



# SCADA Cyber Self-Assessment (SCySAG) Working Group

**Brian Isle**

**PCSF Spring Conference**

**June 6, 2006**

**[Brian.isle@adventiumlabs.org](mailto:Brian.isle@adventiumlabs.org)**

**<https://www.pcsforum.org/groups/68>**

*Collaborating to Advance Control System Security*

# Agenda

- ◆ **Why do this?**
- ◆ **Working Group Charter**
- ◆ **Accomplishments**
- ◆ **Next Steps**

# SCADA Specific Cyber Issues

- ◆ **Multi-generational installations**
- ◆ **Geographically distributed systems**
- ◆ **Graying of the workforce**
- ◆ **Safety focused, not security focused**
- ◆ **Lack of accepted cyber vulnerability measures**
- ◆ **These are “control systems” – NOT – “IT”!**
- ◆ **Mostly privately owned, distaste for regulation**
- ◆ **Assessment scalability issues**

## Why do a Self-Assessment WG?

- ◆ **The threat is real, the Nation can't wait**
- ◆ **Need a reasonable means to measure and compare readiness**
- ◆ **Provide independent voice to advise the standards groups, vendors, & end-users**

**SCADA cyber readiness is largely unknown**

## 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 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**

# SCySAG Core Team

- ◆ Martin Stoddard, P.E.  
Pacific Northwest National  
Laboratory  
[martin.stoddard@pnl.gov](mailto:martin.stoddard@pnl.gov)
- ◆ Mark C. Morgen  
3M - Optical Systems Division IT  
[mark.morgen@mmm.com](mailto:mark.morgen@mmm.com)
- ◆ Carol Muehrcke  
Cyber Defense Agency, LLC  
[cmuehrcke@cyberdefenseagency.com](mailto:cmuehrcke@cyberdefenseagency.com)
- ◆ Matt Earley  
Decisive Analytics Corporation  
[matt.earley@dac.us](mailto:matt.earley@dac.us)

- ◆ Rebecca Freeman  
Charleston (SC) Water System  
[freemanjr@charlestoncpw.com](mailto:freemanjr@charlestoncpw.com)
- ◆ Candace Sands  
EMA  
[csands@ema-inc.com](mailto:csands@ema-inc.com)
- ◆ Brian Isle  
Adventium Labs  
[brian.isle@adventiumlabs.org](mailto:brian.isle@adventiumlabs.org)
- ◆ Cliff Glantz  
Pacific Northwest National  
Laboratory [cliff.glantz@pnl.gov](mailto:cliff.glantz@pnl.gov)

## **SCySAG - Accomplishments**

- ◆ **List of 90+ relevant guidelines standards, tools, & methods**
- ◆ **Selection of sector specific standards**
- ◆ **Initial assessment of 5 tools/methods based on standard template**
- ◆ **Initial cut at SCADA unique cyber requirements**

## Example Activities

- ◆ **Conference call with DHS on Idaho Framework & RAMCAP methodology**
  - Opportunity to comment on DHS cyber security questionnaires
- ◆ **Demo of VSAT tool used by the water sector**
- ◆ **Early look at Control System Self-Assessment Tool under development by DHS/INL**

# Example SCADA-Specific Characteristics

Access Control	
General	Principle of least privilege, controlled management of accounts, coverage of personnel and third parties
SCADA specific	<p>Consideration of:</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• Different policies for administrative vs. control access to control system elements</li> <li>• Different policies for access to critical operator functions and platforms hosting critical components</li> <li>• Use of stronger authentication for remote access</li> <li>• Use of team passwords</li> <li>• Common instances in which “weaker” cyber security mechanisms in control system settings call for stronger physical access controls (e.g. unattended logged in terminals)</li> <li>• Approval of privileges by personnel familiar with control tasks</li> <li>• Modification of access controls cannot cause interruption of operation</li> </ul>

## SCySAG - Plan Forward

- ◆ **Complete the SCADA unique characteristics study and requirements gap analysis**
- ◆ **Complete prioritization of requirement gaps**
- ◆ **Work to resolve the highest priority gaps**

# Discussion