

Process Control Systems Forum 2007 Annual Meeting

Process Control Systems Forum Welcome and PCSF Updates

**Michael Torppey
Technical Manager, PCSF &
Senior Principal, Noblis**

2007 Annual Meeting Program

- ◆ **Conduct Working and Interest Group workshops**
- ◆ **Disseminate information from other organizations/programs**
- ◆ **Provide meeting opportunities to other organizations in conjunction with PCSF**
- ◆ **Gather as a community to recognize challenges/issues, deliver resources, assist each other across organizations and assess solutions, establishing metrics and a baseline for the future**
- ◆ **Created and designed by PCSF Design Team to address most pressing issues, as defined by, solution seekers, and stimulate dialogue to solve these control system security concerns**

2007 Annual Meeting Program

◆ Developed under the guidance of the PCSF Design Team

- Determined goals and objectives for the Annual Meeting
 - Provide end-users with tactical and strategic solutions to the most pressing control system security concerns in the next 0-24 months
- Identified control system security concerns through Questionnaire
- Determined the top 4 areas of concern to end-users
 - Understanding Risk
 - Requirements/Operational Considerations
 - Architecture/Design
 - Devices/Components
- Reviewed and selected presentations/demonstrations from Solution Providers that addressed these areas
- On-site assistance here in Atlanta to achieve objectives

2007 Annual Meeting Program

◆ Facilitators

- Brian Mason, Mason Consulting Group
- Joann Byres, Byres Security

◆ Why they are here

Agenda – Plenary Session

- ◆ **Welcome and update on CSSP from DHS**
- ◆ **Keynote Address**
 - Bruce Landis, Deputy Assistant Secretary for Cyber Security and Telecommunications, Department of Homeland Security
- ◆ **Updates from PCSF Working and Interest Groups**
- ◆ **Control System Community Updates**

Agenda: Day One (PM)

◆ Interest and Working Group Sessions

- Control Systems Research
- Congress of Chairs
- SCADA Cyber Self-Assessment
- Education and Training
- Anti-Virus and Malware
- Control System Technical Security Metrics

◆ Reception

Agenda: Wednesday - Friday

◆ Wednesday

- Presentations and Demonstrations
- Water Sector Roundtable

◆ Thursday

- Plenary Session to review expectations for the day
- Feedback and Recommendations
- Concluding Plenary Session to discuss Feedback and Recommendations

◆ Thursday (post PCSF)

- International Electrotechnical Commission (IEC) TC65/WG10 Meeting
- Solutions for Process Control Security Training Session (pre-registration required)

◆ Friday

- International Electrotechnical Commission (IEC) TC65/WG10 Meeting
- Intermediate Control Systems Security Training Session (pre-registration required)

Meeting Output

◆ Key Findings/Recommendations

◆ Personal/Organizational Value

- Move solution seekers closer to implementing effective solutions, leave this meeting with prospective tools, resources and plans to utilize immediately
- Increase solution provider's awareness of solution seekers needs, requirements and environmental concerns to continue to build increasingly effective resources

◆ PCSF/Community Value

- Establish a benchmark of key metrics to share with the community in order to measure progress
- Utilize the PCSF support structure to work collaboratively and continually towards steps that can drive identification and adoption of effective solutions

◆ Summary Report

Details

- ◆ **Cell Phones**
- ◆ **Emergency Exits**
- ◆ **Breaks/Lunch/Reception**
- ◆ **Meeting Questionnaire (Survey)**
- ◆ **Presentations availability**

Meeting Guidelines

- ◆ **Recognize this is an open, public forum where all ideas/comments are valued contributions**
- ◆ **Speak up and leave your titles at the door**
- ◆ **Think outside of the box – build on each other's ideas**
- ◆ **Ensure that no action leaves the room without a name and date**
- ◆ **Be aware that this is a non-secure environment**
- ◆ **Do not divulge information that may be proprietary to your company**

Expectations of the PCSF in 2007

- ◆ **Increased community role as a one-stop resource center**
 - Develop Interest Group ideas and action items through collaboration, meetings and PCSF support mechanisms
 - Continue to share and add to the value of Working Group deliverables
 - Roadmap Central
 - Federal Coordination
- ◆ **Identify key metrics and deliverables and establish a baseline going forward**
- ◆ **Recognize that mature solutions exist and accelerate implementation and continuous enhancements**
- ◆ **Continuity of effort through PCSF support mechanisms**
- ◆ **Outreach/Liaison**

Honeynet Fun

◆ Simulates a PLC

- Modbus/TCP server with realistic points list
- Http, ftp, telnet and snmp support
- Developed by Digital Bond with support from CPNI
 - CPNI was formerly known as NISCC
- Deploy your own SCADA Honeynet
 - VMware server images at www.digitalbond.com

◆ Available at PCSF via a wireless access point

- SSID: dbelectric_7
- Check out the realism
- Hack away at it, the honeynet will capture your attacks

◆ Results from Honeywall Management console on Thursday

Governing Board Elections

- ◆ **Eight sectors represented, four are up for election in 2007**
 - Chemical Industry
 - Water and Waste Management
 - Vendor Community
 - Federal Government
- ◆ **Nominations collected starting today and ending on Friday, April 6**
- ◆ **Submitting Nomination**
 - Web site: www.pcsforum.org
 - Complete and drop-off the form in your packet to registration desk
 - Download and e-mail to secretariat@pcsforum.org
 - Fax to 703.610.2053

Process Control Systems Forum 2007 Annual Meeting

**Perry A. Pederson
Director, Control Systems Security Program
National Cyber Security Division
Department of Homeland Security**

Process Control Systems Forum 2007 Annual Meeting Keynote Presentation

**Bruce Landis
Deputy Assistant Secretary for
Cyber Security and Telecommunications
Department of Homeland Security**

Process Control Systems Forum Working and Interest Group Updates

Session Leads

Anti-Virus on Control Systems IG

Control Systems Research IG

Control System Technical Security Metrics IG

Education and Training IG

Congress of Chairs WG

SCADA Cyber Self- Assessment WG

Session Lead – Kevin Staggs

Chair – Dr. Ann Miller

Chair – Miles McQueen

Chair – Brian Lopez

Chair – Dr. William Rush

Chair – Mr. Brian Isle

Anti-Virus on Control Systems Interest Group

Kevin Staggs, CISSP
Engineering Fellow, Process Solutions
Honeywell Automation and Control

Anti-Virus on Control Systems IG

- ◆ **Better understand how anti-virus, anti-malware software is deployed in corporate enterprises**
- ◆ **Better understand how SCADA systems are deployed and connected to the enterprise**
- ◆ **Define anti-virus requirements for SCADA systems**

Control Systems Research Interest Group

**Dr. Ann Miller
Professor
University of Missouri-Rolla**

Control System Technical Security Metrics Interest Group

**Miles McQueen
Principal Investigator
Idaho National Laboratory
Miles.McQueen@inl.gov**

Control System Technical Security Metrics IG

◆ Agenda (Tuesday 1:00pm – 3:00pm)

- | | |
|------------------------------|--|
| – Miles McQueen, INL/CSSP | Introduction (10 m) |
| – Cliff Glantz, PNNL/I3P | I3P Metrics accomplishments (25 m) |
| – Ron Halbgewachs, SNL/NSTB | Security metrics taxonomy (25 m) |
| – Eric Byres, Byres Security | MTTC metric: R&D (25 m) |
| – Wayne Boyer, INL/CSSP | Security ideals & baseline set of technical metrics (25 m) |
| – Miles McQueen, INL/CSSP | Open discussion and closeout (10 m) |

◆ Goals:

- Brief participants on work to date in security metrics development (National labs and Byres security)
- Discuss our proposed baseline set of technical security metrics and associated security Ideals
- Form collaborations for further definition and development of control system security metrics
 - Refine metrics
 - Develop examples of how to measure
 - Measurement tool needs?
 - Field trials

Education and Training Interest Group

Brian Lopez
Leader, Vulnerability & Risk Assessment Program
Lawrence Livermore National Laboratory

Education and Training IG

- ◆ **Now Available: "Critical Infrastructure and Control Systems Security Curriculum" developed by a multi-disciplinary group under DHS sponsorship.**
- ◆ **Six modules focused on:**
 - Vulnerability
 - Engineering Approaches
 - Managing Organizations and Risk
 - Securing Networks of Enterprises
 - Creating Markets
 - Building Trust, Public/Private Policy

Education and Training IG

- ◆ **Each module provides**
 - Objectives
 - Key questions
 - Supporting readings
- ◆ **Detailed annotated bibliography to guide further investigation**
- ◆ **Multiple ways to leverage**
 - Corporate training
 - Background to get up-to-speed on issues
 - Academic teaching, etc
- ◆ **Entire curriculum (including all supporting materials) available for free to all attendees**

Education and Training IG

◆ Brainstorm future efforts

- What are our most important needs in the education and training arena?
- We will brainstorm and rank potential efforts for the coming year and determine pathways to achieve them.

The Congress of Chairs Facilitates Multiple Standards Activities

Bill Rush, Chair

*March 6, 2007
Atlanta, Georgia*

**The Goal Is A “Single Point Of Contact For
Standards Information”**

The CoC Seeks To Help Facilitate Standards Work

- ◆ A DHS PCSF Working Group
- ◆ Consisting Of Standards Group Chairs
- ◆ Seeking To Help Compatible Standards
- ◆ By Sharing Ideas Informally
- ◆ And Not Needing “One More Meeting”

CoC Helps “Security Users”

- ◆ **Standards Insight For Owners & Vendors**
- ◆ **Tracking 100 Standards Is Hard**
- ◆ **But Information Is Still Vital To Have**
- ◆ **CoC Is “One Stop Information”**
- ◆ **One FEWER, Not One More Meeting**

CoC Made Progress In 4 Areas

- ◆ **Combined Glossary**
- ◆ **Liaison With IEC Links CoC To International Work**
- ◆ **Inter-Committee Coordination**
- ◆ **Activity Status Site (*Demo Today*)**



- About PCSF
- Participants
- Governance Body
- News
- PCSF Report
- Calendar of Events
- PCSF User Account
- Terms of Use

- Interest Groups
- Working Groups
- Working Group Deliverables
- Reference Library

Google™

www.pcsforum.org

Control Systems Standards Activities Database

[List All](#) | [Search](#) | [Add](#) | [Activi](#)

We welcome your recommendations for improvement, please use the [feedback form](#)
 PCSF Congress of Chairs List of Cyber Security Activities.

Title ?	Sponsor ?	Data Manager ?	Support Item ?	AC ?	UC ?	DI ?	DC ?	RDF ?	TRE ?	NRA ?	Status ?	Date Last Updated ?
Cryptographic Protection of SCADA Communications, Part 1: Background, Policies, and Test Plan	AGA	Dr. William Rush	AGA 12, Part 1	✓	✓	✓	✓	✗	✓	✗	Complete	2006-0
Cryptographic Protection of SCADA Communications, Part 2: Retrofit Link Encryption for Asynchronous Serial Communications	AGA	Dr. William Rush	AGA 12, Part 2	✓	✓	✓	✓	✗	✓	✗	In Progress	2006-0
Cryptographic Protection of Protection of	AGA	Dr. William Rush	AGA 12, Part 3	✓	✓	✓	✓	✓	✓	✗	Not Started	2006-0

- About PCSF
- Participants
- Governance Body
- News
- PCSF Report
- Calendar of Events
- PCSF User Account
- Terms of Use
- Interest Groups
- Working Groups
- Working Group Deliverables
- Reference Library

Google™

WWW
pcsforum.org

Title: IEEE Trial Use Standard for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access

[Update](#) | [Delete](#) | [Back to List](#)

Sponsor ⓘ	IEEE PSSC
Participants ⓘ	PSRC and PSCC
Relevant Sector ⓘ	Electricity, Other (Any SCADA System Operating over Asynchronous Serial Communications and Dial-up to Field Device Maintenance Ports)
Data Manager ⓘ	Mr. Dennis Holstein
Supports ⓘ	IEEE P1689
Standard/Report ⓘ	Standard
Description ⓘ	General requirements to protect serial communications between master stations and remote terminal units from cyber attack, and to strengthen authenticated remote access to maintenance ports in RTUs (Remote Terminal Units) and other IEDs (Intelligent Electronic Devices).
Requirements Addressed ⓘ	
AC (Access Control) ⓘ	✓
Additional Text	[Strong requirements for two factor authentication to access field device maintenance ports. The retrofit solution acts as a guard to maintain a secure channel of communications. It leaves intact the password permissions built into the receiving IED.]
UC (Use Control) ⓘ	✓
Additional Text	[Use control is weakly addressed because it does not address the specific requirements for digital certificates.]
DI (Data Integrity) ⓘ	✓
Additional Text	[Strong data integrity requirements are specified for both access to maintenance ports and for SCADA data between the master station and RTU.]
DC (Data Confidentiality) ⓘ	✓
Additional Text	[Strong data confidentiality requirements for both SCADA communications and dialup to the field device maintenance ports.]

The Status Project Provides Updated Status Of Other Groups

- ◆ **Track Process Control Security Work**
 - Identify Sponsor And Point Of Contact
 - Show Work Product (*Standard, Guide, Recommended Practice, Report, Technical Paper, Etc.*)
 - End User Requirements Addressed
 - Status Of Work
 - Qualifying Remarks
- ◆ **Learn To Use The Web Site At CoC Session**

SCADA Cyber Self-Assessment (SCySAG) Working Group

Brian Isle
Chief of Operations
Adventium Labs
Brian.isle@adventiumlabs.org
<https://www.pcsforum.org/groups/68>

Agenda

- ◆ **Why SCySAG**
- ◆ **SCySAG Objective**
- ◆ **Approach & Status**

Why SCySAG?

- ◆ **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.

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.

SCySAG Approach & Status

1. Identify SCADA/PCS-unique characteristics
 2. Select & analyze “best available” tools/methodologies
 3. Identify requirement gaps
 4. Prioritize and work to define requirements to fill gaps
- ← We are here

See reports at:
<https://www.pcsforum.org/groups/68/library>

SCySAG – Expected Impact

The results of this effort can be used by:

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

SCySAG – Atlanta Workshop

- **Review of results to date**
 - Available self-assessment tools/methods and what they cover
 - Areas of requirements not covered by available tools/methods
- **Complete prioritization of requirement gaps**
 - Your input is needed, please attend the workshop
 - Focus: Water and waste water, Chemicals, Refining & petrochemical, Oil & gas, and Cross-sector
- **Plans to define requirements to cover gaps**

SCySAG

PCS Cyber Security Assessment Requirements Workshop

Tuesday 1:00 pm – 3:00 pm

Contact Information

Brian Isle, WG Chair

Adventium Labs

brian.isle@adventiumlabs.org

Tel: 612-716-5604

Carol Muehrcke, co-Chair

Cyber Defense Agency, LLC

cmuehrcke@cyberdefenseagency.com

Tel: 651-770-6736

Control Systems Community Updates

Process Control Systems Forum 2007 Annual Meeting

**Closing Comments
Michael Torppey**

Tuesday, March 6 - Afternoon

- ◆ Working and Interest Group Workshops
- ◆ Evening Networking Reception