PROCESS CONTROL SYSTEMS FORUM

SCADA Cyber Self-Assessment (SCySAG) Working Group

Workshop

Brian Isle
PCSF Spring Conference
June 7, 2006
Brian.isle@adventiumlabs.org
https://www.pcsforum.org/groups/68

Agenda

10:00

- 5 min - Review the agenda and expectations for the outcome
- 10 min - Introductions
- 20 min - Brief overview of SCySAG & status
- 30 min - Review summaries
- 20 min – Overview of DHS/INL efforts
- 30 min - Identify and prioritize requirements gaps
- 10 min - discuss the results and identify issues

12:00 Working lunch

- 30 min - Discuss plan for follow-on work,
- 20 min - discuss and define the plan for dissemination of the information
- 10 min - wrap-up

Objective of Workshop Session

1. **Identify cyber security SCADA requirement gaps and do first order prioritization**

2. **Define plan forward**

Caveat:
This is going to be quick, messy and imprecise.
We will capture the issues and work them later.

SCADA Self Assessment Requirements Gaps

Requirements Area	Priority	Rationale for priority

Improvements to SCADA unique elements list (add, delete, modify)

1. (item)
2. (item)

Improvements to process of identifying requirements gaps

1. **Additional recommended sources of information**
   a. (item)
   b. (item)
2. **Process/template recommendations**
   a. (item)
   b. (item)

PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Working Group Next Steps

- **Identifying gaps**
  1. item
  2. Item
- **Addressing high priority gaps**
  1. item
  2. item
- **Disseminating group results (resource list, filled in templates and work on gaps)**
  1. item
  2. item

Issues

- (item)
- (item)

Introductions
SCySAG Core Team

- 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

PROCESS CONTROL SYSTEMS FORUM

SCySAG Overview & Status

SCySAG Objective

Enable the development and use of the best possible next generation of self administered tools and methodologies for the assessment of the cyber security readiness of the process control systems. These systems are used in manufacturing, industrial, energy, and utilities.

Scope of SCySAG

By the term SCADA, we mean:

- **.. encompassing all types of manufacturing plants and facilities, as well as other processing operations such as utilities, pipelines and transportation systems or other industries which use automated or remotely controlled assets. Including:**
  - Process control systems, including Distributed Control Systems, Programmable Logic Controllers, Remote Terminal Units, Intelligent Electronic Devices, Supervisory Control and Data Acquisition, networked electronic sensing and control, and monitoring and diagnostic systems
  - Associated information systems such as advanced or multi-variable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems and plant information management systems
  - Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Ref: dISA-99.00.01, Manufacturing and Control Systems Security, Part 1: Concepts, Models and Terminology, October 2005

“SCADA cyber” in the broadest sense

SCySAG Overall Approach

- Identify and publish a compendium of existing SCADA self-assessment efforts/resources
- Gather and distill unique characteristics of the control system environment, identifying the variation of characteristics for the various infrastructure sectors.
- Analyze coverage by control system cyber self-assessment tools and methods efforts.
- Conduct and publish a gap analysis to identify areas of cyber self-assessment requirements that are inadequately covered.
- Prioritize and work to resolve the requirements gaps

SCySAG – Expected Impact

The adoption of the requirements will be voluntary. The results of this effort can be used by:

- **Tool and methodology vendors to develop, deploy, and maintain an assessment solution,**
- **SCADA system vendors to create more secure systems,**
- **Standards bodies and groups, and**
- **Owner/operators developing their internal policies and procedures.**

Requirements Gap Process

- **Select tools/methodologies: Define a set of tools/methodologies we will consider as representative of the "best available."**
- **Define SCADA-unique characteristics: Define a set of SCADA-unique characteristics against which we will evaluate these tools/methodologies for gaps.**
- **Evaluate tools/methodologies: Evaluate the tools/methodologies against the set of SCADA-unique characteristics.**
- **Identify gaps: Review the results of these evaluations to assess coverage, overall and by sector, of the SCADA unique characteristics, and thus identify gaps in the requirements being used to create these tools/methods.**

Representative tools/methodologies/standards

Sector	Tools/Methodologies	Standards/Guidelines
Electric Power	- IT Recovery Plan for Electric Co-ops (NRECA) - Method(s) from NERC's "Risk Assessment Methodologies for Use in the Electric Utility Industry" http://www.esisac.com/library-assessments.htm	NERC CIP 02-09
Water/Wastewater	RAM-W VSAT	Interim Voluntary Security Guidance for Water Utilities, Section 5; http://www.awwa.org/science/wise/#P7_623
Chemical	Use tools/methods evaluated by CIDX in their report at http://www.chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm	Guidance for Addressing Cyber Security in the Chemical Sector
Petro/Petrochem	API Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries (line 4)	API 1164, SCADA Security
Cross-sector	DHS NCSD cyber security questionnaire DHS Control System Self Assessment Tool	ISO 17799 SP-99

Define SCADA-unique characteristics

Created template to summarize tools/methods

- **General overview**
  - *Applicability*
  - *Assessment Process Features*
  - *Deployment Considerations*
- **Technical coverage based on:**
  - Sandia's "Reference Model for Control and Automation Systems in Electric Power,"
  - DOE's "21 Steps to Improve Cyber Security of SCADA Networks"
  - Electric, Gas, and Water: Critical Infrastructure Network Similarities & Differences Security as a Common Denominator
  - Process Control System Security Technical Risk Assessment: Analysis of Problem Domain
  - Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.1

Identify the Requirement Gaps

- **Topic of today**
  - This will be the first pass at reviewing gaps

Reference URLs

- 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