



**PCSF 2005 Fall Meeting**  
**McCormick Place, Lakeside Center**  
**Chicago, IL**  
**Schedule of Events**

Tuesday, October 25

10:00 a.m. – 5:30 p.m.

**PCSF Exhibit Booth #2029**  
**ISA EXPO 2005 Exhibit Floor**

A complete schedule of events for the ISA EXPO is available at: [ISA EXPO 2005](#)

**4:30 p.m. – 5:00 p.m. (ISA Conference Registration Required for Entry to this Session)**

**PCSF Overview - Self Assessment Development, Process, Standards, and Tools Interest Group**

**Chair: Brian A. Isle**, Chief of Operations, Adventium Labs :: [Bio](#) ::

Mr. Isle will provide participants with an overview of the goals of this PCSF Interest Group. All who wish may attend the group's meeting on Thursday, October 27.

This Interest Group will develop requirements for SCADA cyber self assessment tools and methodologies that can be used to strengthen critical infrastructure. As a Working Group, we will look broadly across the sectors (including regulated and non-regulated industries) to review current and past assessment work, and incorporate end-user interaction to develop the requirements. The IG and eventual WG will be an open, industry-driven process and will utilize broad industry, lab, and government participation to ensure that a cross-domain requirement set is delivered. These requirements will be available for use 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.

**4:30 p.m. – 5:00 p.m. (ISA Conference Registration Required for Entry to this Session)**

**Preliminary Results of Tests of Cryptographic Modules on Legacy SCADA Systems**

**Speaker: Bill Rush**, Institute Physicist, Gas Technology Institute & Vice Chair, Process Control Systems Forum :: [Bio](#) ::

The American Gas Association (AGA) has developed the AGA 12 encryption suite as an industry-recommended practice to protect SCADA data and commands by providing message confidentiality, integrity, and authenticity. The current technical specification applies to asynchronous serial data communications and protects existing SCADA systems through the use of retrofit hardware installed between the SCADA system components and the communication network. Laboratory tests have established the functionality of the AGA 12 protocols, and shown that the degradation introduced by using AGA 12-compliant cryptography is negligible for the range of operating speeds of most SCADA systems. AGA 12-compliant modules show similar results in field tests. Features that make the suite "SCADA friendly" include the ability to retrofit to existing systems, the potential to selectively deploy protection to only critical sites, (limited) interoperability among different manufacturers, high speed, low cost, and compatibility with future versions that will be embedded in new equipment.

Wednesday, October 26

10:00 a.m. – 5:30 p.m.

**PCSF Exhibit Booth #2029**  
**ISA EXPO 2005 Exhibit Floor**

|  |  |
|--|--|
| <p><b>4:30 p.m. – 5:00 p.m. (ISA Conference Registration Required for Entry to this Session)</b></p> <p><b>PCSF Overview - Control System Security Event Monitoring</b></p> <p><b>Chair:</b> Dale Peterson, Director, Network Security Practice, Digital Bond, Inc. :: <a href="#">Bio</a> ::</p> <p>Detecting attacks on control systems is critical because many of the applications and protocols have inherent vulnerabilities. Security Event Management (SEM) products and Managed Security Services collect and correlate data from traditional IT sources. The interest group will look to leverage the existing solutions and find ways to augment these solutions with control system detection sources and correlation intelligence. Good practices, information sharing, product and service solutions, and case studies will help asset owners detect cyber attacks on the critical infrastructure.</p> | <p><b>4:30 p.m. – 5:00 p.m. (ISA Conference Registration Required for Entry to this Session)</b></p> <p><b>PCSF Overview - Control Systems Research Interest Group</b></p> <p><b>Chair:</b> Dr. Ann Miller, Professor, University of Missouri - Rolla :: <a href="#">Bio</a> ::</p> <p>Dr. Miller will provide participants with an overview of the goals of this PCSF Interest Group. All who wish may attend the group's meeting on Thursday, October 27.</p> <p>This session will address the newly formed PCSF Interest Group on Control Systems Research and will highlight areas of both basic and applied research in methodologies and technologies related to control systems, including SCADA systems and critical infrastructures. Specific areas include security, safety, reliability, and dependability.</p> |
|--|--|

**Thursday, October 27**

**Please note that all PCSF Interest Group Meetings and Presentations are included in Complimentary EXPO Exhibition Registration**

**10:00 a.m. – 3:30 p.m.**

**PCSF Exhibit Booth - #2029  
ISA EXPO 2005 Exhibit Floor**

|   |  |  |
|---|--|--|
| <p><b>Room E352, Lakeside Center</b></p> <p><b>8:00 a.m. – 10:00 a.m.</b></p> <p><b>PCSF Update, Department of Homeland Security Perspective, and the SAFETY Act</b></p> <p><b>Presenters:</b> Michael Torppey, Senior Principal, Mitretek Systems &amp; Technical Director, Process Control Systems Forum (PCSF) :: <a href="#">Bio</a> ::<br/> Peter Miller, Director, Mission Support Office, HSARPA, Science and Technology, Department of Homeland Security :: <a href="#">Bio</a> ::<br/> David A. McWhorter, Ph.D., Research Staff Member, Operational Evaluation Division, Office of SAFETY Act Implementation :: <a href="#">Bio</a> ::<br/> Michael Friedman, Esq., Special Assistant to the Director, Office of SAFETY Act Implementation (OSAI) :: <a href="#">Bio</a> ::</p> <p>This session will provide participants with an update on the activities of the PCSF since its first meeting in May 2005 including an update on the International Standards Coordination Meeting and PCSF Interest Group progress. Additionally, members of the Office of SAFETY Act Implementation (OSAI) will provide a detailed presentation explaining the potential importance of the SAFETY Act to the control systems community, the application process, and the evaluation process. The SAFETY Act is designed to encourage the development and deployment of anti-terrorism technologies.</p> |  |  |
|---|--|--|

|   |   |   |
|---|---|---|
| <p><b>10:00 a.m. – 11:00 a.m., Room E352, Lakeside Center</b></p> <p><b>Developing a Security Exposure Self-Assessment Tool</b></p> <p><b>Presenters:</b> Candace Chan-Sands, Program Manager, EMA, Inc. :: <a href="#">Bio</a> ::<br/> Matt Earley, Security Consultant, Decisive Analytics Corp. :: <a href="#">Bio</a> ::</p> <p>A beta version of a Process Control Security Exposure Self-Assessment Tool has been developed as part of the Water Environment Research Foundation/AwwaRF 03-CTS-3SCO research project. The project was designed to determine current process control system vulnerabilities and consequences and to quantify them for the water and wastewater sector. This session will provide an overview of the project, its objectives, the technical approach used to design and develop the tool, challenges, and next steps.</p> | <p><b>10:00 a.m. – 11:00 a.m., Room E353B, Lakeside Center</b></p> <p><b>Control Systems Research Interest Group</b></p> <p><b>Chair:</b> Dr. Ann Miller, Professor, University of Missouri - Rolla :: <a href="#">Bio</a> ::</p> <p>This second meeting of the PCSF Control Systems Research Interest Group will highlight areas of both basic and applied research in methodologies and technologies related to control systems, including SCADA systems and critical infrastructures. Specific areas to be covered include security, safety, reliability, and dependability.</p> | <p><b>10:00 a.m. – 11:00 a.m., Room E353C, Lakeside Center</b></p> <p><b>System Analysis and Modeling Interest Group</b></p> <p><b>Chair:</b> Dennis Holstein, Publisher, OPUS Publishing :: <a href="#">Bio</a> ::</p> <p>This Interest Group will develop case studies of the enterprise as a whole to define the common cyber-security requirements that extend the company security policy to all domains and organizational units of the enterprise.</p> |
|---|---|---|

|   |   |  |
|---|---|--|
| <p><b>11:00 a.m. – 12:00 p.m., Room E352, Lakeside Center</b></p> <p><b>Self Assessment Development, Process, Standards, and Tools Interest Group</b></p> <p><b>Chair: Brian A. Isle</b>, Chief of Operations, Adventium Labs :: <a href="#">Bio</a> ::</p> <p>This Interest Group will develop requirements for SCADA cyber self assessment tools and methodologies that can be used to strengthen critical infrastructure. As a Working Group, we will look broadly across the sectors (including regulated and non-regulated industries) to review current and past assessment work, and incorporate end-user interaction to develop the requirements. The IG and eventual WG will be an open, industry-driven process and will utilize broad industry, lab, and government participation to ensure that a cross-domain requirement set is delivered. These requirements will be available for use by:</p> <ul style="list-style-type: none"> <li>• Tool and methodology vendors to develop, deploy, and maintain an assessment solution,</li> <li>• SCADA system vendors to create more secure systems,</li> <li>• Standards bodies and groups, and</li> <li>• Owner/operators developing their internal policies and procedures</li> </ul> | <p><b>11:00 a.m. – 12:00 p.m., Room E353B, Lakeside Center</b></p> <p><b>Business Case Analysis Interest Group</b></p> <p><b>Chair: Evan Hand</b>, Electrical CFL Leader, Kraft Foods, Inc. :: <a href="#">Bio</a> ::<br/> <b>Mark Heard</b>, Engineering Associate, Eastman Chemical Company :: <a href="#">Bio</a> ::</p> <p>This meeting will provide an update of the Business Case Analysis Interest Group and activities to date. Participants will assist in refining objectives and developing a group charter to further progress toward evolving from an Interest Group to a Working Group.</p>   | <p><b>11:00 a.m. – 12:00 p.m., Room E353C, Lakeside Center</b></p> <p><b>Anomaly Detection Improves Process Control Security</b></p> <p><b>Presenter: Ron Derynck</b>, Director Product Strategies, Verano :: <a href="#">Bio</a> ::</p> <p>Unlike other computer networks, control systems normally exhibit stable, predictable characteristics. Any deviations indicate either a performance problem or a possible security breach. Attempted penetrations, viruses, worms, and Trojans leave telltale signs that can be detected. This presentation examines how anomaly detection can effectively improve process control system security.</p> |
| <p><b>12:00 p.m. – 1:00 p.m.</b><br/> <b>LUNCH ON YOUR OWN</b></p>  |   |  |
| <p><b>12:00 pm – 1:00 pm. Room E353C, Lakeside Center</b></p> <p><b>US-CERT Control System Security Center Industry Group Interest Group</b></p> <p><b>Chair: Jeffrey (Jeff) Hahn</b>, Industry Outreach Lead, Control System Security Center, Idaho National Laboratory :: <a href="#">Bio</a> ::</p> <p>The Department of Homeland Security (DHS), US-CERT Control Systems Security Center (CSSC), will present key segments of the program to industry. The DHS has been given the responsibility to increase security of the United States' critical infrastructures. This interest group provides a vehicle for anyone in industry to learn more about the DHS US-CERT CSSC program and to provide input into its direction and product development.</p>   | <p><b>12:00 pm – 2:00 pm, Room 353B, Lakeside Center</b></p> <p><b>Key Management Infrastructure – The Challenge of Managing Large-scale Cyber Security</b></p> <p><b>Panel Facilitator: Dennis Holstein</b>, Publisher, OPUS Publishing :: <a href="#">Bio</a> ::</p> <p><b>Panelists:</b> <b>Gus K. Lott</b>, Principal Engineer, YarCom, Inc.<br/> <b>Paul M. Skare</b>, Product Manager, Siemens Power Transmission &amp; Distribution, Inc.<br/> <b>Jay Wack</b>, Chief Evangelist, TecSec :: <a href="#">Bio</a> ::</p> <p>The challenge of managing large-scale cyber security for the asset owner's enterprise is the hottest topic on the radar screen. We are looking for a comprehensive solution that is based on one security policy with extensions for specific organizations and operations centers, thus avoiding stove-pipe solutions. The solution must suit not only small and medium businesses, but large businesses with complex partnership relationships and interactions with independent system operators and government regulation agencies, and must take into account the trend to outsource critical operational functions, such as protection device settings, to third parties. The hot-button key management issues that have surfaced are legal responsibilities, failure and recovery aspects, and how to manage assured identity; widely distributed platform/device locations requiring keying materials; and controlling regulatory permissions. The panelists will provide insight into these questions and will then answer questions from the floor. Given the controversial nature of these issues, we expect to hear diverging and adversarial opinions on how best to address these issues. Bring your hard hat: This should get exciting!</p> |  |
| <p><b>1:00 p.m. – 2:00 p.m., Room E353C, Lakeside Center</b></p> <p><b>Control System Security Event Monitoring</b></p> <p><b>Chair: Dale Peterson</b>, Director, Network Security Practice, Digital Bond, Inc. :: <a href="#">Bio</a> ::</p>   | <p><b>1:00 p.m. – 3:00 p.m., Room E352, Lakeside Center</b></p> <p><b>Meet the Office of SAFETY Act Implementation (OSAI)</b></p> <p>Members of the OSAI will be available to meet with individuals who have additional questions or would like additional information regarding the SAFETY Act.</p>  | <p><b>1:00 p.m. – 5:00 p.m., Room E256, Lakeside Center</b></p> <p><b>Congress of Chairs Interest Group</b></p> <p><b>Chair: Bill Rush</b>, Institute Physicist, Gas Technology Institute &amp; Vice Chair, Process Control Systems Forum :: <a href="#">Bio</a> ::</p>  |

|  |  |   |
|--|--|---|
| <p>Detecting attacks on control systems is critical because many of the applications and protocols have inherent vulnerabilities. Security Event Management (SEM) products and Managed Security Services collect and correlate data from traditional IT sources. The interest group will look to leverage the existing solutions and find ways to augment these solutions with control system detection sources and correlation intelligence. Good practices, information sharing, product and service solutions, and case studies will help asset owners detect cyber attacks on the critical infrastructure.</p>   | <p><b>David A. McWhorter, Ph.D.</b>, Research Staff Member, Operational Evaluation Division, Office of SAFETY Act Implementation<br/> <b>Michael Friedman, Esq.</b>, Special Assistant to the Director, Office of SAFETY Act Implementation (OSAI)</p>   | <p>This Interest Group provides the opportunity for the international standards bodies and related study committee members to gather, exchange information, and discuss work-in-progress and work planned in cyber security standards associated with critical control systems. By opening the lines of communication across industry sectors, duplication of efforts will be avoided and inconsistent standards will be eliminated. This group will help to accelerate the design, development, and deployment of more secure control systems, including the security of legacy systems.</p>   |
| <p><b>2:00 p.m. – 3:00 p.m., Room E353C, Lakeside Center</b></p> <p><b>Virtual Control System Environment</b></p> <p><b>Presenter:</b> <b>Ray Parks</b>, Member, Technical Staff, Center for SCADA Security, Sandia National Laboratories :: <a href="#">Bio</a> ::</p> <p>This session will describe the Virtual Control System Environment (VCSE) project at Sandia's Center for SCADA Security (CSS). The session will include discussion of why we are building the VCSE, the VCSE architecture, how it works with the CSS Test Bed, and how others will be able to use the VCSE.</p>  | <p><b>2:00 p.m. – 3:00 p.m., Room E353B, Lakeside Center</b></p> <p><b>Safe Zone for Critical Information Sharing Interest Group</b></p> <p><b>Chair:</b> <b>Rita Wells</b>, Critical Infrastructure Assurance, Idaho National Laboratory :: <a href="#">Bio</a> ::</p> <p>The objective of this interest group is to assess how best to create a safe zone for sharing critical information. Specific topics of interest include: trade-offs between maintaining security and sharing best practices; secure mechanisms for sharing of critical information; legal issues associated with sharing information; institutional impediments to sharing best practices and relevant incidents; finding a meaningful manner of exchange for sharing process control security events, incidents, audit logs, etc.; and creating a database of relevant industrial cyber events.</p>   | <p>Scheduled topics include:</p> <ul style="list-style-type: none"> <li>• <b>Common Glossary Project</b> - These are combined terms and acronyms from glossaries to save duplicating efforts, avoid conflicts, and simplify standards development.</li> <li>• <b>Standards Situation Assessment Mapping:</b> <ul style="list-style-type: none"> <li>○ <i>DHS US-CERT Control System Security Center Standards Comparison Study</i> -- This session will present the results of the DHS US-CERT Control System Security Center Standards Comparison Study, which compared various control system security standards with each other and with the Control System Security Center Framework Cyber-requirements. This session will provide an opportunity for the standards community to review and comment on the study and the state of standards development. <b>Presented by: Kevin Robbins</b> :: <a href="#">Bio</a> ::, Information Operations Red Team and Assessments, Sandia National Laboratories</li> </ul> </li> </ul> |
| <p><b>3:00 p.m. – 4:00 p.m., Room E353B, Lakeside Center</b></p> <p><b>Secure Wireless Technology for Use in Process Control Systems</b></p> <p><b>Presenter:</b> <b>Wayne Manges</b>, Oak Ridge National Laboratory :: <a href="#">Bio</a> ::</p> <p>This presentation will cover the various issues surrounding the use of wireless technology in process control systems and will provide a summary of relevant wireless technologies, both current and future. The session will take a systems-level approach and will discuss the need to effectively combine reliability, latency, throughput, and security for a complete system design. We will discuss how these four factors can be fused to provide wireless communications support to process control systems in a secure way.</p> | <p><b>3:00 p.m. – 5:00 p.m., Room E35CB, Lakeside Center</b></p> <p><b>Education Development Workshop<br/>Education and Training Interest Group</b></p> <p><b>Chair:</b> <b>John H. Saunders, Ph.D.</b>, Professor and Director, Center for Information Assurance &amp; Information Resources Management, College, National Defense University :: <a href="#">Bio</a> ::</p> <p>Participants will be updated on Education and Training Interest Group objectives, such as the creation of information and knowledge stores in control systems security education and training. Opportunities to prioritize and assist in further development of objectives will be offered. Interested parties are encouraged to join the Education and Training Interest Group. Information and activities to date are located at <a href="https://www.pcsforum.org/groups/iglist.php">https://www.pcsforum.org/groups/iglist.php</a></p> |   |
| <p><b>4:00 p.m. – 4:30 p.m., Room E353B, Lakeside Center</b></p> <p><b>Cyber-security of Rail Control Systems</b></p> <p><b>Presenters:</b> <b>Dave Teumim</b>, President, Teumim Technical, LLC :: <a href="#">Bio</a> ::<br/> <b>Fred Woolsey</b>, LTK Engineering Services</p> <p>The control security issues faced by rail transit, whether subway, light rail, or intercity rail, resemble those faced by other PCSF sectors, such as utilities. The use of COTS products in railway SCADA systems, the use of wireless systems to monitor and control trains, and the secure connection of transit control systems to enterprise systems are some of the hot issues.</p>   |  |   |

This session will explore commonality of these rail issues with existing PCSF sectors and will seek partners for mutual problem-solving.