



**Process Control Systems  
Industry Conference**

# **Status Review SCADA Cyber Self-Assessment (SCySAG) Working Group**

**August 28, 2008**

**Brian Isle**

**Brian.isle@adventiumlabs.org**

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

**Carol Muehrcke**

**Cyber Defense Agency, LLC**

**[cmuehrcke@cyberdefenseagency.com](mailto:cmuehrcke@cyberdefenseagency.com)**

# Agenda

- ◆ **SCySAG Background**
- ◆ **Topics: Training & Risk Assessment**
- ◆ **Today's objective**
- ◆ **Panel discussions**

# Why SCySAG was Formed in 2005

- ◆ **Pressing need to understand our SCADA cyber security readiness**
  - What is the complete list of SCADA cyber security assessment requirements?
  - Which requirements are relevant to my sector?
  - How do IT and SCADA cyber security assessment differ?
  - What SCADA assessment requirements are unmet by existing tools and methodologies?

## 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.**

Although we used SCADA in the working group name, the group's work:

.. encompasses 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.

# SCySAG Approach & Status

1. **Identify SCADA/PCS-unique characteristics**
2. **Select & analyze “best available” tools/methodologies**
  - ◆ Created methodology to evaluate cyber tools/methodologies
  - ◆ In-depth analysis of 9 tools/methodologies
3. **Identify requirement gaps**
4. **Prioritize and work to define requirements to fill gaps**

We are here

See conference USB key or reports at:  
<https://www.pcsforum.org/groups/68/library>

# Status – Two Highest Priority Unmet Needs

- ◆ **Staff cyber security training**
- ◆ **Risk identification and assessment**
  - Risk vs. vulnerability: vulnerability is a flaw or weakness that might allow an undesired consequence; risk characterizes likelihood and the severity of the consequence
- ◆ **Group identified other high priority needs – but believe they are getting adequate attention**
  - Access control
  - Vulnerability identification

# SCySAG Core Team

- ◆ Garill Coles  
Pacific Northwest National  
Laboratory  
[Garill.Coles@pnl.gov](mailto:Garill.Coles@pnl.gov)
- ◆ Mark C. Morgen  
3M - Optical Systems Division  
[mark.morgen@mmm.com](mailto:mark.morgen@mmm.com)
- ◆ Carol Muehrcke  
Cyber Defense Agency, LLC  
[cmuehrcke@cyberdefenseagen  
cy.com](mailto:cmuehrcke@cyberdefenseagen<br/>cy.com)
- ◆ Matt Earley  
Decisive Analytics Corporation  
[matt.earley@dac.us](mailto:matt.earley@dac.us)

- ◆ Ron Melton  
Decisive Analytics Corporation  
[ron.melton@dac.us](mailto:ron.melton@dac.us)
- ◆ 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)
- ◆ Mary S. Hester  
Intelligent System Solutions  
[mhester@issatlanta.com](mailto:mhester@issatlanta.com)



**Process Control Systems  
Industry Conference**

# Panel Discussion

# Process – Goal & Desired Outcome

## ◆ Panel focus areas

- Staff cyber security training
- Risk identification and assessment

## ◆ The goal of the panel session:

- Validation of the unmet needs
- What should be done?
- Who owns the issue?

SCySAG will capture the reasoning and use as basis for final WG recommendations

## Panel Experts

- ◆ **Mark Fabro, President & Chief Security Scientist, Lofty Perch**
- ◆ **Clifford Glantz, Senior Staff Scientist, Pacific Northwest National Laboratory**
- ◆ **Daniel C. Rees, Vice President, Scientech – A Curtiss-Wright Flow Control company**
- ◆ **Johan B. Nye, Control Systems Chief Engineer ExxonMobil Research and Engineering Co**

## Process - Steps

### ◆ 40 minutes: Process Control Staff Cyber Security Training

- 25 minutes: Panelists address topics selected from:
  - Describe the state of current training practices in your industry
  - What part do self assessment tools play for this topic?
  - What are the gaps in the state of the practice?
  - What part could advanced self assessment tools play to meet the need?
  - How important do you think it is to work the issue and why?
  - Who is best positioned to lead to work the issue?
- 15 minutes: Open discussion to address the outcomes:
  - Validation of the unmet need
  - What should be done?
  - Who owns the issue?
- Capture the comments

### ◆ Repeat for Process Control Cyber Risk Assessment



**Process Control Systems  
Industry Conference**

# Cyber Security Training

# PCS Cyber Security Training – Mark Fabro, Lofty Perch, Inc.

## ◆ Current Situation:

- What are the mandatory training guidelines? Frequency and Discipline are popular
- Training is exceptionally well done in some areas, both hands on and classroom
- Current tools do not address training in-depth, but best-of-breed provide continuous reference to training
- Not a realistic requirement for a technology-focused self-assessment tool

## ◆ Self Assessment tools:

- Should provide output to populate training curricula but not assess actual training content
- Can be used to build effective cross-training with existing resources (i.e. DHS CSSP Online Training)

## ◆ Ideal Case:

- Training is currently **not** a realistic requirement for a self-assessment tool
- Tool output used to shape existing (proven) CBK sets (work with private sector)
- Tools should be used to augment both standard IT **and** Engineering training disciplines

# Cyber Security Training – Cliff Glantz (PNNL)

## ◆ Current Situation in Nuclear Power Sector:

- Industry guidance exists, but implementation on a plant by plant basis seems to vary significantly
- NEI 04-04 Calls for awareness, technical, and specialized training
- Formal guidance on this topic has yet been released by the NRC.

## ◆ Coming Soon:

- 10 CFR 73.54(d)(1): *Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.*
- RG-5022 will provide more detailed guidance on this topic.

## ◆ Best positioned to solve:

- Will produce a consistently high level of cyber security training for this critical infrastructure sector
- Can serve as a model for other sectors.

# PCS Cyber Security Staff Training – Daniel Rees, Sciencetech Water Sector Experience

## ◆ **Current Situation:**

- Extensive training of industry in security issues, risk assessment and tools; (>2300 in VSAT™ alone)
- Many sector specific resources developed for security
- Cyber assessments not at forefront of initial security assessments; now evidence of increased interest and concern
- No “requirement” means long evaluation periods

## ◆ **Self Assessment tools:**

- Compliance with regulations / guidance tools exist; training available
- Needs to be integrated with consequence and vulnerability analysis to provide risk measures

## ◆ **Best positioned to solve:**

- Water Sector SC and GC with DHS
- Local, Regional and National exercises important



**Process Control Systems  
Industry Conference**

# **Risk Assessment**

# Risk Assessment – Mark Fabro, Lofty Perch, Inc.

## ◆ Defining Risk is the Problem

- Risk can be ascertained using any number of variables (stages of attack, skill of attacker, time to compromise, current value, etc)
- Risk is a probability (0 to 1) but variables have different measurement
- Little confidence about (a) risk or (b) the impact of countermeasures on risk
- Existing tools treat risk at a high level; insufficient to prioritize treatment of individual vulnerabilities (Ordinal only)
- Risk can be ‘gap’ between what you know to be vulnerable and what you do to reduce exposure

## ◆ Self Assessment tools:

- Use of consequence is subjective; tools provide ‘big picture’ numbers (i.e. for SAL)
- Variables of threat and vulnerability can be understood
- How does tool provide unit of measurement for ‘risk’?
- Would require agreed-to baseline (historical trending) data to work from

## ◆ Best positioned to solve:

- Industry partnership providing industry data sources
- Need to get incident data to help shape probability

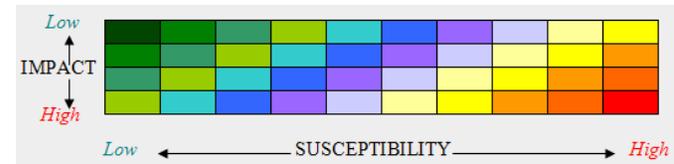
# Risk Assessment – Cliff Glantz (PNNL)

- **Current Situation in the Nuclear Power Sector:**

- Using NEI 04-04 guidance based on NUREG/CR-6847
- Will soon be updated with release of 10 CFR 73.54 and RG-5022

- **Self Assessment Process:**

1. Examine existing plant-wide cyber security practices
2. Identify critical digital assets
3. Conduct tabletop review and validation
4. Conduct susceptibility assessments
5. Conduct risk analysis
6. Conduct risk management activities



- **Best positioned to solve:**

- Can only work as part of a comprehensive cyber security program
- Encourages a comprehensive review of digital control system security
- Focuses resources + brainpower on this issue for an extended period.

# Risk Assessment – Daniel Rees, Scientech

## Water Sector Experience

### ◆ Current Situation:

- Virtually all Water Utilities have performed security risk assessments as required by Bio-Terrorism Response Act of 2002
- Most are evaluating next steps and approaches for continuous improvement and update of risk assessments – SSP compliance a future issue?
- Existing tools can support spending decisions - key issues is which threats are appropriate & regional / national “roll-up”
- Cyber risk is one of multiple assets classes considered – but most have focused on physical assets to date

Criticality Rating				Vulnerability Rating
1 Very High	2 High	3 Moderate	4 Low	
1A	2A	3A	4A	A Very High
1B	2B	3B	4B	B High
1C	2C	3C	4C	C Moderate
1D	2D	3D	4D	D Low

### ◆ Self Assessment tools:

- Tools exist and have been used (RAM-W, SEMS, VSAT™); CS<sup>2</sup>SAT
- Lack of expertise at some utilities in cyber security / risk assessment application an issue
- Need to tie existing “compliance” tools with risk evaluations as well as response planning

### ◆ Best positioned to solve:

- SSA – EPA; Water Sector Coordinating Council, SCC, and Government Coordinating Council, GCC; all in concert with DHS for standard approach

## Process –Steps (continued)

### ◆ Summary and wrap-up

- Summarize what we heard
- Describe next steps
- Questions:
  - How can SCySAG's results to date be leveraged?
  - Is there a future home for analysis work like that performed by SCySAG?

# Contact Information

Brian Isle, WG Chair  
Adventium Labs

[brian.isle@adventiumlabs.org](mailto:brian.isle@adventiumlabs.org)

Tel: 612-716-5604

Carol Muehrcke, co-Chair  
Cyber Defense Agency, LLC

[cmuehrcke@cyberdefenseagency.com](mailto:cmuehrcke@cyberdefenseagency.com)

Tel: 651-770-6736