyber security mechanisms in control system					Determine the depth of coverage in CS2SAT, 1164 & NERC. Is the requirnments applicable to water? Assignment: ???	Yes - Depending on the security standards selected, these topics are addressed . These topics are covered in more than one and some overlap may occur.	SCADA specific issues are not addressed in the questionaire.	Yes: -Unique user IDs required for role-based except for the console, calls this out explicitly -Requires specific password expirations and strengths for general users, adminstrators, service accounts -Provides guideline of logoff after 30 minutes activity. Main standard notes that this is for non-operations applications only. -PC’s/laptops and servers have screen savers -30 minutes account lockout is required on 5 attempts in all cases -Requires two factor authentication for remote access -Case for access to information must be made to information owner -Requires authentication for	Some specific questions but no recommendations	Partial, Calls for special procedures related to use of shared passwords (007), Points out use of strong passwords may not be technically feasible (007)	NOT COVERED.	NOT COVERED.
12.0 Information and Document Management													
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..						Yes - Depending on the security standards selected, these topics are addressed .	Questions specifcally related to managing security of information and documentation are not included.	Yes	General questions	Yes(003)	NOT COVERED.	Yes. Information classification procedure is a countermeasure in the library.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
12.2 SCADA Specific	Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities, etc..					Determine if 1164 and NERC are applicable to Chem & Water. Assignment: ???	SCADA/control system specific devices are included on the component diagram. Questions are then automatically generated for the components.	SCADA specific issues are not addressed in the questionaire.	Yes: -Calls out three levels, public, restricted, confidential. Specific documents are named in both appendices A and B, and in the main body of the standard – the examples in the Appendix B and the main standard are SCADA specific. -Throughout Appendix A, requirements for storage, transmission, destruction, etc. are based on the level of the data.	No coverage	Yes, provides list of examples of specific sensitive documents (003)	NOT COVERED.	NOT COVERED.
13.0 System Development and Maintenance													
13.1 General	Security requirements developed and tested for new or changed systems						Management of change relating to Security is covered in the NERC standards	Questions specifcally related to ensuring appropriate security for new or changed systems are not included.	Yes	Targeted to application development more than system development	Yes	NOT COVERED. However, RAM-W does comment on the necessity for long-term follow-up and review of risk for new (or upgraded) system components.	NOT COVERED.
13.2 SCADA Specific	Integration of security and safety analyses fo new or changed systems					Determine the depth of coverage of 1164 and see if coverage is adequate for other sectors. Assignment: ???	See 13.1	SCADA specific issues are not addressed in the questionaire.	Partial: -Requirements by criticality of system -Calls out separate development/test environment – or mitigating controls as exception -Integration with safety covered under DOT regulations.	This is mentioned, but generally, not specific to process control systems	No	NOT COVERED.	NOT COVERED.
14.0 Staff Training and Security Awareness													

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates						Yes	General questions related to staff training and security awareness are included.	Yes: -Not in Appendix A checklist but Appendix B and main standard	General coverage	Yes	NOT COVERED.	Partial Security awareness program is in countermeasure library
14.2 SCADA Specific	-Awareness and training for control system personnel tailored to specific needs -Guidance on training needs for control system personnel					Determine the depth of coverage of CS2SAT and see if coverage is adequate for other sectors. Assignment: ??	Yes - Depending on the security standards selected, these topics are addressed .	SCADA specific issues are not addressed in the questionaire.	Partial: -A few specific training items mentioned –protection of data about the control system and protection of passwords	The need for job specific training is included.	Partial, does say training applies to those with cyber access or unescorted physical access to critical assets, and it applies to service vendors and contractors. Says should be appropriate for roles and responsibilities, and R2.2 (004) gives short list of topics to train on.	NOT COVERED.	NOT COVERED.
15.0 Compliance													
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements						Yes - Depending on the security standards selected, these topics are addressed .	Questions specifcally related to auditing security policies and procedures are not included.	Yes	Very general coverage	Yes, standard requires specific areas be audited, and NERC will audit overall compliance to standard, each standard has a compliance section. Required to assess compliance to information protection program annually (003)	It is suggested that a long-term iteration follow the initial M69assessment process; recommends annual reviews.	Partial tgechnical audits of process, systems and networks is a countermeasure in the library.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
15.2 SCADA Specific	-Audit for control systems takes into account complementary physical and cyber mitigators -Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems -Audit for control systems does not use automated scans where these might disable equipment -Audit includes configurations of firewalls that protect control system network					Determine the depth of coverage of CS2SAT and 1164 and see if applicable to Chem and water/waste Assignment: ???	Yes - These topics are addressed depending on the security standards selected.	SCADA specific issues are not addressed in the questionaire.	Yes: -Requires review of rccords of access against confidential and classified information monthly -Appendix B suggests periodic audit of documented system and risk analyses, as well as periodic self-assessment (e.g. against Appendix A questionnaire,which covers most listed elements in left column here) and vulnerability assessment	No coverage specific to process control systems	Partial, do include required ports to be open on electronic security perimeter as part of vulnerability analysis requirements. (005)	NOT COVERED.	NOT COVERED.
16. Business Continuity Plan													
17.0 Monitoring and Reviewing the CSMS													
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.						Yes - These topics are addressed depending on the security standards selected.	General questions related to monitoring and incident response are included.	Yes	Very general coverage of this topic	Partial Required controls are defined by the standard, assessment of needed changes is after vulnerability analysis. Requires where feasible, monitoring of accesses to electronic security perimeter (005) Requires monitoring, alerting, logging and review of security events. (007)	NOT COVERED.	No The tool provides a risk assessment given an organization's posture at a given point in time.

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
17.2 SCADA Specific	-Guidance how to monitor the control system threat environment, and specific threats to a given sector -Types of attacks that are reported/detectable against control system provides adequate data for this analysis?					Determine the depth of coverage by CS2SAT, 1164, and NERC. See if applicable to Chem and Water/waste. Assignment: ??	Included as part of ISO/IEC standard questions.	SCADA specific issues are not addressed in the questionaire.	Partial: -No guidance on how to monitor threats -Specifies a minimum set of events to be collected (unauthorized access, account add, etc.) -Other regulations contain additional requirements on monitoring of logs	Nothing specific to SCADA / process control	Partial, requires concept of electronic security perimeter as noted above Acknowledges that electronic access monitoring may not always be technially feasible. (005)	NOT COVERED.	NOT COVERED.
18.0 Maintaining and Implementing Improvements													
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.						Several questions address the need/existence of ongoing reassessment of policies and procedures. None relate to it specifically	Questions specifcally related to an ongoing process for continuous update the CSMS, based on industry benchmarking or availability of new technologies are not included.	Appendix B mentions that self assessments should include tracking new technologies.	Very general coverage of this topic	No	It is suggested that a long-term iteration follow the initial assessment process; recommends annual reviews.	No The tool provides a risk assessment given an organization's posture at a given point in time.
18.2 SCADA Specific	-Sources for benchmark information for sector -Sources for tracking SCADA security technology					Determine if updates of standards will flow down thru CS2SAT to meet this requirnment. Assignment: ??	Standards used currently are NERC, NIST SP800-53, and ISO/IEC 15408 v3.1. Standard sources for questions relating to the SCADA devices is unclear. Need to contact Battelle?	SCADA specific issues are not addressed in the questionaire.	No	No specific coverage for SCADA / process control	No	NOT COVERED.	NOT COVERED.
19.0 Identifying Vulnerabilities													

Category	Topic	Sector Coverage Covered (Green) Partialy covered (Gray) Uncovered (White)				Notes and assignments	CS2SAT	NCSD Cyber VA Questionnaire	American Petroleum Institute Standard 1164	Guidance for Addressing Cyber Security in the Chemical Industry	NERC Critical Infrastructure Protection Standards 002-009	RAM-W Summary	Vulnerability Self Assessment Tool (VSAT)
		Oil & Gas	Chem	Elect pwr	Water Sector		Cross-sector/ Critical Infrastructure	Cross-sector	Oil & Gas	Chemical	Electric Power	Water & Wastewater	Water & Wastewwater
19.1 SCADA Specific	-Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP): Field I/O, Status Data Field Points, System Status Data, Exported Data, Imported Data, External (e.g. regional) control signals, Control systems programs and configuration. -Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: Flow of imported data, Flow of exported data, External control					Determibe the depth of coverage of CS2SAT, 1164, NERC, and VSAT. See if applicable to Chem. Assignment: ???	Every device type is treated very similarly. A core set of questions for most devices consist of Audit, User Data Protection, Identification and Authentication, Security Management, Protection of the System, and System Access. Depending on the device type, other questions pertinent to the device are included. Coverage of devices is extensive, but on a generic, non-vendor specific basis. Devices covered range from the entire IT type devices (firewall, server, switch, router, etc.) to control system devices (RTU, PLC, HMI, etc.). Some topics are		Partial: -Protection of confidential and classified data during transmission called out -Encryption of stored data that is classified or confidential called out -States that no single point of failure can take out a system classified as mission critical -Types of interfaces listed in Appendix B template security plan -Types of components listed in Appendix B -Appendix B discusses looking at configuration of native security features in SCADA applications -For certain categories of data access audit log must include who, what data, action and when -Appendix B discusses 24 hr a day	No coverage of vulnerability assessment.	Partial: Requires review of all connections to electronic security perimeter (ESP) Requires review for default accounts, passwords and network management community strings related to ESP(005) and critical cyber assets (007) Mentions dial-up connections. Requires electronic perimeter protection of critical cyber assets. (005) Requires electronic perimeter protection of critical cyber assets.	NOT COVERED.	Partial: Encrypted traffic is in the countermeasure library. Threat in the library is very general – hacker compromises confidentiality and/or integrity of the SCADA system. Lists firewall as countermeasure in library. Relationship to control systems not mentioned.

PCSF SCySAG Working Group – June 7, 2006

The workshop opened with a review of the agenda and expectations for the outcome. The workshop agenda:

- Review the agenda and expectations for the outcome
- Introductions
- Brief overview of SCySAG objectives, process, template and basis of comparison, and status
- Review cyber self-assessment tool/method summaries completed by the group
- Comparison of this effort with DHS/INL CSSAT efforts (Control System Self Assessment Tool)
- Identify and prioritize requirement gaps
- Discuss the results and identify issues

The overall workshop objectives were:
1. Identify cyber security SCADA self assessment requirement gaps and do first order prioritization of the gaps. The definition of requirements gap; Unique characteristic of SCADA cyber security that is not adequately covered by existing self assessment tools
2. Define plan forward

The SCySAG core team was introduced and then the attendees did a quick introduction with emphasis on special SCADA cyber expertise they might have. Nearly 40 people attended the workshop.

Brian Isle gave a brief overview of SCySAG objectives, process, template and basis of comparison, and status of the project. The template is the group's working list of SCADA unique cyber security characteristics.

Rebecca Freeman and Candace Sands provided an overview of the RAM-W methodology as compared to the summary template. Carol Muehrcke reviewed the summary of the VSAT tool. Julio Rodriquez provided an overview of DHS' Control System Security program and the CSSAT tool development. Ron Melton provided a summary of the CSSAT coverage as compared to the summary template. They noted that CSSAT would not be mandated, but was expected to be made available to asset owners through sector organizations. The summary templates described above will be posted to the PCSF SCySAG web page.

The workshop attendees provided their input on which of the SCADA-unique requirements needed additional attention based on the three summaries and their own understanding of the SCADA cyber issues.

The main workshop meeting was adjourned. The core team discussed the next steps for the SCySAG team. The actions include:

1. Complete and solidify the group's search for and evaluation of tools and methodologies against the template
2. This includes a review the CSSAT requirements and questionnaire documents to further understand the framework coverage.
3. Update the CSSAT template summary based on the latest understanding.
4. Provide responsible organizations with the opportunity to comment on our evaluations.
5. Clarify and vet the prioritization of the requirement gaps once evaluation work is solidified.
6. Coordinate with the DHS/INL team to share results.
7. Continue to identify end-users for the SCySAG results.
8. Adopt a numbering system for the summary template to enable easier comparison.

Conclusions:

1. The template that describes the SCADA-unique characteristics was in general accepted. Two additional subtopics were included: configuration management of process applications, and sector-specific processes to determine critical assets. It was also suggested to clarify that the scope includes physical protection of cyber assets.
2. It was generally agreed that no single tool was likely to cover all elements of the template, that an asset owner likely would use a number of tools.
3. The top six requirements topics needing additional study based on the initial prioritization during the workshop (note: these are likely to change as the team investigates):
    a. Risk identification, classification, and assessment – 10
    b. Importance of cyber security in business – 7
    c. Security policy – 6
    d. Personnel security 5
    e. Incident planning and response – 5
    f. Identifying vulnerabilities - 5

The SCySAG core team includes:

- Martin Stoddard, P.E.
  Pacific Northwest National Laboratory
  martin.stoddard@pnl.gov
- Mark C. Morgen
  3M - Optical Systems Division IT
  mark.morgen@mmm.com
- Carol Muehrcke
  Cyber Defense Agency, LLC
  cmuehrcke@cyberdefenseagency.com
- Matt Earley
  Decisive Analytics Corporation
  matt.earley@dac.us
- Rebecca Freeman
  Charleston (SC) Water System
  freemanjr@charlestoncpw.com
- Candace Sands
  EMA
  csands@ema-inc.com
- Brian Isle
  Adventium Labs
  brian.isle@adventiumlabs.org
- Cliff Glantz
  Pacific Northwest National Laboratory cliff.glantz@pnl.gov

Notes from the Workshop on 6/7/06

Methodology/Tool Analysis Template
SCADA Cyber Self Assessment Working Group, Process Control System Forum

Draft 7/27/06
Requirements Requiring Additional Effort
Authors: Brian Isle, Carol Muehrcke
Rev. 07/27/06

This document records (in the right column) the vote by the June 7 2006 attendees at the SCADA cyber self assessment working group meeting at PCSF in La Jolla CA – voting on which areas they felt were of most importance for emphasis by the group. It also records comments on specific areas of concern, and the improvements we made to the coverage topics based on these comments.

Technical Coverage

Category	***Topic***	***Vote, comments, and topic changes incorporated***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	
1.2 Control system Specific	• Methodology for determining and model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	7 Votes Comments: Need additional work to translate business processes to risk management Based on comments, added "methodology" in first bullet
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment,	0 Votes This area is critical – and – is well covered in CSSAT

Category	*Topic*	*Vote, comments, and topic changes incorporated*
	real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	
3.0 Security Policy		
3.1 General	Existence of documented security policy	
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Best practices for juridiction and relationship between overall cyber policy, IT policy and control systems policy • Elements needed in control system policy	6 votes Additional clarification of the relationship between IT and controls dept - who has jurisdiction? - policy coverage for IT and controls dept - there is a general lack of knowledge about each other, they view each other as untrusted partners - how do we determine the 60% that is common and the 40% that is different - note: API 1164 covers some of these issues in it's sample policy in an Appendix Additional coverage for training (esp. topics like social engineering)? Additional coverage on traceability and audit? - added second bullet based on these comments
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	
4.2 SCADA specific	• Individual exists with clear definition of responsibility for	0 Votes Well covered in CSSAT

Category	*Topic*	*Vote, comments, and topic changes incorporated*
	control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on specific kind of screening needed for control-related jobs (most likely sector specific) • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	5 Votes Additional coverage on background screening specific to job needs "fitness for duty" - added second bullet based on comments
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	
6.2 SCADA specific	• Considers trade-offs between safety and security (e.g. safety implications of locking up control system elements vs. 24 X 7 guard) • Considers interaction of physical and cyber controls (locked door or guard vs. stronger authentication)	3 Votes Comments: - Wholistic view of security Shed light on the interaction of physical and cyber - Ref: API 1123 (or 1113) Control Room Design - Added second bullet based on comments
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	
7.2 SCADA Specific	• Both physical and schematic topology of control system network	10 Votes Additional coverage of:

Category	***Topic***	***Vote, comments, and topic changes incorporated***
	are documented • Guidance for enumerating critical assets at next level down from 1.2 • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Identify critical cyber assets (Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?) • See last entry in table for SCADA specific vulnerability assessment elements.	- Adversary goals and threats Interdependency (internal & external) - Cyber compatible probability models - Critical assets based on an architectual view point Ref: IEEE 37.1, 12 criteria
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems • Need a business case to justify the improvements (requires to be modeled by sector) • Best practices such as reference architectures to help support business case • Risk management tied to the business drivers and process – making tradeoffs.	4 Votes Additional coverage for: - Design trades - Reference architecture - Best practices Risk management tied to the business practices - added bullets 2-4 based on comments
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response,	

Category	***Topic***	***Vote, comments, and topic changes incorporated***
	communications at time of incident, reporting, post mortem.	
9.2 SCADA specific	• Cyber response plan for process control systems, considering continuity, mitigation and recovery • Integration with organization's existing crisis and emergency management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	5 Votes Additional coverage on: - Cyber response plannng - Continuity and recovery - Regulatory and certification issues - Emergency management systems - Mitigation of effects - added first bullet and added emergency process to second bullet based on these comments
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments • Integration and change management for controls applications (note: only DOT for pipeline include a regulation for change management) • Change and configuration management for control programs	3 Votes Well covered in CSSAT Comments: - configuration management of process application including redundant systems - management of control programs - added fourth and fifth bullet based on comments
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	
11.2 SCADA specific	Consideration of: • Best practices for role definition in process control environment, may	1 Vote Well covered in CSSAT Comments:

Category	*Topic*	*Vote, comments, and topic changes incorporated*
	be specific to sector • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation	-Role-based password management -Means to prevent colusion (e.g. two man rule) -Host-policy vs control-policy -Define levels of authentification - added first bullet based on comments
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	1 Vote Process control systems/programs constantly change – need better config management (this was moved to 10.0 above)
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems	2 Votes Comments: - this is not in CSSAT - e.g. regression testing for

Category	*Topic*	*Vote, comments, and topic changes incorporated*
		cyber security - training
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	1 Votes - Strengthen the link from training to policy. - This is well covered in CSSAT
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	4 Votes This is pretty well covered in CSSAT
16.0 Business Continuity Plan	(Propose not to review this topic)	Move this to Incident recovery and response
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed in near real time to determine need for response, and historically to determine needed changes to the CSMS.	
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for near real time and historical	0 Votes Additional coverage on the traceability from policy to implementation - Additional coverage on people and system audit logs was mentioned under

Category	*Topic*	*Vote, comments, and topic changes incorporated*
	analysis?	compliance, moved here, so may have more votes - Based on comments, added need for real time analysis as part of this category, as distinguished from historical analysis.
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	4 Votes Issues include - entropy takes over - lack of resources
19.0 Identifying Vulnerabilities		

19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP)
	  o Field I/O
	  o Status Data Field Points
	  o System Status Data
	  o Historical Status Data
	  o Exported Data
	  o Imported Data
	  o External (e.g. regional) control signals
	  o Control systems programs and configuration
	• Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are:
	  o Flow of imported data
	  o Flow of exported data
	  o External control signals
	  o Access to historical status data
	  o Other business system
		5 Votes
		- This is well covered in CSSAT
		- need to review this list to make sure it covers control systems in general

Category	*Topic*	*Vote, comments, and topic changes incorporated*
	interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access • Protection from compromise and interruption: o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS	

Category	***Topic***	***Vote, comments, and topic changes incorporated***
	protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

Methodology or Tool Analysis

In the questions below, substitute the term "methodology" if you are assessing a methodology and not a tool.

1. **Overview:** *Provide a brief overview of the tool.*

zzzz

Applicability

2. **Target Organization:** *What kinds of organizations would find this tool useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.*

Zzzzz

3. **Scope of Assessment:** *Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.*

Zzzz

4. **Coverage of Cyber Security:** *How focused is the tool on cyber security? Does the tool provide in depth guidance for assessing cyber security? By "in depth guidance" we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.*

zzzz

5. **Target Audience for Results:** *What is the intended audience for the results – upper management, middle management, systems experts?*

zzzz

Assessment Process Features

6. **Data Collection Approach:** *What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?*

zzzzz

7. **Detailed Operator Guidance:** *Does the tool or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?*

zzzzz

8. **Results:** *Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool produce specific recommendations?*

Zzzzz

9. **Support for Ongoing Assessment Program:** *What features does the tool have to assist in effectively performing periodic assessments? For example, can the tool compare assessments done at different times? Does the tool support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?*

Zzzzzz

Deployment Considerations

10. **Learning curve:** *Is the tool intuitive and easy to use?*

Zzzzzz

11. **Cost:** *What is the total cost of the tool, including the purchase price and the cost of implementation and operation?*

Zzzzz

12. **Schedule:** *How long does it normally take to carry out an assessment using this tool?*

Zzzzzz

13. **Technical requirements:** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).*

Zzzzz

14. **Installed base:** *How widespread is the use of the tool – in what sectors?*

Zzzzz

15. Vendor support: *What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?*

Zzzzzz

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)
- NERC Critical Infrastructure Protection Standards 002-009 (found at http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection)
- NERC Top Ten Vulnerabilities of Control Systems and Their Associated Mitigations 2006 (found at ftp://www.nerc.com/pub/sys/all_updl/cip/Top_10_vuln_2006_16mar2006_ss.pdf)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen).

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.
- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.

Methodology/Tool Analysis
Process Control System Forum
SCADA Cyber Self Assessment Working Group
Template rev. 11/28/06

- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	***Topic***	***Comments on Coverage***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	zzzzz
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	zzzzz
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	zzzzz
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	zzzzz
3.0 Security Policy		

Methodology/Tool Analysis
Process Control System Forum
SCADA Cyber Self Assessment Working Group
Template rev. 11/28/06

Category	***Topic***	***Comments on Coverage***
3.1 General	Existence of documented security policy	zzzzzz
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	zzzzzz
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	zzzz
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	zzzzz
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	zzzzz
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on type of screening required based on job criticality • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	zzzzzz
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	zzzzz
6.2 SCADA	• Guidance on level of physical	zzzzzz

Category	***Topic***	***Comments on Coverage***
specific	protection required for various types of cyber assets • Consider safety implications of locking up control system elements (e.g. vs. 24 X 7 guard)	
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	zzzzzz
7.2 SCADA Specific	• Diagram of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process? • See last entry in table for SCADA specific vulnerability assessment elements.	zzzzz
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	zzzzz
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	zzzzzz
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response,	zzzz

Category	***Topic***	***Comments on Coverage***
	communications at time of incident, reporting, post mortem.	
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	Zzzz
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	zzzz
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	zzzz
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	zzzz
11.2 SCADA specific	Consideration of: • Network and host access • Identifying control network access points • Removal of default accounts and passwords • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status	zzzz

Category	***Topic***	***Comments on Coverage***
	information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation • Agreements on access control policies in vendor RFPs	
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	zzzz
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	zzzz
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	zzzz
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems • RFPs include security requirements for vendors • Vendor agreements include interval	zzzzz

Category	***Topic***	***Comments on Coverage***
	for security patch updates • Separation of runtime and development environments • Designs consider risks of connections between business and control networks • Designs consider risk of control and non-control traffic on same network	
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	zzzzz
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	zzzz
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	zzzz
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	zzzzz
16.0 Business Continuity Plan	(Propose not to review this topic)	
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	zzzzz

Category	***Topic***	***Comments on Coverage***
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	zzzzz
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	zzzzz
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	zzzz
19.0 Identifying Vulnerabilities		
19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP) o Field I/O o Status Data Field Points o System Status Data o Historical Status Data o Exported Data o Imported Data o External (e.g. regional) control signals o Control systems programs and configuration • Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: o Flow of imported data o Flow of exported data o External control signals o Access to historical status data o Other business system	zzzzz

Category	*Topic*	*Comments on Coverage*
	interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access • Protection from compromise and interruption: o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs	

Category	***Topic***	***Comments on Coverage***
	o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

APPENDIX B

Tool and Methodology Reports

CS2SAT Summary Review *(CS2SAT-Summary_V05.doc)* **B-2**
CS2SAT Feedback *(CS2SAT_feedback_v04.doc)* **B-20**
PHAWorks Summary *(PHAWorks_Summary_v1.0.doc)* **B-23**
CIDX Assessment *(CIDX_Assessment_v2.0.doc)* **B-36**
Assessment of NERC CIP 002-009 Using Template *(NERC_CIP_002-009_Assessment.doc)* **B-47**
Methodology Tool Analysis for API SVA *(API_SVA_Assessment_v2.0.doc)* **B-59**
Evaluation of API 1164 Appendices A and B *(API1164_060802.doc)* **B-62**
NCSD Cyber VA Questionnaire Summary (Ver. 2) *(NCSD_Cyber_VA_Questionnaire_summary_v2.0.doc)* **B-77**
VSAT Assessment *(VSAT_assessment_v2.0.doc)* **B-90**
RAMCAP Assessment Synopsis *(RAMCAP_Assessment_Synopsis_v2.0.doc)* **B-102**
RAM-W *(RAM-W_v2.0.doc)* **B-107**
Industry Tool Evauation *(IndustryTool_evaluation_v03.doc)* **B-120**

Methodology/Tool Analysis
Process Control System Forum
SCADA Cyber Self Assessment Working Group
Template rev. 10/25/06

Draft
Tool name: CS^{2}SAT (generic version)
Review author(s): Mark C. Morgen 3M / Garill Coles PNNL / Mary S. Hester Intelligent System Solutions
Review date: June 2007
External reviewer and date: N/A

Tool Analysis

1. **Overview:** *Provide a brief overview of the tool.*

CS2SAT is cyber security assessment tool funded by the Department of Homeland Security to provide owner/operators with a tool to examine the vulnerability of control system cyber security implementation. The tool is a desktop application that walks users through a series of questions that assesses security posture and provides recommendation for areas identified as potential weaknesses. The tool can be used by a business to baseline their security exposure and track progress through periodic reassessment. The tool is based on recognized standards, and gaps can also be identified through standards-specific reporting to help identify potential problems with compliance.

Applicability

2. **Target Organization:** *What kinds of organizations would find this tool useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.*

The target for the tool is utilities and other public service type organizations that support critical infrastructure for the United States. These would include waste water facilities, electrical power utilities, water treatment plants, etc. Currently, CS^{2}SAT is specifically targeted for use by the water and wastewater industries, although an Electric Power module is currently being developed. The architecture of the tool makes adaptation for other energy sectors possible. Embedded applicable cyber security standards would need to be changed to reflect the energy sector being assessed. This evaluation was conducted using a generic version that could be used by a more general industry or business.

The tool seems to be targeted at a broad range of users in terms of organizations and their experience as the tool is very easy to use.

3. **Scope of Assessment:** *Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.*

The scope of the assessment can be plant or site coverage. The tool is targeted at Cyber Security for industrial control systems and deals mainly with the network and control devices on the network. The coverage is basically devoted to the physical devices and the policies and procedures revolving around them. It does not deal with physical security, general security policy, threat assessment, etc.

- The tool is non-threat specific (i.e tool does not differentiate between a terrorism, accident, criminal, or inadvertent threat or incident). The tool only addresses threat to the extent that the embedded standards address them (e.g. human intentional, human non-intentional, natural and environmental).
- The assessment questionnaire is organized by system element (e.g. system, database server, HMI, PLC, firewall, and application server) and covers Life Cycle Support, Independent Testing, User documentation, Contingency Plans, Security Event Monitoring, Physical Security, Security Policy, Data Protection and Privacy, and Identification and Authentication.

4. **Coverage of Cyber Security:** *How focused is the tool on cyber security? Does the tool provide in depth guidance for assessing cyber security? By "in depth guidance" we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.*

The tool is designed with Control System Cyber Security as its main focus. It provides in-depth guidance on recommendations and solutions to security issues revolving around the physical devices on the network. For example there are specific sets of questions related to Programmable Logic Controllers (PLCs) and SCADA firewalls. The extent or scope of these recommendations depends on the assurance level that is calculated by the tool based on the initial answers to site specific requirements. The worst case consequence resulting form a compromise of the overall control system is used determine the Security Assurance Level. The Security Assurance level is used to determine the significance of vulnerabilities.

5. **Target Audience for Results:** *What is the intended audience for the results – upper management, middle management, systems experts?*

The reports generated can be tailored both to upper management as a 30,000 foot level for each layer, as well as a detailed analysis of each item in the assessment and where that item evaluates against the standard. The tool also has links to the detailed security requirement and how to make it comply or what is missing. The consideration of compromise consequence is addressed at very high level but the examination of the cyber system itself is detailed.

Assessment Process Features

6. **Data Collection Approach:** *What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?*

This is a questionnaire- driven assessment. However, the questionnaire requires subject matter experts, therefore, operators, system administrators, and managers will need to be consulted. The assessment is a Software application (Java based) with a knowledge base

that is interactive and guides you through the process. The user can skip around, but some answers will branch the survey and add new areas with additional questions to answer. The user of the tool will very early in the process make a determination based on the initial responses of the Security Assurance Level your site is at.

7. **Detailed Operator Guidance:** *Does the tool or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?*

The tool steps the user through the entire process, adding or removing some questions depending on the answers or choices the user supplies. It is somewhat interactive. Detailed information related to vulnerabilities is provided. The multiple choice answers provide good examples of good to poor control system design and good to poor security policy/procedure design. Threat (i.e. adversaries) is not addressed. Given the appropriate subject matter experts, the question/answer portion should proceed smoothly.

8. **Results:** *Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool produce specific recommendations?*

The tool presents the vulnerabilities of the control system in terms of non-compliance to standards. Threat is not explicitly quantified. Consequence (i.e. another quantitative risk element) is only addressed globally. The worst case consequence resulting form a compromise of the overall control system is used determine the Security Assurance Level. The Security Assurance level helps determine the significance of vulnerabilities.

The tool generates a report that can be either a summary type document for upper management, or a detailed section for each item touched upon by the tool, with the questions and answers, the level of compliance, and the detailed references from which the recommendations are drawn. Recommendations are tailored to the requirements determined by the assurance level and the answers to the questions. Recommendations are included in the tool as a knowledge base. Guidance documents from which the recommendations are drawn are included on the CD as references.

9. **Support for Ongoing Assessment Program:** *What features does the tool have to assist in effectively performing periodic assessments? For example, can the tool compare assessments done at different times? Does the tool support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?*

The update would be a manual process of the user modifying the answers to the questions, changing the component diagrams, and reevaluating the system. Assessment could be saved to file and updated at a later date. The software does not currently have a feature that would compare assessments done at different times. Comparisons would be a manual process.

Deployment Considerations

10. **Learning curve:** *Is the tool intuitive and easy to use?*

The tool is mechanically easy to use. The tool can be run from the CD with the files saved on a local file share. The user interface is relatively intuitive. The user guide included with the tool does a reasonable job of describing the tool, defining security assurance, and includes some security scenarios to allow the user to consider how an intruder could access a control network. It also defines some typical control systems, how to construct the component diagrams and a glossary. The tool is designed such that the user does not need to be a security expert in order to obtain useful information from the exercise.

11. **Cost:** *What is the total cost of the tool, including the purchase price and the cost of implementation and operation?*

This tool will be free but a licensing agreement will be required (for liability reasons).

12. **Schedule:** *How long does it normally take to carry out an assessment using this tool?*

It is easy to use but you need a team of technical expertise or system documentation with you at the time of the assessment.. Creating a diagram of the SCADA or Process Control network is tedious and would require some time. Given that, a team of the right members could probably assess a reasonably complex system in less than a week. Even a couple of days if the users had the right skill set.

13. **Technical requirements:** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).*

The Java runtime (included on CD) is needed to run the tool. Everything else is included on the CD and no external connections are required. Any updates to the rules or knowledge base used in the recommendation would have to be considered.

14. **Installed base:** *How widespread is the use of the tool – in what sectors?*

This tool is only in the beta testing stage for the water sector and a generic version for general industry. This assessment was conducted using the generic version.

15. Vendor support: *What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?*

This is essentially a government developed software tool so the software and consulting support will probably be minimal.

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is an initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cyber security in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen). The raw list of data extracted from the above documents that was used to create the table below, is retained below in an appendix for reference.

The coverage focuses mainly on the individual components on a SCADA network. As such, there are certain criteria that are applied to each type of device. There is a default set of questions that can be answered once and suffice for each type of device. If, for example all the RTU's in the system are configured identically, the default set of question only can be answered. If one or more of the RTU's are configured differently, each device can be addressed individually. The component diagram samples are a starting point to begin the diagram. It is the option of the assessment team to make the system diagram as generic or detailed as they like. This would allow for a high level assessment of the major components, or a very low level assessment of all the devices in the control system.

Currently the tool contains questions pertaining to the standards NERC CIP-002 through CIP-009, NIST SP800-53, and ISO/IEC 15408 v3.1 Assurance Requirements. The users can select none, any, or all of these standards and a section will be added to the assessment for each standard.

Most questions in the tool can be answered in one of three answers. Yes, we do what the question asks; No we do not; Unknown. This makes it very straightforward, but many answers may not be so clear cut.

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.
- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.
- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	***Topic***	***Comments on Coverage***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	This is addressed in the user guide as scenarios. Business processes or high level policies are not covered in the tool. Questions are asked as to whether the policies exist, but make no judgement as to the accuracy, completeness, or effectiveness of the policy
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	Very extensive coverage of components in a control system down to the field device level. Initial questions deal with consequences of injury, death, damage to the environment and infrastructure and are used to assess the assurance level of the site or plant. No specific sector specific consequences in the version that was tested. The generic version does not identify incidents.

Category	*Topic*	*Comments on Coverage*
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	Scope is set by the choice of Applied Standards the assessment team chooses to evaluate. The NERC, NIST, and ISO standards included overlap in some areas. Some processes may not be covered by one or more of the included standards. For most complete coverage and scope, use all during the assessment. Some overlap will occur, but more complete coverage will result.
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	Touched on all aspects of a control and IT systems. From the Internet/Firewall/Router level to field devices. Yes, there is guidence on devices that span to the business or internet level, including outside vendors or remote users.
3.0 Security Policy		
3.1 General	Existence of documented security policy	Choice of several standards: NERC CIP-002 thru CIP 009, NIST SP800-53, and ISO/IEC 15408 v3.1 Assurance Requirements.
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	Designed for SCADA assessments. I couldn't think of any missing elements.
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	Assumes there is an entity within the organization that sets policys for the network and control system. Depending on standard selected, several questions address the organizational security policies.

Category	*Topic*	*Comments on Coverage*
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	Focusses on SCADA systems. Deals with interfaces or links between business and SCADA. Several questions focus on the policies and procedures in place for responsibilities.
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	Yes – These topics are addressed depending on the security standards selected.
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	Yes - These topics are addressed depending on the security standards selected.
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	Most devices have questions dealing with these types of issues.
6.2 SCADA specific	• Consider safety implications of locking up control system elements (e.g. vs. 24 X 7 guard)	Has questions related to physical security of devices, but no outside the device type security questions such as “are their guards?”
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	Questions assess the organizations policies and procedures on how often Risks are evaluated and assessed. Does not deal with specific threat profiles.
7.2 SCADA Specific	• Diagram of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat	Yes, allows you to create and edit to whatever detail required. Has several templates to start with as examples.

Category	*Topic*	*Comments on Coverage*
	sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process? • See last entry in table for SCADA specific vulnerability assessment elements.	Does not specifically enumerate threats or probablility of one incident vs. another. Initial questions direct the user to state the consequences of a compromise of the system. The tool has very little on specific threat assessment. More general threat profiles are discussed.
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	Questions assess whether these types of strategies are evaluated and reviewed. Risks are categorized as dollar amounts (large, medium, small), loss of life or injury, and range of these consequences (in plant, local, or widespread)
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	Tool does identify these issues and has questions relating to strategies.
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	Yes – These topics are addressed depending on the security standards selected.
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need	Yes – These topics are addressed depending on the security standards selected.

Category	*Topic*	*Comments on Coverage*
	alerts, alarms, and to be able to start, stop or modify a process?	
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	Yes – These topics are addressed depending on the security standards selected.
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	Yes – These topics are addressed depending on the security standards selected. Some support of this in the ISO/IEC questions. Questions relate to independent testing and verification. NERC system mentions items like patch management and avti virus updates and need for testing.
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	Yes it is very targeted towards this type of policy. Many questions relating to accounts, authentication, and authorization.
11.2 SCADA specific	Consideration of: • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended	Yes – These topics are addressed depending on the security standards selected. These topics are covered in more than one and some overlap may occur.

Category	*Topic*	*Comments on Coverage*
	logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation	
11.0 Access Control		Analysis specific to NERC CIP 002 -009
11.2 SCADA specific	Consideration of: A) Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service	A) The tool queries the user for compliance to the NERC CIP guidelines for passwords, but does not give guidance on these items. No discussion on account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service is present in the NERC portion of the tool. There are questions on password and authentication in the Identification & Authorization portion of the tool.
	B) Different policies for administrative vs. control access to control system elements	B) The tool addresses control access policies as outlined in CIP 003-1 – Security Management
	C) Different policies for access to critical operator functions and platforms hosting critical components	C) The tool addresses control access policies as outlined in CIP 003-1 – Security Management
	D) Use of stronger authentication for remote access	D) The tool addresses external access as general questions on the assessment. The following is excerpted: NERC **CIP 005-1 R2.4.** Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical

Category	*Topic*	*Comments on Coverage*
		controls at the access points to ensure authenticity of the accessing party, where technically feasible.
	E) Use of team passwords	E) There is no discussion or questions on team or shared passwords.
	F) Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals)	F) The NERC CIP does not specifically address this issue so it is not included in the NERC portion of the tool. There are some general questions in the tool that address this item. There are questions on support time out and termination session policies for various equipment.
	G) Approval of privileges by personnel familiar with control tasks	G) Questions on access control follow the CIP.
	H) Modification of access controls cannot cause interruption of operation	H) The questions on access control in the tool follow the CIP. There is no discussion on disruption or interruption of operation due to access control modifications.
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	Yes – These topics are addressed depending on the security standards selected.
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	SCADA specific devices are included on the component diagram and questions relating to these devices are accessable when these devices are created on the diagram.
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	Management of change relating to Security is covered in the NERC standards
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems	see 13.1

Category	*Topic*	*Comments on Coverage*
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	Yes
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	Yes
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	Yes – These topics are addressed depending on the security standards selected.
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	Yes – These topics are addressed depending on the security standards selected.
16.0 Business Continuity Plan	(Propose not to review this topic)	
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	Yes – These topics are addressed depending on the security standards selected.
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	Included as part of ISO/IEC standard questions.
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry	Several questions address the existance of ongoing

Category	*Topic*	*Comments on Coverage*
	benchmarking, availability of new technologies, etc.	reassessment of policies and procedures. None relate to specifically
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	Standards used currently are NERC, NIST SP800-53, and ISO/IEC 15408 v3.1. Standard sources for questions relating to the SCADA devices is unclear. Need to contact Battelle?
19.0 Identifying Vulnerabilities		

19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP)
	  o Field I/O
	  o Status Data Field Points
	  o System Status Data
	  o Historical Status Data
	  o Exported Data
	  o Imported Data
	  o External (e.g. regional) control signals
	  o Control systems programs and configuration
	• Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are:
	  o Flow of imported data
	  o Flow of exported data
	  o External control signals
	  o Access to historical status data
	  o Other business system interfaces
	  o Internet access
	  o Wireless, modem or dial-up access
	  o Vendor, business partner or regulatory agency access
	• Protection from compromise and interruption:
		Every device type is treated very similarly. A core set of questions for most devices consist of Audit, User Data Protection, Identification and Authentication, Security Management, Protection of the System, and System Access. Depending on the device type, other questions pertinent to the device are included.
		
		Coverage of devices is extensive, but on a generic, non-vendor specific basis.
		
		Devices covered range from the entire IT type devices (firewall, server, switch, router, etc.) to control system devices (RTU, PLC, HMI, etc.).
		
		Some topics are addressed in a more general manner via the security standards chosen at the start of the assessment.

Category	*Topic*	*Comments on Coverage*
	o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks	

Category	*Topic*	*Comments on Coverage*
	• Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	
		Analysis specific to NERC CIP 002 -009
	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP) o Field I/O o Status Data Field Points o System Status Data o Historical Status Data o Exported Data o Imported Data o External (e.g. regional) control signals o Control systems programs and configuration	A) The tool queries the user on protection of data based upon the requirements of the CIP. Like hardware and software, data can be considered a critical asset. However, there is no specific treatment of field, historical, imported, exported, etc. data as it is the user's responsibility to define what is critical data. Protection of data that is considered critical is mainly addresses in CIP 007-1 – Systems Security Management.
	• Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: o Flow of imported data o Flow of exported data o External control signals o Access to historical status data o Other business system interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access o	B) The tool and the CIP address policy for all Critical Cyber Assets. This includes all interfaces and consider both physical and electronic perimeters.
	• Protection from compromise and interruption:	C) The tool and the CIP do not specifically address

Category	*Topic*	*Comments on Coverage*
	o Local automated controls o System or plant automated controls	compromise and interruption.
	• Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software	D) These SCADA features and components are given coverage in the tool and the CIP. The tool includes components that are critical cyber assets.
	• Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters	E) Mechanical objects are only included if there are considered critical cyber assets.
	• Configuration of security features offered by SCADA systems	F) This topic is not explictly covered in the tool or the CIP.
	• Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network	G) The tool and the CIP address detecting cyber intrustion through various available means including log and audit files and intrusion detection.
	• Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks	H) The tool and CIP give considerable attention to malicious attacks, patch management and prevention tools. However, neither the tool nor the CIP serve as a primer on cyber attacks.

Category	*Topic*	*Comments on Coverage*
	• Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

Review of CS^{2}SAT

Report produced by the PCSF SCySAG Working Group
August 6, 2008
V04 bai 8/30/07
Brian.isle@adventiumlabs.org
Carol Muehrcke - cmuehrcke@cyberdefenseagency.com

Summary of CS^{2}SAT Findings

Purpose

The purpose of this document is to offer feedback on the CS^{2}SAT tool. This feedback is based on the work of the PCSF SCADA Cyber Self Assessment Working Group, and is intended for DHS and the CS^{2}SAT team. The working group's intent and charter is to improve available tools for process control cyber security self assessment.

Background

The PCSF SCADA Cyber Security Self Assessment working Group (SCySAG) conducted an in depth review of the CS^{2}SAT developed by Idaho National Lab for Department of Homeland Security. The purpose of the CS^{2}SAT review was to add to the body of knowledge about the requirements for control system cyber security self assessment. The CS^{2}SAT was one of 8 tools and methodologies selected as best-in-class. The tools and methodologies were reviewed against 19 general topical areas of cyber self assessment requirements. The results of the 8 reviews are summarized in the "Summary of SCADA Cyber Self Assessment Methods and Tools Survey" report at https://www.pcsforum.org/groups/68/library/ .

In addition to the CS^{2}SAT report described above, SCySAG held a workshop to gather input to prioritize unmet cyber security self assessment requirement needs at the PCSF meeting in Atlanta March 6 2007. The approximately 50 workshop attendees had a diverse background from industrial control end-users, IT, control system vendors, consultants/service providers, and cyber security researchers. The workshop attendees were very engaged and provided excellent discussion and feedback. The attendees at this workshop, uniformly across sectors, identified the following self assessment areas as most critical for them:

- Identifying Vulnerabilities
- Access Control
- Risk Identification, Classification, and Assessment
- Staff Training and Security Awareness

Based upon this output, the working group further analyzed CS^{2}SAT coverage of Identifying Vulnerabilities and Access Control. The group also recognized that the areas of Risk and Training did not appear to be in the scope of CS^{2}SAT, and plans further work on self-assessment requirements in those areas.

Feedback on CS^{2}SAT

The feedback regarding CS^{2}SAT below is an output of the working group activities just described. The SCySAG tool reviews were not intent on doing relative comparisons, nor on picking the "winner" among the set of available tools. However, the group believes the CS^{2}SAT belongs in the category of "best-in-class" cyber self assessment tool. We encourage the reading of the full report "CS^{2}SAT Summary_V05" located at the PCSF web site https://www.pcsforum.org/groups/68/library/. The CS^{2}SAT highlights include:

- Intuitive to use (for IT & tool experts)
- Broadly applicable, including manufacturing
- Requires multi-disciplinary assessment team (this is good)
- Overall good coverage of high priority topics Identifying Vulnerabilities and Access Control to the level covered by standards incorporated, when these standards are selected
- References the standards from which self-assessment items are derived
- Rationale under questions and document references in the reporting part of the tool provide a good framework within which one could add improvements such as mitigation information and further guidance
- Self contained on CD
- Able to select appropriate standards
- Reports can be customized

In addition, it has been recently reported that funding will be available to extend the number of sectors and standards covered, to maintain the tool software, and to aid in the roll out. We believe that it is critical to fund the maintenance and extension of the CS2SAT to encourage end-users to commit to using the tool.

The group identified the following general areas that CS^{2}SAT does not fully cover. This can mean a further development opportunity for CS^{2}SAT, or that complementary tools or other resources will be used in conjunction with CS^{2}SAT. Based on our understanding of the intended scope of CS^{2}SAT, we propose this division in the list below.

- **Potential further CS^{2}SAT development**
    - Component level view point
        - Lacks system/architecture view
        - Per component questions can become repetitive
    - Consequence measurements used to determine security assurance level are described at global level and are often difficult to assess.
    - Use of the tool requires considerable cyber security background which based on our industry feedback, many users do not possess.
    - Doesn't address security issues with non-routable protocols.
    - There is additional opportunity for providing guidance on solutions, which adds considerable value to the assessment for the users, possibly in the help document section of the assessment report function of CS^{2}SAT. This type of information is more perishable than the CS^{2}SAT questions and could also be provided separately from CS^{2}SAT.

- Core questions do not provide a comprehensive self-assessment if all possible standards are not selected. Notably difficult areas for control systems that do not appear to be mentioned by core questions unless a specific standard is selected include: shared accounts, patch management, protection against malware (e.g. antivirus)
- Doesn't support comparison of assessment results over time.
- Some questions are IT generic instead of covering the unique issues for control systems. If users perceive the tool as IT-centric, they may reject it. Examples:
    - CS^{2}SAT Core Question: *Does the xxx component support time out and termination policies?* CS^{2}SAT Rationale for requirement: *It is good security practice to ensure that an active user session on an unattended xxx component be blocked.* Under this question, the case of a control system requiring an "always-on monitoring" terminals could be acknowledged.
    - CS^{2}SAT Question under NIST 800-53: *Using appropriate vulnerability scanning tools and techniques, does the organization scan for vulnerabilities in the system…?* CS^{2}SAT rationale: *The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques…*Under this question, the potential for equipment outage and damage when using scanning tools on control networks should be acknowledged.
    - CS^{2}SAT Question under NIST 800-53*: Does the system enforce a lockout for failed login attempts?* CS^{2}SAT rationale for requirement: *Due to the potential for denial of service, automatic lockouts…usually… automatically release…after a predetermined time period…* This rationale is useful, but may not go far enough, since for some control systems any length of lockout may create a safety hazard. It is quite possible for a high stress situation to cause errors in password entry causing lockout and catastrophic results.
    - We point out that we did see a different but overlapping question, in the core set, that explicitly acknowledges the control systems concern in the previous bullet example: CS^{2}SAT question: *Can the xxx component detect unsuccessful user authentication events…define a threshold…automatically locked out….Note 2: This should not be implemented on industrial control system applications that cannot tolerate creating lockout conditions…*

- **Complementary tools**
    - Threat (i.e. adversaries) is not addressed (consequences only)
    - Training (the people side of an assessment)
    - Policy and planning
        - Risk Management and Implementation
        - Incident Planning and Response

Methodology/Tool Analysis
Process Control System Forum
SCADA Cyber Self Assessment Working Group
Template rev. 11/28/06

Draft
Tool name: PHA Works by PrimaTech with companion documents
Review author(s): Brian Isle
Review date: 2/7/2007
External reviewer and date: March 6, 2007

Tool Analysis

In the questions below, substitute the term "methodology" if you are assessing a methodology and not a tool.

1. **Overview:** *Provide a brief overview of the tool.*

PHAWorks and the related tool, PHA Audit, provides a versatile general framework for documenting the assessment process that was developed for the process safety management assessment and adapted for security. The tools have been widely used in the chemical sector and the Primatech has built a solid service business in support of the tool application. The tool can work down to the component level, or at the subsystem level, or a combination of the two. PHAWorks has not been made specific for the assessment of control system cyber security, however the tool is very flexible and when combined with a knowledgeable security expert, a facility could do a competent cyber security readiness assessment. Primatech has published many articles on cyber security assessment which can be directly integrated into the tool. This summary is based on the combination of the PHAWorks tool combined with the following Primatech reports discussing cyber security:

1. P. Baybutt, "An Asset-based Approach for Industrial Cyber Security Vulnerability Ananlysis", 2003
2. P. Baybutt, "Sneak Path Analysis Applied to Industrial Cyber Securty", 2003
3. P. Baybutt, "A Scenario-Based Approach for Industrial Cyber Security Vulnerability Analysis", 2004
4. P. Baybutt, "Assessing Risks From Threats to Processing Plants" Threat and Vulnerability Analysis", 2002
5. P. Baybutt, "Process Security Management Systems: Protecting Plants Against Threats", 2003

Applicability

2. **Target Organization:** *What kinds of organizations would find this tool useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.*

The tool has been used in the process safety industry and the much of the help functions are relate to understanding regulation and compliance related to safety. The sectors most likely to use the tool are the chemical and petro-chem related. I believe that the

PHAWorks could be used effectively for cyber security assessment if the organization had a mature SCADA cyber team.

3. **Scope of Assessment:** *Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.*

The tool can scale to include large facilities/plants including the control systems, policy and procedures, and the link to related IT and business systems. The tool can be used from any of three assessment approaches: scenario-based, asset-based or sneak-path-based. The companion documents listed above discuss and provide cyber-related checklists and guidance that can be integrated into the tool and cover all aspects of a security assessment from the management of change to the mitigation of vulnerability.

4. **Coverage of Cyber Security:** *How focused is the tool on cyber security? Does the tool provide in depth guidance for assessing cyber security? By "in depth guidance" we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.*

PHAWorks was initially developed for assessing safety and compliance, and by itself does not provide coverage for cyber-specific topics nor cyber-related guidance. PHA Audit has an example cyber application. PHA Works combined with the articles noted above results in partial coverage for SCADA cyber assessment.

5. **Target Audience for Results:** *What is the intended audience for the results – upper management, middle management, systems experts?*

The reports generated by PHAWorks are focused at the assessor/technician level, but could be used at the middle management level to track action items and responsibilities. The companion articles describe a format for report targeted at higher level recipients.

Assessment Process Features

6. **Data Collection Approach:** *What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?*

PHAWorks is a flexible framework that can be organized in several ways, with questionnaire/checklist being common.

7. **Detailed Operator Guidance:** *Does the tool or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?*

Documentation is focused on safety and is inadequate for cyber assessments. PHAWorks is quite flexible, which is great for experts who know what they want, however I suspect the average operator will be at a loss trying to figure out how to get started, or able to do a complete assessment.

8. **Results:** *Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool produce specific recommendations?*

PHAWorks use a risk calculation to enable prioritization of vulnerabilities. The mitigation recommendations maybe sorted from a cost standpoint.

9. **Support for Ongoing Assessment Program:** *What features does the tool have to assist in effectively performing periodic assessments? For example, can the tool compare assessments done at different times? Does the tool support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?*

PHAWorks does not have a function that automatically computes the changes year over year. There is a recommendation tracking report. It would be easy to utilize previous reports to accelerate subsequent reports. Individual items of the assessment can be updated or added and new reports run without starting from scratch.

Deployment Considerations

10. **Learning curve:** *Is the tool intuitive and easy to use?*

I believe that an expert assessor could be functional in a few hours. The expert would know what he/she wants to do, and would keep looking until they find it. The average plant operator would need training and a better help function to be able to use PHAWorks.

11. **Cost:** *What is the total cost of the tool, including the purchase price and the cost of implementation and operation?*

Unknown

12. **Schedule:** *How long does it normally take to carry out an assessment using this tool?*

Estimated 5 to 10 days for a team of 3 to 5 assessors for a mid-sized plant with access to documents and plant personnel,

13. **Technical requirements:** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).*

Primatech tools require a license. The tools can be downloaded and included an installation wizard. The installation was straightforward. License can be obtained on line. Once the tool is installed and license is obtained, the user can work off-line.

14. **Installed base:** *How widespread is the use of the tool – in what sectors?*

Primatech tools are broadly used in the chemical and petro-chem market place. It has been reported that more then 10,000 assessments have been made using PHAWorks.

15. Vendor support: *What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?*

Primatech has a comprehensive service offering support the tools and assessments.

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)
- NERC Critical Infrastructure Protection Standards 002-009 (found at http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection)
- NERC Top Ten Vulnerabilities of Control Systems and Their Associated Mitigations 2006 (found at ftp://www.nerc.com/pub/sys/all_updl/cip/Top_10_vuln_2006_16mar2006_ss.pdf)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen).

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.
- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.

- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Note: The following analysis is based on the review of the PHAWorks assessment tool – and – the four companion documents available at www.primatech.com below. The documents provide a set of checklists that can be input into the PHA Works or Audit tools and together they provide a fairly complete assessment approach. The Primatech web site states that the PHA Works will be replace with SVAWorks which I believe will be the integration of the tool with the checklist contained in the documents.

6. P. Baybutt, "An Asset-based Approach for Industrial Cyber Security Vulnerability Ananlysis", 2003
7. P. Baybutt, "Sneak Path Analysis Applied to Industrial Cyber Securty", 2003
8. P. Baybutt, "A Scenario-Based Approach for Industrial Cyber Security Vulnerability Analysis", 2004
9. P. Baybutt, "Assessing Risks From Threats to Processing Plants" Threat and Vulnerability Analysis", 2002
10. P. Baybutt, "Process Security Management Systems: Protecting Plants Against Threats", 2003

Category	***Topic***	***Comments on Coverage***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	Yes, documents discuss the linkage between IT and business and control systems
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	Partial - Documents include a typical list of cyber assets, a risk rubicon for considering the impacts. - Does not break down or provide guidance for particular sectors.
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	Yes, documentation provides good coverage
2.2 SCADA	• Guidance on systems and processes	Partial

Category	***Topic***	***Comments on Coverage***
specific	unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	- Provides guidance on security procedures process with broad coverage on contractors, training, system integrity, change management, incident reporting, response and auditing. - Does not cover specific interface between systems e.g. control and business systems
3.0 Security Policy		
3.1 General	Existence of documented security policy	Yes, specificaly calls out documented security policy
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	Partial - does not separate IT and control system policy - does suggest categories of policy and describes
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	Yes, calls for clear roles and responsibility
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	Partial - Does include recommendation for single point authority who has complete process system security coverage - Does not cover topic of coordination between control and business systems
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	Partial - Does not cover multiple access levels based on job responsibilities
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on type of screening required based on job criticality • Guidance on security	Partial - Does discuss screening in general, access control, and contractors - Does not cover job related

Category	*Topic*	*Comments on Coverage*
	responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	access or level of screening.
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	Yes
6.2 SCADA specific	• Guidance on level of physical protection required for various types of cyber assets • Consider safety implications of locking up control system elements (e.g. vs. 24 X 7 guard)	Yes - does includes guidance in a list of mitigation suggestion for the cyber-ralated physical facility
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	Yes
7.2 SCADA Specific	• Diagram of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process? • See last entry in table for SCADA specific vulnerability assessment elements.	Partial - Does cover and give example of specific categories of adversaries, discusses adversary goals and possible attacks. - Does provide list possible cyber critical assets and possible crticality scoring - Does provide rubicons for calculating risk. - does not cover interdependency, timeliness of the response
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences,	Yes

Category	***Topic***	***Comments on Coverage***
	and to accept residual risk.	
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	Yes - Documents cover cyber risk assessment
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	Partial
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	Partial - Documents cover need for incident planning and resonse, provide quidelines for what should be covered. - Does not cover temporal response requirnments nor integration with other processes.
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	Yes, general coverage of change management
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	Partial - Change management is not specific to cyber security
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	Partial
11.2 SCADA specific	Consideration of: • Network and host access • Identifying control network access	Partial - documents have a fair list of access control topics and

Category	*Topic*	*Comments on Coverage*
	points • Removal of default accounts and passwords • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation • Agreements on access control policies in vendor RFPs	management - Does not include multi-level access, relate to access to control specific requirnments, remote locations, nor discuss trade-offs between physical and cyber access control
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	No
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	No
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	Partial
13.2 SCADA specific	• Integration of security and safety analyses for new or changed	No

Category	*Topic*	*Comments on Coverage*
	systems • RFPs include security requirements for vendors • Vendor agreements include interval for security patch updates • Separation of runtime and development environments • Designs consider risks of connections between business and control networks • Designs consider risk of control and non-control traffic on same network	
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	Partial
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	No Not specific to cyber
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	Yes, covers the need to incorprate compliance audits into the overall management system
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	Yes - Need for audits are covered - Documents include a reasonable list of topics for audit for control systems.
16.0 Business Continuity Plan	(Propose not to review this topic)	
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and	No

Category	*Topic*	*Comments on Coverage*
	its environment are assessed to determine needed changes to the CSMS.	
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	Partial - Does cover the need to audit the compliance and the need to report and track incidents - does not link the analysis back into the CSMS for improvements
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	No
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	No - no sector specific information, nor benchmarks
19.0 Identifying Vulnerabilities		

19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP)
	  o Field I/O
	  o Status Data Field Points
	  o System Status Data
	  o Historical Status Data
	  o Exported Data
	  o Imported Data
	  o External (e.g. regional) control signals
	  o Control systems programs and configuration
	• Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are:
	  o Flow of imported data
	  o Flow of exported data
	  o External control signals
	  o Access to historical status data
	  o Other business system
		Partial
		- documents cover apx. 50% of the topics listed

Category	Topic	Comments on Coverage
	interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access • Protection from compromise and interruption: o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but	

Category	Topic	Comments on Coverage
	devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

Methodology/Tool Analysis
Process Control System Forum
SCADA Cyber Self Assessment Working Group
Template rev. 10/25/06

Draft
Tool name: Guidance for Addressing Cyber Security in the Chemical Industy
Review author(s): Ron Melton
Review date: 11/28/06
External reviewer and date: zzzz

Tool Analysis

1. **Overview:** *Provide a brief overview of the tool.*

This isn't a tool, per se, but is a set of self assessment questions.

Applicability

2. **Target Organization:** *What kinds of organizations would find this tool useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.*

This is a general purpose set of cyber security questions intended for use in the chemical industry.

3. **Scope of Assessment:** *Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.*

The scope of assessment is broad with no depth of coverage. Specific technical controls are not addressed.

4. **Coverage of Cyber Security:** *How focused is the tool on cyber security? Does the tool provide in depth guidance for assessing cyber security? By "in depth guidance" we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.*

The term cyber security is used broadly here and is not limited to network security. There is no specific focus on process control systems as a class of networked systems. The questionnaire appears to be based on ISO 17799.

5. **Target Audience for Results:** *What is the intended audience for the results – upper management, middle management, systems experts?*

Middle to upper management.

Assessment Process Features

6. **Data Collection Approach:** *What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?*

Questions, generally open ended.

7. **Detailed Operator Guidance:** *Does the tool or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?*

No

8. **Results:** *Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool produce specific recommendations?*

This is strictly a questionnaire and not a tool. No results are collected and no recommendations made. The questions are generally open-ended and will stimulate inquiry and thought on the part of the user.

9. **Support for Ongoing Assessment Program:** *What features does the tool have to assist in effectively performing periodic assessments? For example, can the tool compare assessments done at different times? Does the tool support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?*

None

Deployment Considerations

10. **Learning curve:** *Is the tool intuitive and easy to use?*

There should be a low learning curve for IT professionals. A process control engineer would probably find the questions difficult to interpret.

11. **Cost:** *What is the total cost of the tool, including the purchase price and the cost of implementation and operation?*

The questionnaire is free. The cost of implementation will be widely variable depending on how the organization uses the questionnaire.

12. **Schedule:** *How long does it normally take to carry out an assessment using this tool?*

Days to weeks.

13. **Technical requirements:** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).*

Not applicable

14. **Installed base:** *How widespread is the use of the tool – in what sectors?*

Don't know

15. Vendor support: *What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?*

Not applicable

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen). The raw list of data extracted from the above documents that was used to create the table below, is retained below in an appendix for reference.

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.
- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.
- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.

- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	***Topic***	***Comments on Coverage***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	This is where most of the questions are targeted. Consequences, etc. are not specifically addressed.
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	There is no specific coverage of SCADA.
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	This is covered generally.
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	No specific coverage of SCADA or process control systems.
3.0 Security Policy		
3.1 General	Existence of documented security policy	General coverage
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	No specific coverage

Category	*Topic*	*Comments on Coverage*
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	General coverage
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	No specific coverage
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	General coverage
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	No specific coverage
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	General coverage
6.2 SCADA specific	• Consider safety implications of locking up control system elements (e.g. vs. 24 X 7 guard)	No
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	Very general coverage, no specific approach provided
7.2 SCADA Specific	• Diagram of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat	No coverage

Category	*Topic*	*Comments on Coverage*
	sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process? • See last entry in table for SCADA specific vulnerability assessment elements.	
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	Very general coverage, no specific approach provided
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	No coverage
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	Very general coverage
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	Process control system is mentioned but only in the context of reporting incidents.
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change	Very general coverage

Category	***Topic***	***Comments on Coverage***
	management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	No coverage
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	Detailed procedure and policy questions
11.2 SCADA specific	Consideration of: • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation	Some specific questions but no recommendations
12.0 Information and Document Management		

Category	*Topic*	*Comments on Coverage*
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	General questions
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	No coverage
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	Targeted to application development more than system development
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems	This is mentioned, but generally, not specific to process control systems
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	General coverage
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	The need for job specific training is included.
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	Very general coverage
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	No coverage specific to process control systems
16.0 Business Continuity Plan	(Propose not to review this topic)	There are questions on this topic

Category	*Topic*	*Comments on Coverage*
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	Very general coverage of this topic
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	Nothing specific to SCADA / process control
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	Very general coverage of this topic
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	No specific coverage for SCADA / process control
19.0 Identifying Vulnerabilities		
19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP) o Field I/O o Status Data Field Points o System Status Data o Historical Status Data o Exported Data o Imported Data o External (e.g. regional) control signals o Control systems programs and configuration • Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: o Flow of imported data o Flow of exported data	No coverage of vulnerability assessment.

Category	Topic	Comments on Coverage
	o External control signals o Access to historical status data o Other business system interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access • Protection from compromise and interruption: o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks	

Category	***Topic***	***Comments on Coverage***
	o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

Methodology/Tool Analysis
Process Control System Forum
SCADA Cyber Self Assessment Working Group
Template rev. 10/25/06

Draft
Methodology name: NERC Critical Infrastructure Protection Standards 002-009
Review author(s): Carol Muehrcke
Review date: 10/27/06
External reviewer and date: zzzz

Tool Analysis

1. **Overview:** *Provide a brief overview of the tool.*

The NERC standard would not normally be considered a tool or a methodology. It however does require the entity to take some specific actions in a specific order, and covers many of the elements in the assessment template.

We compare it to the template here in order to extract SCADA specific items that we may have missed in the template, but that the electric sector finds important. These new items are highlighted in yellow.

Applicability

2. **Target Organization:** *What kinds of organizations would find this tool useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.*

The standard applies to a list of particular types of entities specifically defined by NERC and listed in the standard, such as Transmission and Generation Owners and Operators, and Reliability Coordinators.

3. **Scope of Assessment:** *Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.*

Coverage is defined to cover critical cyber assets, as defined by the organization using guidance in the standard. Standard covers topics from management responsibility, to policies and procedures, to specific technical and nontechnical controls, including physical security of cyber assets.

4. **Coverage of Cyber Security:** *How focused is the tool on cyber security? Does the tool provide in depth guidance for assessing cyber security? By "in depth guidance" we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.*

The standard is specific to cyber security, though it also includes physical security of cyber assets. It touches on all specific cyber elements in the template table below.

5. **Target Audience for Results:** *What is the intended audience for the results – upper management, middle management, systems experts?*

Only specific results are NERC levels of compliance, audience for these is middle and upper management.

Assessment Process Features

6. **Data Collection Approach:** *What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?*

Not defined by the standard.

7. **Detailed Operator Guidance:** *Does the tool or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?*

Standard does contains lists of example critical assets, critical cyber assets, sensitive documents that need protection that are specific to this sector. Lists default passwords and open ports as specific items for vulnerability analysis.

8. **Results:** *Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool produce specific recommendations?*

NERC defines compliance levels to these standards as part of the standards. Standard does not by its nature "produce recommendations" other than to comply.

9. **Support for Ongoing Assessment Program:** *What features does the tool have to assist in effectively performing periodic assessments? For example, can the tool compare assessments done at different times? Does the tool support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?*

N/A

Deployment Considerations

10. **Learning curve:** *Is the tool intuitive and easy to use?*

Standard language is straightforward.

11. **Cost:** *What is the total cost of the tool, including the purchase price and the cost of implementation and operation?*

Standard is free, cost of compliance by entities is to be determined.

12. **Schedule:** *How long does it normally take to carry out an assessment using this tool?*

N/A, this standard is not a tool or method, it is an ongoing process of compliance.

13. **Technical requirements:** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).*

N/A

14. **Installed base:** *How widespread is the use of the tool – in what sectors?*

Electric sector requirement.

15. Vendor support: *What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?*

N/A

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen). The raw list of data extracted from the above documents that was used to create the table below, is retained below in an appendix for reference.

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.

- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.
- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	***Topic***	***Comments on Coverage***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	**Partial** No general discussion of this, however, it is implicit in the requirement to meet this standard and in requirement for risk-based identification of critical cyber assets in (002).
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	**Partial** Yes, gives examples to consider in determining assets critical to bulk power system and defines critical cyber assets as those essential to these critical assets. Also gives examples and other criteria that define critical cyber assets. Yes, Consequence of interest is lack of reliability of the bulk power system. No, does not give numerical targets but requires risk-based determination of critical assets. (all 002) Also requires that electronic security perimeter protection cyber assets be protected (005)
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	**Yes**, Standard applies to critical cyber assets, and entity must list what they are (002).
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment,	**Partial**, gives examples of critical cyber assets unique to this sector (002) and calls out dial-up access to electronic

Category	*Topic*	*Comments on Coverage*
	real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	security perimeter. (005)
3.0 Security Policy		
3.1 General	Existence of documented security policy	**Yes** (003)
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	Partial, states policy must address requirements of this standard (003)
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	**Yes**
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	Partial Senior manager must be designated to insure compliance with standard (which includes physical and cyber aspects) and approve exceptions to policy (003)
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	**Partial**, requires personnel risk assessment (004). Does not require in general that job responsibilites for security be clearly defined, other than at executive level in (003)
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	**Partial**, Personnel risk assessment required for those with cyber access or unescorted physical access to critical cyber assets. Some guidance given on what type of screening to do. Does not discuss cyber responsibilities

Category	*Topic*	*Comments on Coverage*
		of personnel, or mention contracts, but does require risk assessment for service contractors and vendors. (004)
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	**Yes** Does not call out speciic threats but requires physical security perimeter around critical cyber assets. (006) Requires procedures for disposing of critical cyber assets (007)
6.2 SCADA specific	• Consider safety implications of locking up control system elements (e.g. vs. 24 X 7 guard)	**Partial** Requires 24X7 control of physical security perimeter, lists choice of protection methods. Requires notification on failed access, logging of accesses and testing of system. (007) Template could add "guidance on level of physical protection required for cyber assets"
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	**Yes** Calls out in general for a risk based assessment to determine cyber assets (002) Requires vulnerability analysis (005)
7.2 SCADA Specific	• Diagram of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be	**Partial**, Guidance on defining critical cyber assets (002)

Category	*Topic*	*Comments on Coverage*
	able to start, stop or modify a process? • See last entry in table for SCADA specific vulnerability assessment elements.	
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	**No**, Not a general requirement, but see next line.
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	Partial, not a general requirement, but in many specific areas calls out the fact that some technical controls may not be feasible, and requires acceptance of risk and mitigations. (e.g. shutting down ports, use of strong passwords, applying antivirus etc.)
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	**Yes** (008)
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	**Partial**, requires procedure for reporting to the Electric Sector ISAC
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	**Yes** Change management system required (003) Requires access points to electronic security perimeter to have minimum ports and services open. (005) Requires that ports on hosts to

Category	***Topic***	***Comments on Coverage***
		have only necessarily services and ports open. (007) Requires patch management program (007) Requires anti-virus (007) Requires backup/restore process and testing (009)
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	**Partial**, points out that testing should minimize impact on production environment (007) Points out that may not be technically feasible to close some unused ports, apply patches or use antivirus, and requests acceptance of risk and mitigating controls (007)
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	**Yes**, requires close management of access to critical cyber assets (004, 007), mentions "need to know" (007)
11.2 SCADA specific	Consideration of: • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals)	**Partial**, Calls for special procedures related to use of shared passwords (007), Points out use of strong passwords may not be technically feasible (007)

Category	*Topic*	*Comments on Coverage*
	• Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation	
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	**Yes** (003)
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	**Yes**, provides list of examples of specific sensitive documents (003)
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	**Yes**
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems	**No**
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	**Yes**
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	**Partial**, does say training applies to those with cyber access or unescorted physical access to critical assets, and it applies to service vendors and contractors. Says should be appropriate for roles and responsibilities, and R2.2 (004) gives short list of topics to train on.
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	**Yes** standard requires specific areas be audited, and NERC will audit overall compliance to standard, each standard has a compliance section. Required to assess compliance to information protection program annually (003)
15.2 SCADA	• Audit for control systems takes into	**Partial**, do include required

Category	*Topic*	*Comments on Coverage*
specific	account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	ports to be open on electronic security perimeter as part of vulnerability analysis requirements. (005)
16.0 Business Continuity Plan	(Propose not to review this topic)	
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	**Partial** Required controls are defined by the standard, assessment of needed changes is after vulnerability analysis. Requires where feasible, monitoring of accesses to electronic security perimeter (005) Requires monitoring, alerting, logging and review of security events. (007)
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	**Partial**, requires concept of electronic security perimeter as noted above Acknowledges that electronic access monitoring may not always be technially feasible. (005)
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	**No**
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	**No**
19.0 Identifying Vulnerabilities		
19.1 SCADA specific	• Protection of data for integrity/confidentiality (as	**Partial** Requires review of all

Category	Topic	Comments on Coverage
	appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP) o Field I/O o Status Data Field Points o System Status Data o Historical Status Data o Exported Data o Imported Data o External (e.g. regional) control signals o Control systems programs and configuration • Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: o Flow of imported data o Flow of exported data o External control signals o Access to historical status data o Other business system interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access • Protection from compromise and interruption: o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators	connections to electronic security perimeter (ESP) Requires review for default accounts, passwords and network management community strings related to ESP(005) and critical cyber assets (007) Mentions dial-up connections. Requires electronic perimeter protection of critical cyber assets. (005)

Category	Topic	Comments on Coverage
	o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

Methodology/Tool Analysis Template
SCADA Cyber Self Assessment Working Group, Process Control System Forum
Template rev. 3/27/06

Draft
American Petroleum Institute (API) Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries
Author: Martin Stoddard
Revision 9/12/06 (editorial)
External Review: Pending

1. **Overview:** The SVA recommends a multidisciplinary team based approach to conducting a security risk assessment of facilities and operations. The objective of the assessment is to identify hazards, threats, and vulnerabilities faced by a facility as a tool for decision makers to apply appropriate countermeasures to protect the public, workers, national interests, the environment, and the company.

   The general approach is to identify critical assets and infrastructure and potential threats, screen out those with low consequences or low target attractiveness to adversaries, and conduct vulnerability analysis on the remaining targets. Finally, risk is evaluated using a risk matrix of consequence and likelihood where likelihood is a function of attractiveness, threat, and vulnerability.

   Recommendations are provided for the makeup of the evaluation team and checklists are provided for data collection requirements, countermeasures, and interdependencies. Scenario based examples are provided for several oil and gas segments.

Applicability

2. **Target Company:** The methodology is specifically intended for the petroleum and petrochemical industries and is not segment specific (e.g. refineries, pipelines, transportation, etc.). The methodology is general in nature and could be used outside of the oil and gas industry. However, the examples used throughout the document are specific to petroleum and petrochemical companies as well as the checklists.
3. **Scope of Assessment:** The assessment is a general security assessment methodology covering physical and cyber security. The recommended assessment team is broken down into two teams: a full time "core" team and a supporting optional part-time team.

   The SVA Core Team members should have the following skill sets and experience:
   - Team leader—knowledge of and experience with the SVA methodology;
   - Security representative—knowledge of facility security procedures, methods and systems;
   - Safety representative—knowledge of potential process hazards, process safety procedures, methods, and systems of the facility;
   - Facility representative—knowledge of the design of the facility under study including asset value, function, criticality, and facility procedures;
   - Operations representative—knowledge of the facility process and equipment operation;

- Information systems/Automation representative (for cyber security assessment) —knowledge of information systems technologies and cyber security provisions; knowledge of process control systems.

The SVA Optional/Part-time Team members may include the following skill sets and experience:

- Security specialist—knowledge of threat assessment, terrorism, weapons, targeting and insurgency/guerilla warfare, or specialized knowledge of detection technologies or other countermeasures available;
- Cyber security specialist—knowledge of cyber security practices and technologies;
- Subject matter experts on various process or operations details such as process technologies, rotating equipment, distributed control systems, electrical systems, access control systems, etc.;
- Process specialist—knowledge of the process design and operations
- Management—knowledge of business management practices, goals, budgets, plans, and other management systems.

4. **Target Audience for Results:** The result of the assessment is recommended to be summarized in a written report that identifies security vulnerabilities and risk reduction recommendations. The target audience of the report is not explicitly stated but it is recommended that a resolution management system be established to resolve the issues.

Assessment Process Features

5. **Data Collection Approach:** An extensive data collection process is recommended including the collection of facility and right of way records, system information, operations records, outside support and regulatory issues, site inspections, previous incident reports, and threat intelligence. Appendix A of the methodology provides a list of supporting data that should be provided to the SVA team. With this information in hand, a series of forms and checklists are provided to assess the information.
6. **Results:** For each of the primary elements of the assessment a scale of one to five is typically used in a qualitative manner. For example, threats are rated from one to five with one being very low indicating no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets to five indicating that a credible threat exists against the asset and that the adversary demonstrates capability and intent to launch an attack. A prescreening is used to remove both low consequence assets and low attractiveness assets (thus low threat). Assets that remain are evaluated and a risk ranking matrix is recommended to evaluate the likelihood and severity of an attack. Risk reduction through countermeasure analysis is then recommended.
7. **Support for Ongoing Assessment Program:** The assessment methodology is sufficiently general in nature that it is left to the owner/operator and the assessment team to determine the level of detail and the specific data collection and targets of evaluation. There are no specific mechanisms for additions and trending.

Deployment Considerations

8. **Learning curve:** The "core" team leader is recommended to have knowledge and experience with the SVA methodology. However, the assessment methodology does

not use complicated algorithms or aggregation methods. Little training is required to understand the approach.

9. **Cost:** The methodology is publicly available and requires no additional tools for application. However, the core team recommendation is for three to five full time staff plus part-time supporting staff. The actual cost will depend on the scope defined for the study and the depth of data collection.
10. **Schedule:** This is not explicitly stated but will clearly depend on a number of variables including commitment by team members, data and record availability, organization size and complexity, and defined scope.
11. **Technical requirements:** Technical requirements are minimal. The ability to read facility drawings, understand logic diagrams, etc. may be required but the methodology does not require significant technical skill.
12. **Installed base:** Unknown.
13. **Vendor support:** The methodology can be applied entirely by inside personnel. However, for deeper assessments outside contractors may be required. For example, if plant personnel are not trained on cyber security and cyber security is included in the scope of the assessment the contracting of a cyber security professional may be required.

[Ed note 9/12/06: Marty noted in his 3/29/06 email transmitting this draft that the specific technical coverage is not included, but that he felt the SVA was not focused on specifics so coverage would be light. (Also the template for that material was in its infancy at the time when Marty developed this draft.)]

Methodology/Tool Analysis Template
SCADA Cyber Self Assessment Working Group, Process Control System Forum
Template rev. 5/26/06

Draft
American Petroleum Institute Standard 1164 – Appendices A and B Summary
Author: Carol Muehrcke
Revision 8/2/06
External Review: Pending

Note many of the questions in the Tools and Methods sections were adapted from a CIDX document "Report on the Evaluation of Cyber Security Tools and Methods" that analyzed cyber security tools that for the chemical industry found at http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm .

Methodologies

1. ***Overview:*** *Provide a brief overview of the methodology.* The overall standard API 1164 provides guidance to the operators of Oil and Gas liquid pipeline systems for managing SCADA system integrity and security. In this evaluation, we are looking at the methodology encapsulated in Appendices A and B of API 1164. Appendix A is a table formatted as a checklist with room for compliance notes. Appendix B is a template security plan. The checklist is intended as self-assessment guidance for small and medium size pipeline operators to assist them in securing their SCADA systems. The template security plan is intended to assist them in laying out an overall cyber security program.

Applicability

2. ***Target Organization:*** *What kinds of organizations would find this methodology useful?* The Appendix A and B material was aimed at small and medium size pipeline operators. It was intended for organizations with little expertise in cyber security.
3. ***Scope of Assessment:*** *Describe the intended scope of the assessment supported by the methodology. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.* The elements covered are comprehensive and detailed, including physical, network, applications, personnel, policy. As can be seen in the table below, the combination of Appendices A and B cover most items in the SCADA unique element list except: discussion of high level scope of application, assessing the threat, integration of physical and cyber security at the organizational level (though the impact of physical security on cyber assets is clearly covered), types of attacks detectable (though several levels of intrusion detection are suggested), periodic testing of security functions (although test for recovery is covered), and explicit documentation of processes for risk management and vulnerability analysis. These items reflect the fact that the document is focused on giving practical guidance that asset owners can immediately implement to raise the bar for the industry.

4. ***Coverage of Cyber Security:*** *How focused is the methodology on cyber security? Does the methodology provide in depth guidance for assessing cyber security? By "in depth guidance," we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.* The entire focus of this standard is SCADA cyber security.
5. ***Target Audience for Results:*** *What is the intended audience for the results – upper management, middle management, systems experts?* Appendix A is a working checklist, with room for notes about compliance, and does not give formatted results. First tier management or system experts would work with this checklist.

Assessment Process Features

6. ***Data Collection Approach:*** *Is the methodology interview based, questionnaire based or web based?* There is not specific approach suggested to gather the information required to fill out the checklist.
7. ***Detailed Operator Guidance:*** *Does the methodology or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?* The Appendix A checklist has significant detail, in. Appendix B of the standard includes a template security plan.
8. ***Results:*** *Explain how the results are provided and used by the participants – e.g., does the methodology specify what minimum acceptable performance is and how to target areas of concern?* The results are simply compliance or noncompliance with the elements in the Appendix A. An operator would tailor Appendix B to create their own security plan.
9. ***Support for Ongoing Assessment Program:*** *What features does the methodology have to assist in effectively performing periodic assessments? For example, can the methodology compare assessments done at different times? Does the methodology support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?* No.

Deployment Considerations

10. ***Learning curve:*** *How much training is required for participants to use the methodology?* No specific training required.
11. ***Cost:*** *Describe the costs of applying this methodology.* Intended to be low cost for small to medium operators.
12. ***Schedule:*** *How long does it normally take to carry out an assessment using this methodology?* TBD
13. ***Technical requirements:*** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).* None.
14. ***Installed base:*** *How widespread is the use of the methodology – in what sectors?* Widely used by target audience.
15. ***Vendor support:*** *What portion is required to be performed by a service provider versus what is required from the participating organization? Can the participating*

organization use the methodology without contracting a service provider? This is intended to be done by the asset owner themselves.

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen). The raw list of data extracted from the above documents that was used to create the table below, is retained below in an appendix for reference.

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.
- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.
- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.

- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	***Topic***	***Comments on Coverage***
Importance of Cyber Security in Business		
General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	Partial • Appendix B calls for acceptance of residual risk and for analysis of consequences if SCADA system is completely taken over • System used in this standard divides applications into consequence categories and applies different controls to each. Hence there is an implicit "acceptance" of the risk of certain consequences.
SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	Yes • Divides applications into categories depending upon specific consequences of their malfunction, and requirements are levied by category of application • Specific dollar amounts for financial loss, loss of human life, environmental impact inconvenience (odor) are part of categorization
Scope of the Cyber Security Management System (CSMS)		
General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	Partial • Scope is not explicitly stated, but applications, interfaces and equipment involved is required to be enumerated in Appendix B
SCADA specific	• Guidance on systems and processes	Yes.

Category	Topic	Comments on Coverage
	unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	• SCADA unique components and interfaces are listed in the Appendix B template security plan
Security Policy		
General	Existence of documented security policy	Main standard calls for documented security policy but this is not mentioned in this manner in the Appendices.
SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	Yes. • The Appendix A checklist itself could function as a security policy. It is quite specific. • Appendix B has template security plan.
Organizational Security		
General	Organizational entity exists responsible for overall security of organization, including physical and cyber	No
SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	Partial • Sample security plan Appendix B states that there will be a SCADA cyber security manager, lists responsibilities of this individual, and suggests they meet Cyber Security Team across the organization • IT is considered untrusted, coordination not covered • Not necessarily

Category	*Topic*	*Comments on Coverage*
		specific point of responsibility for physical/cyber, however many requirements in appendices touch both areas
Personnel Security		
General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	
SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	Partial • States that responsibilities of information owner should be documented, several of these are noted in Apendix A • Appendix B calls out users, managers and administrators as jobs for which cyber security responsibilities should be defined • Appendix B covers responsibilities of cyber security manager • Third parties – Appendix A covers contracts but not background screening – however, main standard says to consider screening for third parties with access to confidential and restricted information, or physical access to computer rooms, control centers, wiring closets, and for employees based on their physical access

Category	*Topic*	*Comments on Coverage*
		(not cyber)
Physical and Environmental Security		
General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	Yes
SCADA specific	• Considers trade-offs between safety and security (e.g. safety implications of locking up control system elements vs. 24 X 7 guard)	Yes • Provides specific guidelines for physical security of systems based on criticality • Appendix B calls for physical security audit of remote sites that may have access to SCADA network
Risk Identification, Classification, and Assessment		
General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	Yes
SCADA Specific	• Topology? Both physical and schematic of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Identify critical cyber assets (Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?) • See last entry in table for SCADA specific vulnerability assessment elements.	Partial • Required to document all applications in some categories and their location • Requires all connections into network be documented • Topology required under Appendix B template security plan, gives details of what exactly to document and lists of interfaces and components • Provides categories of application by defining levels of consequence, but does not cover how to determine consequences • Appendix B gives example of how to

Category	*Topic*	*Comments on Coverage*
		rank interfaces and equipment types by "value." It also suggests to rank these by impact and susceptibility. It also gives some factors to consider when ranking by susceptibility. These three factors go into an overall "risk" ranking. • Appendix B also calls for assessment of consequences of unauthorized complete control of SCADA system • Does not cover threat agents specifically
Risk Management and Implementation		
General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	Yes
SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	Partial • Process mentioned specifically in Appendix B but not elaborated upon - process covered in API SVA • Some specific strategies are suggested in Appendix B as follows. • Appendix B calls for physical backups to mitigate some specific consequences in the event of unauthorized control of the SCADA system • Appendix B calls for consideration of removal of interfaces, hardening of

Category	*Topic*	*Comments on Coverage*
		components, based on risk level
Incident Planning and Response		
General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	Yes
SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	Partial • Integration not discussed, not normally related • Refers to company incident reporting standards • States that information owners must determine how long their data can be unavailable in backup/recovery procedure • Regulations require backup system and backup control center, so not covered here
Infrastructure-related Operations and Change Management		
General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	Yes
SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	Partial • States that backup/restore tests not be done in production environment • Appendix B gives examples of functions that may be removed from computers in the SCADA system • Specifically prohibits "leaving in" emergency changes that circumvented

Category	*Topic*	*Comments on Coverage*
		normal procedures • Requires documentation of emergency changes • Calls for separation of roles of programmer and implementer – or mitigating controls as exception • Patching called out • Antivirus called out in Appendix B, specific systems to consider called out in main standard • Backup/test already regulated in other documents so not covered here • Does not call for periodic testing other than for backup/restore and business continuity/disaster recovery procedures
Access Control		
General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	Yes
SCADA specific	Consideration of: • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access	Yes • Unique user IDs required for role-based except for the console, calls this out explicitly • Requires specific password expirations and strengths for general users, adminstrators, service accounts • Provides guideline of logoff after 30 minutes activity. Main standard notes that this is for non-operations

Category	Topic	Comments on Coverage
	• Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation	applications only. • PC's/laptops and servers have screen savers • 30 minutes account lockout is required on 5 attempts in all cases • Requires two factor authentication for remote access • Case for access to information must be made to information owner • Requires authentication for access unless system is in physically controlled environment
Information and Document Management		
General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	Yes
SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	Yes • Calls out three levels, public, restricted, confidential. Specific documents are named in both appendices A and B, and in the main body of the standard – the examples in the Appendix B and the main standard are SCADA specific. • Throughout Appendix A, requirements for storage, transmission, destruction, etc. are based on the level of the data.
System Development and Maintenance		
General	Security requirements developed and tested for new or changed systems	Yes
SCADA specific	• Integration of security and safety analyses for new or changed	Partial • Requirements by

Category	Topic	Comments on Coverage
	systems	criticality of system • Calls out separate development/test environment – or mitigating controls as exception • Integration with safety covered under DOT regulations.
Staff Training and Security Awareness		
General	Need for timely awareness and specific technical cyber security training plus periodic updates	Yes • Not in Appendix A checklist but Appendix B and main standard
SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	Partial • A few specific training items mentioned –protection of data about the control system and protection of passwords
Compliance		
General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	Yes
SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	Yes • Requires review of rccords of access against confidential and classified information monthly • Appendix B suggests periodic audit of documented system and risk analyses, as well as periodic self-assessment (e.g. against Appendix A questionnaire,which covers most listed elements in left column here) and vulnerability assessment

Category	*Topic*	*Comments on Coverage*
Business Continuity Plan	(Propose not to review this topic)	
Monitoring and Reviewing the CSMS		
General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	Yes
SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	Partial • No guidance on how to monitor threats • Specifies a minimum set of events to be collected (unauthorized access, account add, etc.) • Other regulations contain additional requirements on monitoring of logs
Maintaining and Implementing Improvements		
General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	Appendix B mentions that self assessments should include tracking new technologies.
SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	No
Identifying Vulnerabilities		
SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP) o Field I/O o Status Data Field Points o System Status Data o Historical Status Data o Exported Data o Imported Data o External (e.g. regional) control signals o Control systems programs and configuration • Enforcement of policy by	Partial • Protection of confidential and classified data during transmission called out • Encryption of stored data that is classified or confidential called out • States that no single point of failure can take out a system classified as mission critical • Types of interfaces

Category	Topic	Comments on Coverage
	mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: o Flow of imported data o Flow of exported data o External control signals o Access to historical status data o Other business system interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access • Protection from compromise and interruption: o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA	listed in Appendix B template security plan • Types of components listed in Appendix B • Appendix B discusses looking at configuration of native security features in SCADA applications • For certain categories of data access audit log must include who, what data, action and when • Appendix B discusses 24 hr a day logging on the network and daily review of logs • Requires network and based intrusion detection in DMZ • Requires network intrusion detection on remote connections to company network

Category	Topic	Comments on Coverage
	applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, □rojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols – Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

Methodology/Tool Analysis Template
SCADA Cyber Self Assessment Working Group, Process Control System Forum
Template rev. 5/17/06

Draft
NCSD Cyber VA Questionnaire
Authors: Cliff Glantz, Garill Cole
Rev. 07/27/06
External review: pending

Note many of the questions in the Tools and Methods sections were adapted from a CIDX document "Report on the Evaluation of Cyber Security Tools and Methods" that analyzed cyber security tools that for the chemical industry found at http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm

Tools

1. **Overview:** Provide a brief overview of the tool.
   - The NCSD Cyber VA Questionnaire was developed by the Department of Homeland Security as a self assessment tool for asset owners and operators. Assessment using the questionnaire provides a high level indication of the status (i.e. well-being) of cyber security for an asset. It is not a risk assessment or management tool.

Applicability

2. **Target Organization:** What kinds of organizations would find this tool useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.
   - The questionnaire is intended for cross-sector application (i.e. all assets). In 2004, for example, RAMCAP was targeted at Nuclear Power, Nuclear Fuel Storage, Chemical, Petroleum Refining, and LNG Storage and Terminal. In 2005 it was targeted at a different set of sectors.

3. **Scope of Assessment:** Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.
   - The questionnaire covers:
     1. Plans, Policies and Documentation
     2. Identification, Authentication and Logical Access Control
     3. Personnel Security
     4. Physical and Environmental
     5. Monitoring and Incident Response
     6. Disaster Recovery and Business Continuity
     7. Configuration Management
     8. Risk and Vulnerability Management

9. General Concerns

4. **Coverage of Cyber Security:** How focused is the tool on cyber security? Does the tool provide in depth guidance for assessing cyber security? By "in depth guidance" we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.
   - The tool consists of about 100 questions supplemented by a 25 page primer on business and control system cyber security. Relatively detailed guidance is provided in the primer in each subject area. Questions covering the elements of a risk assessment are addressed.

5. **Target Audience for Results:** What is the intended audience for the results – upper management, middle management, systems experts?
   - The questionnaire contains general questions for management (e.g. questions about plans policies and documentation) as well as for those experts with responsibility for implementing the different elements of cyber security (e.g. configuration management or risk management). The intended audience is an asset owner or operator. Answering the questionnaire requires the participation of applicable management and staff.

Assessment Process Features

6. **Data Collection Approach:** What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?
   - This a questionnaire-driven assessment with a scoring system based on multiple choice answers and the weight given to the question.

7. **Detailed Operator Guidance:** Does the tool or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?
   - Yes. The questionnaire is supplemented with a primer that provides guidance and provides insights on what is important.

8. **Results:** Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool produce specific recommendations?
   - The results are the answers to the questionnaire and the score obtained given the selected answers and the weight given to each question. The answers and overall score provide a general idea of the status of cyber security of the asset compared what is optimal. It would be interesting to see the scores from several "real" assessments to determine if this method's scoring system "works." In other words, do the scores generated using this method provide a useful measure of the overall level of cyber security of the asset and do they accurately indicate the relative difference in cyber security among multiple assets. Some scoring methods can produce results which do not hold up under a thorough analysis, it will be interesting to see how well this scoring method performs in actual assessments.

9. **Support for Ongoing Assessment Program:** What features does the tool have to assist in effectively performing periodic assessments? For example, can the tool compare assessments done at different times? Does the tool support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?
   - The tool does have a scoring mechanism but is intended only as a high level indicator of the status of cyber security of the asset.

Deployment Considerations

10. **Learning curve:** Is the tool intuitive and easy to use?
    - Yes. It is simple questionnaire with multiple choice answers.

11. **Cost:** What is the total cost of the tool, including the purchase price and the cost of implementation and operation?
    - Inexpensive. Indirect costs include some work hours from applicable managers, operators and system administrators.

12. **Schedule:** How long does it normally take to carry out an assessment using this tool?
    - Quickly. It shouldn't take more than several hours to complete.\

13. **Technical requirements:** Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).
    - None.

14. **Installed base:** How widespread is the use of the tool – in what sectors?
    - There was a report on the Internet (dated 4/17/06) indicating that the questionnaire was been applied to the 5 sectors targeted in 2004.

15. Vendor support: What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?
    - None needed.

Methodologies

1. **Overview:** Provide a brief overview of the methodology.

Applicability

2. **Target Organization:** What kinds of organizations would find this methodology useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.

- (Same as above)

3. **Scope of Assessment:** Describe the intended scope of the assessment supported by the methodology. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.

- (Same as above)

4. **Coverage of Cyber Security:** How focused is the methodology on cyber security? Does the methodology provide in depth guidance for assessing cyber security? By "in depth guidance," we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.

- (Same as above)

5. **Target Audience for Results:** What is the intended audience for the results – upper management, middle management, systems experts?

- (Same as above)

Assessment Process Features

6. **Data Collection Approach:** Is the methodology interview based, questionnaire based or web based?

- (Same as above)

7. **Detailed Operator Guidance:** Does the methodology or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?

- (Same as above)

8. **Results:** Explain how the results are provided and used by the participants – e.g., does the methodology specify what minimum acceptable performance is and how to target areas of concern?

- (Same as above)

9. **Support for Ongoing Assessment Program:** What features does the methodology have to assist in effectively performing periodic assessments? For example, can the methodology compare assessments done at different times? Does the methodology support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?

- (Same as above)

Deployment Considerations

10. **Learning curve:** How much training is required for participants to use the methodology?

- (Same as above)

11. **Cost:** Describe the costs of applying this methodology.

- (Same as above)

12. **Schedule:** How long does it normally take to carry out an assessment using this methodology?

- (Same as above)

13. **Technical requirements:** Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).
- (Same as above)

14. **Installed base:** How widespread is the use of the methodology – in what sectors?
- (Same as above)

15. Vendor support: What portion is required to be performed by a service provider versus what is required from the participating organization? Can the participating organization use the methodology without contracting a service provider?
- (Same as above)

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen). The raw list of data extracted from the above documents that was used to create the table below, is retained below in an appendix for reference.

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.

- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.
- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	***Topic***	***Comments on Coverage***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	General questions related to dependencies and adequate redunancy are included. Questions related to consequence characterisztion are included in the questionaire.
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	SCADA specific issues are not addressed in the questionaire.
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	Questions specific to the statement of the scope of the cyber security management system is not addressed in the questionaire.
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces,	SCADA specific issues are not addressed in the questionaire.

Category	*Topic*	*Comments on Coverage*
	control signals from remote systems.	
3.0 Security Policy		
3.1 General	Existence of documented security policy	General questions related to security policy documentation are included.
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	SCADA specific issues are not addressed in the questionaire.
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	Questions related specifically to the overall security of organization are not addressed in the questionaire.
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	SCADA specific issues are not addressed in the questionaire.
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	General questions related to personnel screening and personnel security responsibilities are included.
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	SCADA specific issues are not addressed in the questionaire.
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	Some general questions related to physical threats are included. Questions related to a power outage threat are not included.

Category	*Topic*	*Comments on Coverage*
6.2 SCADA specific	• Considers trade-offs between safety and security (e.g. safety implications of locking up control system elements vs. 24 X 7 guard)	SCADA specific issues are not addressed in the questionaire.
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	General questions related to identification of threats, vulnerabilities and consequences are included. Questions related to probability of occurance are not covered.
7.2 SCADA Specific	• Topology? Both physical and schematic of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Identify critical cyber assets (Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?) • See last entry in table for SCADA specific vulnerability assessment elements.	SCADA specific issues are not addressed in the questionaire.
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	Questions specific to risk mitigation strategies are not addressed in the questionaire.
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	SCADA specific issues are not addressed in the questionaire.
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are	General questions related to

Category	*Topic*	*Comments on Coverage*
	developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	monitoring and incident response are included.
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	SCADA specific issues are not addressed in the questionaire.
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	General questions related to configuration management of cyber systems are included.
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	SCADA specific issues are not addressed in the questionaire.
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	General questions related to identification, authentication and logical access control are included.
11.2 SCADA specific	Consideration of: • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system	SCADA specific issues are not addressed in the questionaire.

Category	*Topic*	*Comments on Coverage*
	elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation	
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	Questions specifcally related to managing security of information and documentation are not included.
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	SCADA specific issues are not addressed in the questionaire.
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	Questions specifcally related to ensuring appropriate security for new or changed systems are not included.
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems	SCADA specific issues are not addressed in the questionaire.
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	General questions related to staff training and security awareness are included.
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for	SCADA specific issues are not addressed in the questionaire.

Category	*Topic*	*Comments on Coverage*
	control system personnel	
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	Questions specifcally related to auditing security policies and procedures are not included.
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	SCADA specific issues are not addressed in the questionaire.
16.0 Business Continuity Plan	(Propose not to review this topic)	
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	General questions related to monitoring and incident response are included.
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	SCADA specific issues are not addressed in the questionaire.
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	Questions specifcally related to an ongoing process for continuous update the CSMS, based on industry benchmarking or availability of new technologies are not included.
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	SCADA specific issues are not addressed in the questionaire.

Category	***Topic***	***Comments on Coverage***
19.0 Identifying Vulnerabilities		

19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP)
	  o Field I/O
	  o Status Data Field Points
	  o System Status Data
	  o Historical Status Data
	  o Exported Data
	  o Imported Data
	  o External (e.g. regional) control signals
	  o Control systems programs and configuration
	• Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are:
	  o Flow of imported data
	  o Flow of exported data
	  o External control signals
	  o Access to historical status data
	  o Other business system interfaces
	  o Internet access
	  o Wireless, modem or dial-up access
	  o Vendor, business partner or regulatory agency access
	• Protection from compromise and interruption:
	  o Local automated controls
	  o System or plant automated controls
	• Consideration of SCADA system components:
	  o HMI/MMI
	  o Alarm subsystems
	  o Data archiving
	  o Front end processor/local data storage
		SCADA specific issues are not addressed in the questionaire.

Category	Topic	Comments on Coverage
	o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

Methodology/Tool Analysis
SCADA Cyber Self Assessment Working Group, Process Control System Forum
Template rev. 7/27/06

Draft
Vulnerability Self Assessment Tool (VSAT)
Authors: Carol Muehrcke
Rev. 07/27/06
External review: pending

Tool Analysis

1. **Overview:** *Provide a brief overview of the tool.*

VSAT is a software tool currently targeted for the water and wastewater sectors, that walks a user through identifying assets, threats, current countermeasures and level of risk. It then allows application of new countermeasures and lets you see the new level of risk. It covers all kinds of assets and risks including physical, cyber, and SCADA.

Applicability

2. **Target Organization:** *What kinds of organizations would find this tool useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.*

The tool is populated with particular sets of assets and threats as a starting point intended for the water and wastewater sectors. It can and has been used by small, medium and large organizations.

3. **Scope of Assessment:** *Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.*

This tool is for assessment of risk to specific assets from specific threats. It is not intended to review the overall security program of the organization such as management responsibilities, procedures, policies, etc.

4. **Coverage of Cyber Security:** *How focused is the tool on cyber security? Does the tool provide in depth guidance for assessing cyber security? By "in depth guidance" we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.*

The tool has a generic list of cyber assets for a water/wastewater organization that can be tailored for a particular organization. This includes the major cyber systems that a utility may have – management, customer, maintenance, laboratory, plant and pump station control. The tool also has a library including of 30 built-in threats to cyber assets, and VSAT's countermeasure library includes about a dozen possible cyber countermeasures. Note that the tool allows the user to augment the asset, threat and countermeasures lists.

5. **Target Audience for Results:** *What is the intended audience for the results – upper management, middle management, systems experts?*

There is graphical output – a before and after risk profile, and detailed reports. These are suitable for all of these audiences. There is also an automatically generated Word report intended for the EPA regulatory audience.

Assessment Process Features

6. **Data Collection Approach:** *What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?*

There is no particular data collection approach implied by the tool, however the existing libraries of threats and countermeasures serve as a checklist for the user to refer to and augment. The tool has a wizard that steps the user through setting up threat/analysis pairs and going through the analysis for threat/asset pairs, which includes filling in several elements that determine criticality and vulnerability (see #8).

7. **Detailed Operator Guidance:** *Does the tool or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?*

Yes. The tool has a generic list of assets built into the tool, and libraries of threats and countermeasures that can be referenced by the user. It has built in descriptions for the items in the library. Countermeasures are not tied to specific threats, this association is made by the user. There is no specific guidance for the assignment of probabilities or the factors that determine criticality, that are input by the user (per #8).

8. **Results:** *Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool produce specific recommendations?*

Risk is viewed as the pair (criticality, vulnerability) for a particular asset and threat, where each element of the pair is assigned to one of four buckets. The number of asset/threat pairs that fall in each of the 4x4 = 16 categories are depicted in a matrix type layout. Criticality is calculated based on several components which are extent, severity, temporal effects, recoverability, collateral damage. Vulnerability to a specific threat is the product of its probability of occurrence and the probability of failure of the set of countermeasures that are applied to this threat. Countermeasures can serve to detect, delay, or respond to the threat. The tool also has a concept or risk reduction units (RRUs) and calculates risk reduction units and annual cost for various countermeasure scenarios, so that the user can compare options. The tool has a generic list of countermeasures but does not recommend countermeasures for specific threats.

9. **Support for Ongoing Assessment Program:** *What features does the tool have to assist in effectively performing periodic assessments? For example, can the tool compare assessments done at different times? Does the tool support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?*

The tool allows using a previous implemented plan as a baseline plan for a new analysis. It also provides a report that summarizes countermeasures implemented over various years. [ed: haven't studied this feature yet]

Deployment Considerations

10. **Learning curve:** *Is the tool intuitive and easy to use?*

The tool appears to be easy to use. There is a 2.5 day class for users of the tool. Most utilities have used it on their own without help from a consultant.

11. **Cost:** *What is the total cost of the tool, including the purchase price and the cost of implementation and operation?*

The tool is free to the water/wastewater sector. The training in the past was also free.

12. **Schedule:** *How long does it normally take to carry out an assessment using this tool?*

Schedule will depend upon the number of threats considered. Recommendation is to start with 5-8 threats. Typical experience is a 2 to 3 month effort.

13. **Technical requirements:** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).*

The tool is easy to install on a standard Windows PC. An internet connection allows access to threat and countermeasure library updates. The license restricts use to the water and wastewater sector.

14. **Installed base:** *How widespread is the use of the tool – in what sectors?*

The tool was used by 30-40% of the water/wastewater sector to create their mandatory risk report to the EPA several years ago. There are 6500 copies in circulation, and 2000 people have been trained on the tool.

15. Vendor support: *What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?*

The developer provides a phone support line and email address.

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)

- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen). The raw list of data extracted from the above documents that was used to create the table below, is retained below in an appendix for reference.

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.
- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.
- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	***Topic***	***Comments on Coverage***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	Yes, in the sense that use of this tool will achieve this – so the tool does not ask the user whether they already have it.
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	Partial Has model lists of critical assets – mentions plant and pump station control systems. Has model definitions of criticality including level of consequence and incorporating types of consequences, by asset category. Does not have guidance on making a particular consequence level assignment.

Category	*Topic*	*Comments on Coverage*
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	Partial The tool does not specifically address processes and organizations covered. The scope of the analysis of the tool is determined by the assets and threats selected for analysis.
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	Partial Since has default modifiable model list of critical assets under control systems, including Server, PLCs, RDUs, CRTs and instrumentation interface. Does not detail potential interfaces.
3.0 Security Policy		
3.1 General	Existence of documented security policy	No Not intended to audit cyber security management system, but rather to assess risk
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	No, focuses on countermeasures rather than policy.
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	No Not intended to audit cyber security management system, but rather to assess risk
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system	No, although it should be noted that the tool allows physical countermeasures to be applied to cyber threats.

Category	*Topic*	*Comments on Coverage*
	security	
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	Partial Library does contain employee and vendor screening countermeasures. Job responsibilities not addressed.
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	No Not specific to SCADA, however screening countermeasures noted above could be applied by the user to address a SCADA threat.
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	Partial Threat library includes theft of documents, employee cutting power. Note that there is a physical access countermeasure in the library related to IT. Not completely covered, focus is on IT threats to IT systems and physical threats to physical systems.
6.2 SCADA specific	• Consider safety implications of locking up control system elements (e.g. vs. 24 X 7 guard)	No The "Disadvantages" information given for the IT physical access countermeasure would be a good place to discuss this topic. This was not discussed in the library version reviewed.
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	Yes Has built in template threat heirarchy of specific threats and categories of threats, which is customizable. There are 30 IT threats included. Does not specifically look at vulnerabilities as an item in and of themselves, but rather looks at level of vulnerability to a specific threat given the

Category	*Topic*	*Comments on Coverage*
		existing countermeasures, in what is called the "baseline analysis." Probability of occurance of attempt is a user input.
7.2 SCADA Specific	• Diagram of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process? • See last entry in table for SCADA specific vulnerability assessment elements.	Partial Has model list of SCADA system critical assets. Does consider temporal aspect of criticality in default definitions for levels of criticality – how long will be out of service. If network diagrams or characteristics of adversaries are used to set the factors that determine vulnerability or criticality, this would be done outside of the tool.
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	Yes, in the sense that the tool itself supports a process to trade off annual cost with risk reduction units, examining various scenarios for adding countermeasures.
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	Yes, in the sense that SCADA systems are one type of asset being considered by this tool, and see remarks above.
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	No The tool focuses on countermeasures in response specifically to water crisis such as boil water alerts, announcements, not cyber events specifically.

Category	***Topic***	***Comments on Coverage***
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	No
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	Partial Antivirus and configuration management are mentioned as countermeasures
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	No Nothing specific to SCADA systems is mentioned.
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	No Not mentioned as countermeasures.
11.2 SCADA specific	Consideration of: • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical	No

Category	*Topic*	*Comments on Coverage*
	components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation	
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	Yes. Information classification procedure is countermeasure in library.
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	No No SCADA specifics mentioned.
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	No
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems	No
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	Partial Security awareness program is in countermeasure library
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	No No SCADA specifics mentioned
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	Partial Technical audits of process, systems and networks is a countermeasure in the library.

Category	*Topic*	*Comments on Coverage*
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	No No SCADA specifics mentioned.
16.0 Business Continuity Plan	(Propose not to review this topic)	
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	No The tool provides a risk assessment given an organization's posture at a given point in time.
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	No
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	No The tool provides a risk assessment given an organization's posture at a given point in time.
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	No
19.0 Identifying Vulnerabilities		
19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP) o Field I/O	Partial Encrypted traffic is in the countermeasure library. Threat in the library is very general – hacker

Category	Topic	Comments on Coverage
	o Status Data Field Points o System Status Data o Historical Status Data o Exported Data o Imported Data o External (e.g. regional) control signals o Control systems programs and configuration	compromises confidentiality and/or integrity of the SCADA system. Lists firewall as countermeasure in library. Relationship to control systems not mentioned.
	• Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: o Flow of imported data o Flow of exported data o External control signals o Access to historical status data o Other business system interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access	
	• Protection from compromise and interruption: o Local automated controls o System or plant automated controls	
	• Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software	As mentioned above, has default modifiable model list of critical assets under control systems, including Server, PLCs, RDUs, CRTs and instrumentation interface.

Category	***Topic***	***Comments on Coverage***
	• Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	Countermeasure library includes application monitoring and network intrusion detection. No mention of control systems.

Methodology/Tool Analysis
SCADA Cyber Self Assessment Working Group, Process Control System Forum
Template rev. 4/17/06

Draft
RAMCAP Assessment Synopsis
Authors: Carol Muehrcke
Rev. 07/27/06
External review: pending

Open questions –

1. Does DHS work on RAMCAP with each infrastructure owner/operator individually? (template question #1)

2. What are three sector specific RAMCAP versions that we have heard are available? Where are they available? (#2)

3. Slides say RAMCAP framework to be available in Sept 2005. Is it available and where? (#1)

4. Slides say that RAMCAP framework is being developed for five sectors in 2004 and started for more in 2005. Where do these stand now? (#2)

Started in 2004:

- Nuclear Power Plant Risk Assessment
- Chemical Sector Risk Assessment
- Nuclear Fuel Storage
- Petroleum Refining
- LNG Storage/Terminals

Intended for start in 2005:

- Rail Cargo
- Electric Power Generation and Transmission
- Cyber/IT
- Water Treatment
- Dams, Locks, and Levees

5. Does above list imply that cyber is being treated by RAMCAP as a separate infrastructure, in addition to being a part of other critical infrastructures? (#4)
6. To which 5 sectors has the cyber assessment questionnaire been applied? (#4, #14)
7. What would trigger a RAMCAP assessment by an owner/operator? (#1)
8. Do we know anything about training on RAMCAP? (#10)
9. Do we know anything about sector-specific step by step approaches for consequence analysis, and benchmark threat scenarios mentioned in the DHS exec summary? (#7)

---

1. **Overview:** *Provide a brief overview of the methodology.*

Method developed by DHS to allow "harmonization" of terrorist risk results across the government and privately owned critical infrastructure sectors. Steps in the process are:

- Asset characterization and screening
- Threat characterization
- Consequence analysis
- Vulnerability analysis
- Asset attractiveness and threat assessment
- Risk assessment
- Risk management.

RAMCAP is intended to be mathematically rigorous at an appropriate level, and to allow for future integration of more sophisticated quantitative risk methods in the future. It was created to allow DHS to work with critical infrastructure owners/operators to carry out its mission of protecting the US critical infrastructures.

Applicability

2. **Target Organization:** *What kinds of organizations would find this methodology useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.*

Intended for government or private organizations responsible for critical infrastructure. This synopsis looks at the generic RAMCAP framework. Sector-specific versions are under development. As of April 2006, three sector specific versions are available (?) Note sector specific guidelines were reported as under development in 2004 for:

- Nuclear Power Plant Risk Assessment
- Chemical Sector Risk Assessment
- Nuclear Fuel Storage
- Petroleum Refining
- LNG Storage/Terminals

3. **Scope of Assessment:** *Describe the intended scope of the assessment supported by the methodology. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.*

Intended to assess risk of terrorist attack against government or private sector owned critical infrastructure. Assessment team to include DHS at some steps, for purpose of providing information about intentions and capabilities of terrorist adversary. DHS notes that some consequences found during the RAMCAP process may be carried forward by the operator/owner even if they do not meet DHS risk screening criteria for further DHS scrutiny. Includes assessment of supporting/surrounding infrastructures.

4. **Coverage of Cyber Security:** *How focused is the methodology on cyber security? Does the methodology provide in depth guidance for assessing cyber security? By "in depth guidance," we mean information about cyber specific assessment elements such as those listed in the Technical Coverage section below.*

In the RAMCAP executive summary, the terms “cyber” and “computer” do not appear. However, RAMCAP has developed a set of cyber screening questions that have been applied to 5 sectors.

5. **Target Audience for Results:** *What is the intended audience for the results – upper management, middle management, systems experts?*

DHS itself is one audience, as the method is intended to be part of an overall assessment of national risk, and allow comparison of risks across different critical infrastructures. Management of the owner/operator is also an audience. We expect that the target management audience will depend upon the level of detail of the assessment.

Assessment Process Features

6. **Data Collection Approach:** *Is the methodology interview based, questionnaire based or web based?*

At this draft, only detail we know is existence of cyber screening questionnaire noted above.

7. **Detailed Operator Guidance:** *Does the methodology or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?*

Will add additional details here once we obtain a copy of the RAMCAP cyber screening questionnaire noted above. RAMCAP executive summary also mentions sector-specific step by step approaches for consequence analysis, and benchmark threat scenarios, but at this writing we do not have details about these.

8. **Results:** *Explain how the results are provided and used by the participants – e.g., does the methodology specify what minimum acceptable performance is and how to target areas of concern?*

Risk is calculated by multiplying quantitative measures of consequence, vulnerability and threat. Determination of acceptable level of risk is a step within the methodology itself.

DHS will determine a level of risk at that provides a screen for whether it will further consider an asset or not. DHS will maintain a database of critical assets based on the RAMCAP activities from various sectors that pass this screen.

9. **Support for Ongoing Assessment Program:** *What features does the methodology have to assist in effectively performing periodic assessments? For example, can the methodology compare assessments done at different times? Does the methodology support efficient update of previous analyses when the participant’s target of assessment changes (e.g. to incorporate new systems and applications)?*

Deployment Considerations

10. **Learning curve:** *How much training is required for participants to use the methodology?*
11. **Cost:** *Describe the costs of applying this methodology.*
12. **Schedule:** *How long does it normally take to carry out an assessment using this methodology?*

DHS points out that the methodology can be applied at various levels of detail. The level of detail would impact the length of the assessment.

13. **Technical requirements:** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).*

14. **Installed base:** *How widespread is the use of the methodology – in what sectors?*

Five sectors have completed reports based on the cyber security questionnaire. These sectors are: [].

15. Vendor support: *What portion is required to be performed by a service provider versus what is required from the participating organization? Can the participating organization use the methodology without contracting a service provider?*

Although support by vendors is not mentioned, DHS notes that their participation is required during the threat characterization and threat assessment steps of the methodology.

Note we have kept the section below for possible use in future drafts once we have a copy of the RAMCAP cyber assessment questionnaire.

Technical Coverage

Does the assessment review the following elements?

1. *Protection of data for integrity/confidentiality (as appropriate), at rest and in transit:*
   - *Field I/O*
   - *Status Data Field Points*
   - *System Status Data*
   - *Historical Status Data*
   - *Exported Data*
   - *Imported Data*
   - *External (e.g. regional) Control Signals*

2. *Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are:*
   - *Flow of imported data*
   - *Flow of exported data*
   - *External control signals*
   - *Access to historical status data*
   - *Other business system interfaces*
   - *Internet access*
   - *Wireless, modem or dial-up access*
   - *Vendor, business partner or regulatory agency access*

3. *Protection from compromise and interruption:*

- *Local automated controls*
- *System or plant automated controls*

4. *Protection from unauthorized use:*
   - *System management functions*
   - *Interfaces to oversight entities or external SCADA system*

5. *Consequences of component failures (identification of critical components)*
6. *Access controls for:*
   - *Critical operator functions*
   - *Platforms hosting critical components*

7. *Operating system platforms, for patch level and unnecessary services*
8. *Configuration of security features offered by SCADA systems*
9. *Capability to detect and respond to cyber intrusions*
10. *Clarity and adherence to responsibilities/roles for SCADA security, by management and other personnel*
11. *Personnel background checks appropriate to access allowed*
12. *Documentation of SCADA network configuration*
13. *Process for modifying network configuration*
14. *Residual risks to SCADA systems accepted by management*
15. *Protection of information useful for finding vulnerabilities of SCADA network*

Methodology/Tool Analysis Template
SCADA Cyber Self Assessment Working Group, Process Control System Forum
Template rev. 5/26/06

Draft
RAM-W Summary
Authors: Rebecca Freeman, Candace Sands
Rev. 07/27/06
External review: pending

Note many of the questions in the Tools and Methods sections were adapted from a CIDX document "Report on the Evaluation of Cyber Security Tools and Methods" that analyzed cyber security tools that for the chemical industry found at http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm .

Methodologies

1. **Overview:** Provide a brief overview of the tool.

   The RAM-W tool/methodology was developed Sandia National Laboratories, in conjunction with the EPA, and the AWWARF. The tool/methodology assigns quantification of consequences, identification of threats, policy, equipment, and human procedures that can reduce risk It is specifically targeted for the water and wastewater industries.

Applicability

2. **Target Organization:** What kinds of organizations would find this tool/methodology useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.

   The RAM-W is specifically designed for the water and wastewater industries. There are numerous references in the assessment tool/methodology that refer to the immature (but growing) structure of SCADA systems in the water and wastewater industry. The move from proprietary to open architecture is mentioned in theory, but not addressed specifically. Smaller utilities, or utilities with older architecture, would still find the RAM-W recommendations applicable; larger utilities with more advanced technology will appreciate the traditional I.T. focus of the RAM-W security template.

3. **Scope of Assessment:** Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.

The first focus of the RAM-W is the identification of threats. Four are identified: human intentional, human unintentional, natural , and environmental. The RAM-W focuses primarily on human intentional threats, with a much more brief overview of human unintentional threats. Natural and environmental threats are given secondary consideration, only.

The assessment covers emerging system weaknesses (moves from proprietary to open architecture control systems), especially the merging of SCADA and Administrative (physical) networks.

4. **Coverage of Cyber Security:** How focused is the tool/methodology on cyber security? Does the tool/methodology provide in depth guidance for assessing cyber security? By "in depth guidance" we mean information about cyber specific assessment elements such as those listed in the Technical Coverage section below.

   The tool/methodology has a 3-page overview of CyberSecurity where the threats referred to in section 5 are mentioned. The individual threats are then broken down into levels of sophistication, resources, mission, risk tolerance, and motivation. They are assigned a cost on the threat scale, accordingly.

5. **Target Audience for Results:** What is the intended audience for the results – upper management, middle management, systems experts?

   Upper management, primarily, and those involved in risk management. If the assessment identifies weaknesses, the necessary personnel will be consulted for the possible addition or upgrade of equipment and processes.

Assessment Process Features

6. **Data Collection Approach:** What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?

   Primarily a checklist- and questionnaire- driven assessment. Questionnaires for operators, system administrators, and managers. Interview-based, as well. The creation of the questionnaires and interviews are left to the discretion of the utility performing the assessment.

7. **Detailed Operator Guidance:** Does the tool/methodology or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?

   Yes. The tool/methodology requests specific SCADA security policies and plans, control procedural documentation, and SCADA security training documentation. It also requests network diagrams, logical topology diagrams, lists of network and SCADA/field equipment, ACL's, and any identification of crossover points between the SCADA and Administrative networks. Experienced network staff should be able to identify weaknesses and suggest reinforcement, based on those documents.

8. **Results:** Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool/methodology produce specific recommendations?

   RAM-W^{SM} Methodology Risk Equation Synopsis
   Risk equation: $R = P_A * (1 – P_E) * C$
   Risk = Likelihood of occurrence [insider, outsider, cyber] * (1 – System effectiveness [or likelihood of successful attack]) * Consequence
   Risk aspects: cost; operational impact; loss of public confidence, etc.
   P_A = Likelihood of occurrence is set to 1 (highest value) per RAM-W methodology unless you have credible info.
   $(1 – P_E)$ = system effectiveness: level of effectiveness provided by physical protection system(s), operating system (people, procedures, & technology/equipment), & cyber protection.
   C= Consequence: impact on mission objectives; liabilities; mitigation

   All of the variables are given a low, medium, or high ranking. These are than transposed into quantifiable values (0.1, 0.5 or 0.9, respectively).

   Example: if P_E = low = (1-0.1) = 0.9

   and C = High = 0.9

   than your risk is:

   R = 1 * 0.1 *0.9 = 0.81 = high risk

9. **Support for Ongoing Assessment Program:** What features does the tool/methodology have to assist in effectively performing periodic assessments? For example, can the tool/methodology compare assessments done at different times? Does the tool/methodology support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?

   Good question that will require follow-up, and a review of the entire document, rather than just the SCADA-specific measures.

Deployment Considerations

10. **Learning curve:** Is the tool/methodology intuitive and easy to use?

    Relatively, yes. It took about 8 hours of training to prepare users to work with the RAM-W.

11. **Cost:** What is the total cost of the tool, including the purchase price and the cost of implementation and operation?

    Inexpensive – the indirect costs can be totaled as they relate to work hours of the assessment team members.

12. **Schedule:** How long does it normally take to carry out an assessment using this tool?

It took Charleston Water System nearly 2 years to complete the entire assessment. The average time for an assessment to be completed is 3-6 months, and it was highly recommended that utilities review the assessment annually, to make sure assets and threats are current.

13. **Technical requirements:** Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).

    The tool/methodology is entirely paper-based and requires no external technology. There is a secondary tool/methodology called the VSAT that is available for download, that requires internet access and a basic PC to run the software.

14. **Installed base:** How widespread is the use of the tool/methodology – in what sectors?

    The RAM-W is the primary assessment tool/methodology for water and wastewater vulnerability evaluation. It was required, by law, that all utilities meeting the criteria established by the EPA complete the RAM-W assessment. The deadlines for assessment completions were assigned based on the size of the utility. It was developed, first, under the Clinton administration and then refined into a second revision that was much more comprehensive than the first. Version 1 made no mention of CyberSecurity at all.

15. **Vendor support:** What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?

    None. The EPA trained the RAM-W trainers, and those trainers hosted classes; some utilities hired consultants to help with the completioNot Coveredpplication of the methodology.

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen). The raw list of data extracted from the above documents that was used to create the table below, is retained below in an appendix for reference.

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.
- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.
- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	*Topic*	*Comments on Coverage*
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	The critical business process is defined by the utility as a primary mission. The RAM-W does allow for consequence prioritization and it documents a fault tree of possible breaches and outcomes.
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	NOT COVERED.
2.0 Scope of the Cyber Security Management System (CSMS)		
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	CybserSecurity is indirectly addressed in section 4.6: Cyber-Threat.
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	NOT COVERED.
3.0 Security Policy		
3.1 General	Existence of documented security policy	The RAM-W requires a thorough review of all security policies in existence with the utility.
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	The review of documentation covers all technology-related policies, for both traditional I.T. and SCADA.

Category	*Topic*	*Comments on Coverage*
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	There is a statement of importance regarding organization security, but no specific guildelines.
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	NOT COVERED.
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for security clearly defined.	
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	The RAM-W has two sections (6 & 7) that address physical security. Common PPS hardware items are provided, for consideration of vulnerability.
6.2 SCADA specific	• Considers trade-offs between safety and security (e.g. safety implications of locking up control system elements vs. 24 X 7 guard)	Hardware is discussed (i.e., door locks) but no specific address of safety vs. security is contained in the methodology.
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	The utility's assessment team is tasked with identifying threats and vulnerabilities.

Category	*Topic*	*Comments on Coverage*
		Basic categories of threat / vulnerability are identified: loss of personnel, chemical contamination, etc.
7.2 SCADA Specific	• Topology? Both physical and schematic of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Identify critical cyber assets (Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?) • See last entry in table for SCADA specific vulnerability assessment elements.	Importance of network documentation / diagrams is repeatedly emphasized. A basic list of network and control system hardware is provided, and the utility is encouraged to complete the list with any site-specific hardware. Cost assignment is done, and a pairwise relationship for both threat matrices: the "benefit to threat" matrix and the "degree of vulnerability" matrix.
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	A risk equation is provided, to assist in the definition of a process for identification, prioritization, and mitigation of vulnerabilities.
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	There is some guidance for determining the numerical ranking value for each SCADA hardware item, and evaulating those items in a pairwise matrix.
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	Documents for threat identification are present, but nothing specifically geared towards cyber incidents. Templates (2) are provided for assessment of an insider and

Category	*Topic*	*Comments on Coverage*
		outside threat.
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	NOT COVERED.
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	NOT COVERED.
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	NOT COVERED.
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	NOT COVERED, other than a general emphasis on reviewing all existing I.T. policies.
11.2 SCADA specific	Consideration of: • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical	NOT COVERED.

Category	*Topic*	*Comments on Coverage*
	components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation	
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying, transmittal, retention, etc..	NOT COVERED.
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	NOT COVERED.
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	NOT COVERED, but the RAM-W does comment on the necessity for long-term follow-up and review of risk for new (or upgraded) system components.
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems	NOT COVERED.
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	NOT COVERED.
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	NOT COVERED.
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber	It is suggested that a long-term

Category	*Topic*	*Comments on Coverage*
	security policies and procedures, that controls are working as intended and all of these meet business requirements	iteration follow the initial assessment process; no specific guidelines are provided.
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems • Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	NOT COVERED.
16.0 Business Continuity Plan	(Propose not to review this topic)	
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	NOT COVERED.
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	NOT COVERED.
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	It is suggested that a long-term iteration follow the initial assessment process; no specific guidelines are provided.
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	NOT COVERED.
19.0 Identifying Vulnerabilities		
19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in	

Category	Topic	Comments on Coverage
	light of protocols used (e.g. ModBus/TCP/IP) o Field I/O o Status Data Field Points o System Status Data o Historical Status Data o Exported Data o Imported Data o External (e.g. regional) control signals o Control systems programs and configuration • Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: o Flow of imported data o Flow of exported data o External control signals o Access to historical status data o Other business system interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access • Protection from compromise and interruption: o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops	

Category	Topic	Comments on Coverage
	o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	

Methodology/Tool Analysis
Process Control System Forum
SCADA Cyber Self Assessment Working Group
Template rev. 11/28/06

Draft
Tool name: Example Industry PCN Assessment Tool
Review author(s): Brian Isle
Review date: 1/31/07
External reviewer and date: 1/31/2007

Tool Analysis

In the questions below, substitute the term "methodology" if you are assessing a methodology and not a tool.

1. **Overview:** *Provide a brief overview of the tool.*

This is a proprietary tool developed and used by major corporation and user of process control systems. This summary will refer to the tool as Example PCN Assessment Tool (EPAT). EPAT is an Excel spreadsheet-based and includes separate pages for: Instructions, Information, Impact, Environment, Network, Modems, OS, App& PLC, Summary, and Risk Acceptance. The spreadsheet utilizes pull down menus and embedded help/explanations. EPAT is focused on process control cyber security, but includes physical security to the extent need to protect the cyber assets. EPAT is easy to use and is very intuitive.

Applicability

2. **Target Organization:** *What kinds of organizations would find this tool useful? Some characteristics to consider are sector, size of organization, experience/maturity of organization in their SCADA security program.*

EPAT is fairly versatile with good coverage for remote locations and applicable to the refining, chemical, oil & gas storage and movement, water and waste water control systems sectors.

3. **Scope of Assessment:** *Describe the intended scope of the assessment supported by the tool. Scope includes the system/operations boundary to which the assessment applies, the topics the assessment covers and the recommended participants in the assessment team. Typical topics are organization for security, policies and procedures, architecture, system controls.*

EPAT handles plant and facility scale cyber assessments. The assessment is at the component and sub-system level with focus on networks, wireless, modems, operating systems, applications, and controllers/RTUs. EPAT includes coverage for security policy including topics like change management and personnel management. It appears that EPAT requires a companion standards document calling out specific security standards.

4. **Coverage of Cyber Security:** *How focused is the tool on cyber security? Does the tool provide in depth guidance for assessing cyber security? By "in depth guidance"*

we mean information about cyber specific assessment elements such as those listed in the "General" rows of the table in the Technical Coverage section below.

EPAT is focused on the control system, the interface to the business systems and the related physical security necessary to protect the cyber assets. The tool provides best practice guidance for most of the questions and topics.

5. **Target Audience for Results:** *What is the intended audience for the results – upper management, middle management, systems experts?*

The report would be suitable for the operations group responsible for cyber security and the operations management. The report would need an executive summary for upper management. The report forms an audit that can be used as a checklist and comparison over time.

Assessment Process Features

6. **Data Collection Approach:** *What type of approach is used for performing the assessment (e.g., questionnaire/checklist, interview/audit)?*

EPAT uses an Excel spreadsheet-based questionnaire with pull-down answers and some "fill in the blank" for applicable standards.

7. **Detailed Operator Guidance:** *Does the tool or its documentation provide detailed guidance to assist the operator, such filled out examples or checklists of assets to consider, potential vulnerabilities, adversaries, etc.?*

EPAT provides best practice guidance and helps provide the proper frame-of-mind for the assessor.

8. **Results:** *Describe the kinds of results provided by the tool. What are the scoring techniques? Does the tool produce specific recommendations?*

EPAT assesses the level of criticality and flows down the requirements and related question down stream thru the tool. The report makes specific recommendations, who in the organization to work with, and reasoning behind the recommendations.

9. **Support for Ongoing Assessment Program:** *What features does the tool have to assist in effectively performing periodic assessments? For example, can the tool compare assessments done at different times? Does the tool support efficient update of previous analyses when the participant's target of assessment changes (e.g. to incorporate new systems and applications)?*

EPAT does not have temporal comparison features. The tool is mostly static and does not appear to lend itself well for backward compatibility for new features or applications.

Deployment Considerations

10. **Learning curve:** *Is the tool intuitive and easy to use?*

EPAT is very intuitive and easy to use. The operator should easily understand the terminology and find EPAT easy to navigate.

11. **Cost:** *What is the total cost of the tool, including the purchase price and the cost of implementation and operation?*

NA.
EPAT is a proprietary tool.

12. **Schedule:** *How long does it normally take to carry out an assessment using this tool?*

My guess is one week with a team of 5 people for a moderate sized facility.

13. **Technical requirements:** *Describe any technical requirements (e.g., external connection requirements, ease or difficulty in installation, licensing requirements).*

EPAT requires a companion document of cyber standards

14. **Installed base:** *How widespread is the use of the tool – in what sectors?*

EPAT is believed to be used broadly across the corporation who developed the tool.

15. Vendor support: *What if any support is needed, and what support is available from the vendor or others in order to successfully use this tool?*
The corporation appears to have a dedicated group to maintain the tool.

Technical Coverage

Note that none of the above characteristics touch on whether the assessment tool or methodology covers the right topics. This is a tougher list but is central to the gaps analysis the working group is interested in. Below is a initial list of "right topics" based on:

- Sandia's "Reference Model for Control and Automation Systems in Electric Power," (found at: http://www.sandia.gov/scada/documents/NSTB_Ref_Model_V1_2.pdf)
- DOE's "21 Steps to Improve Cyber Security of SCADA Networks" (found at: http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf)
- Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator (found at: http://www.digitalbond.com/SCADA_security/UTC_Final.pdf)
- Process Control System Security Technical Risk Assessment: Analysis of Problem Domain (found at: http://www.mitre.org/work/tech_papers/tech_papers_06/06_0045/index.html)
- Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1 (found at: http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm)
- NERC Critical Infrastructure Protection Standards 002-009 (found at http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection)

- NERC Top Ten Vulnerabilities of Control Systems and Their Associated Mitigations 2006 (found at ftp://www.nerc.com/pub/sys/all_updl/cip/Top_10_vuln_2006_16mar2006_ss.pdf)

This work is in fact called out in the group's task called "SCADA environment unique characteristics."

This table is organized by elements used by ISA SP-99 Part II. This same list is used by the CIDX document in the fifth bullet above (which adds one) and ISO 17799, (which uses ten of the eighteen).

Filling in the Table

To evaluate a methodology or tool against these elements:

- The purpose of the the table is to identify strong and weak areas this methodology has in terms of cyber security generally, but most importantly in terms of SCADA-specific cyber self-assessment topic areas.
- There are two separate judgements you make under each of the 18 categories – one is whether the topic is covered in terms of general cyber security, and secondly whether specific control system topics are treated by the tool or methodology.
- Fill in the rightmost column of the table, noting whether and to what extent the methodology or tool covers the item in the Topic column. Do this by filling in one of the words Yes, No, Partial and any explanatory comments.
- It is not expected that you will detail coverage of every bullet point in the table.
- However, if you find a SCADA specific topic covered by your methodology/tool that is not listed here, record this in your comments.

Category	***Topic***	***Comments on Coverage***
1.0 Importance of Cyber Security in Business		
1.1 General	Critical business processes and IT system dependencies are identified at a high level, consequences of security breaches understood, profile of acceptable/unacceptable consequences agreed	No
1.2 SCADA Specific	• Model lists of typical critical control system assets for entities in specific sector • Consequences to be considered include those possible via control systems such as loss of life, damage to infrastructure, environmental damage • Guidance on assessing consequences of incidents typical in a particular sector	Partial - Does not include model list of assets (maybe included in companion documents) - Includes impacts related to 3 scenarios, where assessor answers relative to their understaning of the PCN system - The selectable impacts are typical for the process control industry
2.0 Scope of the Cyber Security Management System (CSMS)		

Category	***Topic***	***Comments on Coverage***
2.1 General	Existence of statement for scope of cyber security management system, including systems, processes and organization interfaces covered	Partial - CSMS scope is distributed across the 5 topic areas (environment, network, modems, OS, applications, & controllers
2.2 SCADA specific	• Guidance on systems and processes unique to control systems such as control room, plant, remote stations, the lab configuration environment, real time and historical data availability. • Guidance on interfaces unique to control systems such as interfaces between control and business systems, interfaces to oversight entities, external vendor interfaces, emergency remote interfaces, control signals from remote systems.	Yes (caveat – requires companion reference document) - Good coverage and guidance on interface between PCN and non-PCN networks, including wireless
3.0 Security Policy		
3.1 General	Existence of documented security policy	Yes
3.2 SCADA specific	• Areas of policy that may differ for IT systems and control systems • Elements needed in control system policy	Yes - It appears the policy is either embedded in the tool or reflects and tests a companion document.
4.0 Organizational Security		
4.1 General	Organizational entity exists responsible for overall security of organization, including physical and cyber	Yes
4.2 SCADA specific	• Individual exists with clear definition of responsibility for control system cyber security • Clear coordination point between business side IT cyber security and control system security • Specific point of responsibility exists for ensuring that combination of physical and cyber mechanisms provide adequate control system security	Yes - Covers roles and responsibilities clear and stresses importance of coordination between IT, physical, and PCN security
5.0 Personnel Security		
5.1 General	Employees and contractors are screened upon employment and job changes, based on criticality of job. Job responsibilities for	No - Not covered

Category	***Topic***	***Comments on Coverage***
	security clearly defined.	
5.2 SCADA specific	• Guidance on defining job criticality for control system personnel • Guidance on type of screening required based on job criticality • Guidance on security responsibilities of control room and other control system personnel. • Third party contracts related to control room have provisions for cyber security.	Partial - Does disscuss formal controls on passwords and userids - Does discuss restricting access to PCN systems - Doesn't cover background checks on employees
6.0 Physical and Environmental Security		
6.1 General	Physical threats to cyber systems considered, including physical damage, tampering with removable media, tampering with external interfaces, equipment failure, power outage	Partial
6.2 SCADA specific	• Guidance on level of physical protection required for various types of cyber assets • Consider safety implications of locking up control system elements (e.g. vs. 24 X 7 guard)	Yes - Physical security is covered in companion document - Does cover Utilities, physical restricted access, and protection against fire & floods.
7.0 Risk Identification, Classification, and Assessment		
7.1 General	Identify threats, vulnerabilities, consequences, probability of occurance for realization of threats identified	Partial - does not calculate probablities - threats are limited to Hacker, Fire, & Flood
7.2 SCADA Specific	• Diagram of control system network • Guidance for enumerating critical assets • Enumeration and characteristics/preferences of threat sources (e.g. terrorist, activists, employees, criminals) • Guidance for assessing probability of control system security incidents • Guidance on assessing consequences • Consider: interdependencies and cascading effects • Consider when defining criticality: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a	Partial - Uses 3 scenarios and multiple question to consider for the plant that determine the impact levels - Does not include reference archtecture - Does not list critical assets - Scenarios assume a serious "hacker", randon virus, and fire/flood. - Includes some guidance on selecting impacts of the scenarios. EPAT picks the risk level and suggests next steps in the tool based on the severity of the impact selected by the assessor.

Category	*Topic*	*Comments on Coverage*
	process? • See last entry in table for SCADA specific vulnerability assessment elements.	- Suggests changes to PCN components and policy based on risk level - No guidance is prodived for timely response
8.0 Risk Management and Implementation		
8.1 General	Defined process in place to evaluate and select mitigation strategies for risks identified, based on cost and consequences, and to accept residual risk.	Yes
8.2 SCADA specific	• Process in place for management to select mitigation strategies and accept residual risks related to control systems	Yes - Tool suggests mitigation changes to system based on risk. Uses color code identify critical suggestions.
9.0 Incident Planning and Response		
9.1 General	Procedures for cyber incidents are developed, documented and communicated. These procedures include response, communications at time of incident, reporting, post mortem.	Partial
9.2 SCADA specific	• Integration with organization's existing crisis management processes • Possibly unique reporting requirements for control system incidents • Consider when designing response procedure: how long can you operate without control, without visibility? How fast do you need alerts, alarms, and to be able to start, stop or modify a process?	Partial - Coverage limited to containment of cyber threats and problem resolution
10.0 Infrastructure-related Operations and Change Management		
10.1 General	Existence of processes for change management, removal of unnecessary services from platforms, patch management, backup/restore, anti-virus application	Yes
10.2 SCADA Specific	• Consider that all of these processes for control systems require particular attention to testing in off-line environment, may be different than parallel IT processes • Consider that servers running control system components may	Yes - Change management is covered in each category

Category	*Topic*	*Comments on Coverage*
	have different profile of required services than business servers • Periodic testing of security controls for high risk control environments	
11.0 Access Control		
11.1 General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties	Yes
11.2 SCADA specific	Consideration of: • Network and host access • Identifying control network access points • Removal of default accounts and passwords • Control risks due to: forgotten passwords, expiring passwords, account lockout on login failures, screen savers blocking status information, authentication using remote servers or LAN/WAN elements causing denial of service • Different policies for administrative vs. control access to control system elements • Different policies for access to critical operator functions and platforms hosting critical components • Use of stronger authentication for remote access • Use of team passwords • Common instances in which "weaker" cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals) • Approval of privileges by personnel familiar with control tasks • Modification of access controls cannot cause interruption of operation • Agreements on access control policies in vendor RFPs	Yes - Provides both questionair and policy suggestions for centralized control and at section level (e.g. network, OS, applications)
12.0 Information and Document Management		
12.1 General	System for classifying information that determines policies on access, copying,	No

Category	***Topic***	***Comments on Coverage***
	transmittal, retention, etc..	
12.2 SCADA specific	• Model list of potentially sensitive control system information such as equipment diagrams, logic or programs, any information useful for finding vulnerabilities etc..	No
13.0 System Development and Maintenance		
13.1 General	Security requirements developed and tested for new or changed systems	No
13.2 SCADA specific	• Integration of security and safety analyses for new or changed systems • RFPs include security requirements for vendors • Vendor agreements include interval for security patch updates • Separation of runtime and development environments • Designs consider risks of connections between business and control networks • Designs consider risk of control and non-control traffic on same network	Partial - Includes good coverage of change management - Development environments are not covered - Good coverage of connection of business and control networks - Might be covered in companion documents
14.0 Staff Training and Security Awareness		
14.1 General	Need for timely awareness and specific technical cyber security training plus periodic updates	Yes
14.2 SCADA specific	• Awareness and training for control system personnel tailored to specific needs • Guidance on training needs for control system personnel	Yes - calls out specific and periodic PCN training
15.0 Compliance		
15.1 General	Audit in place for compliance to cyber security policies and procedures, that controls are working as intended and all of these meet business requirements	Yes - compliance with cyber requirnments are specifically called out and tool forms the basis of the audit
15.2 SCADA specific	• Audit for control systems takes into account complementary physical and cyber mitigators • Audit for control systems takes into account differences in upgrade, patch, anti-virus and minimal platform services procedures for control systems	Yes - Covers the intersection of physical and cyber - Audit specifically checks on upgrades, patch, etc and the process to keep “evergreen”

Category	*Topic*	*Comments on Coverage*
	• Audit for control systems does not use automated scans where these might disable equipment • Audit includes configurations of firewalls that protect control system network	
16.0 Business Continuity Plan	(Propose not to review this topic)	NA
17.0 Monitoring and Reviewing the CSMS		
17.1 General	Data on failed and successful incidents, audits and changes to the organization and its environment are assessed to determine needed changes to the CSMS.	No
17.2 SCADA specific	• Guidance how to monitor the control system threat environment, and specific threats to a given sector • Types of attacks that are reported/detectable against control system provides adequate data for this analysis?	No - Tool does not track incident or threat
18.0 Maintaining and Implementing Improvements		
18.1 General	Ongoing process exists for continuous update the CSMS, based on industry benchmarking, availability of new technologies, etc.	Yes
18.2 SCADA specific	• Sources for benchmark information for sector • Sources for tracking SCADA security technology	Partial - Describes the "evergreen" approach to renew the process - does not include benchmarking
19.0 Identifying Vulnerabilities		
19.1 SCADA specific	• Protection of data for integrity/confidentiality (as appropriate), at rest and in transit, in light of protocols used (e.g. ModBus/TCP/IP) o Field I/O o Status Data Field Points o System Status Data o Historical Status Data o Exported Data o Imported Data o External (e.g. regional) control signals o Control systems programs and configuration	Partial - Good coverage of network including wireless, modems, OS, servers, applications, database, and controllers (e.g. PLC, RTU) - Does not consider types of cyber attacks and IDS is limited to enforcement of firewalls

Category	Topic	Comments on Coverage
	• Enforcement of policy by mechanisms that protect all interfaces to SCADA systems. Policy includes controls on physical access to remote access point of origin, authentication of access attempt, and authorized information flow. Typical interfaces are: o Flow of imported data o Flow of exported data o External control signals o Access to historical status data o Other business system interfaces o Internet access o Wireless, modem or dial-up access o Vendor, business partner or regulatory agency access • Protection from compromise and interruption: o Local automated controls o System or plant automated controls • Consideration of SCADA system components: o HMI/MMI o Alarm subsystems o Data archiving o Front end processor/local data storage o RTUs/IEDs/PLCs o Sensors o Control equipment and actuators o Global control loops o Local control loops o SCADA/PCS system software • Consider items being controlled: underlying mechanical objects such as pumps, valves, switches and heaters • Configuration of security features offered by SCADA systems • Capability to detect cyber intrusions using available data - usage of IDS, log files in firewalls/routers, operating	

Category	Topic	Comments on Coverage
	systems, business and SCADA applications, for critical servers, field devices and network • Kinds of attacks that are detectable o Reconnaissance to identify vulnerabilities o Exploit attempts on unpatched systems o Worms, trojans, denial of service attacks o Security events in control application logs o Attacks using SCADA/DCS protocols - Some simple but devastating attacks (detectable by Digital Bond SCADA IDS attack signatures for Modbus TCP, DNP3) – Denial of service attacks • Force reboot • Force listen only mode – Unauthorized client reads and writes – Reconnaissance attempts – Buffer overflow attacks	