



2006 Spring Meeting  
June 6 – 7 • La Jolla, CA  
Sessions and Workshops  
*Industrial Cyber Security Research Consortium: June 5*  
*PCSRF Meeting and I3P Workshop: June 8*  
(As of May 11, 2006. Subject to change.)

## Monday, June 5, 2006

**12:00 pm – 7:00 pm: Registration and Information Open**

**1:00 pm – 4:00 pm**

### **Industrial Cyber Security Research Consortium Meeting**

Eric Byres, cyber security researcher and professional engineer, will discuss the creation of a member organizations' consortium for facilitating research and certification testing for cyber security of SCADA, process automation, and industrial control systems. The consortium will consist of petrochemical, energy, and critical infrastructure organizations and will help in sharing research outcomes, knowledge, and best practices for the benefit of all member organizations. For additional information, please contact Joann Byres at [jbyres@wurldtech.com](mailto:jbyres@wurldtech.com)

**Speaker:** **Eric Byres**, Director of Industrial Cyber Security, Wurldtech Analytics Inc. – [Bio](#)

**5:00 pm – 5:45 pm**

### **PCSF Orientation**

Those new to the PCSF are encouraged to attend this useful introductory session, organized by the PCSF Secretariat to provide background on the formation of the PCSF; an explanation of the unique value, goals, and objectives the Forum brings to the control systems community; and an overview of the tools and information resources available to participants.

**Presenter:** **Michael Torppey**, PCSF Technical Manager & Senior Principal, Mitretek Systems, Inc. – [Bio](#)

**6:00 pm – 7:00 pm**

### **PCSF Working & Interest Group Chairs Session**

This session will provide information and updates on PCSF resources and support tools, including the Web site, meeting options, funding opportunities, marketing/participant building, IG to WG transition process, and more. This session also provides an opportunity to cross-connect Chairs and Group activities.

**Presenter:** **Michael Torppey**, PCSF Technical Manager & Senior Principal, Mitretek Systems, Inc. – [Bio](#)

## Tuesday, June 6, 2006

**7:00 am – 7:45 am: Continental Breakfast**

**7:00 am – 5:00 pm: Registration and Information Open**

**7:00 am – 5:00 pm: SAFETY Act and You**

David McWhorter of the Office of SAFETY Act Implementation (OSAI) will be available throughout the meeting to talk one-on-one with interested companies about 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.

**12:00 pm – 12:45 pm: Lunch**

**6:00 pm – 8:00 pm: Welcome Reception**

Enjoy an evening reception pool including an assortment of delicious food, excellent conversation, and a one hour hosted soft drink, beer, and wine bar provided by the Hilton La Jolla Torrey Pines Hotel. A cash bar will be available after 7:00pm.

**8:00 am – 5:15 pm**

### PLENARY SESSION

#### Keynote Presenters

Leading executives share their perspectives on overcoming the challenges of embracing a pervasive security management approach, how to deal with the unique challenges to securing control systems, and what hurdles are facing the control systems community.

**Speakers:** **William P. Crowell**, Independent Consultant & Former Deputy Director, National Security Agency – [Bio](#)  
**Dr. Paul Dorey**, Vice President of Digital Security & Chief Information Security Officer, BP p.l.c. – [Bio](#)  
**Margaret (Peg) E. Grayson**, President of AEP Government Solutions Group & Executive Vice President of AEP Networks – [Bio](#)

---

### PCSF Update & Working Group and Interest Group Updates

The PCSF Secretariat will provide participants with an overview of the Forum's accomplishments during the past year. In addition Working and Interest Group Chairs will provide updates on their accomplishments to date and will share with attendees an overview of goals and objectives for their Groups' workshops on Wednesday, June 7.

**Speakers:** **Michael Torpey**, PCSF Technical Manager & Principal, Mitretek Systems, Inc. – [Bio](#)  
**Ernie Rakaczky**, Director of Control System Security, Invensys Systems Canada, Inc. & Member, PCSF Spring Meeting Design Team – [Bio](#)  
**Dennis Holstein**, Publisher, OPUS Publishing – [Bio](#)  
**Brian Isle**, Chief of Operations, Adventium Labs – [Bio](#)  
**Dale Peterson**, Director, Digital Bond, Inc. – [Bio](#)  
**Bill Rush**, Institute Physicist, Gas Technology Institute & PCSF Vice Chair – [Bio](#)

2006 Spring Meeting  
June 6 – 7 • La Jolla, CA  
Sessions and Workshops  
*Industrial Cyber Security Research Consortium: June 5  
PCSRF Meeting and I3P Workshop: June 8  
(As of May 11, 2006. Subject to change.)*

---

## Vulnerability Disclosure Session – First SCADA Disclosure: A Case Study, Panel Discussion, and Workshops

### First SCADA Disclosure: A Case Study

Although numerous claims have been made about SCADA product vulnerabilities, few details have been publicly released, and national coordination centers (CERTs) have yet to issue a single advisory for a control system hardware or software flaw. During Fall 2005, Digital Bond discovered a number of security bugs in a popular utility infrastructure protocol that impacted multiple SCADA vendors and a significant user base. Shortly thereafter, the process began of notifying impacted vendors and working with vulnerability coordination centers to assess the impact of these flaws and define a process of releasing this information to a wider audience. During this talk, the presenter will provide detailed “behind the scenes” information such as response timelines, summary of vendor/CERT communications, and actions to measure the effectiveness of current response procedures and frame the debate within the control system security community.

**Presenter:** **Matt Franz**, Senior Security Consultant, Control Systems Security Practice, Digital Bond, Inc. – [Bio](#)

### Panel Discussion & Debate

Four panels representing control system vendors, national coordination centers, security researchers, and asset owners will discuss and debate the central questions regarding the disclosure and dissemination of information on control system vulnerabilities:

- Should end users be notified of vulnerabilities before a fix is available?
- What is a reasonable code of conduct for vulnerability researchers who find flaws in products used in critical infrastructure?
- Is “silent fixing” ever an appropriate vendor response?
- What level of information should be released publicly regarding control system vulnerabilities? When?
- What are acceptable timelines for vendors to respond and fix externally reported software vulnerabilities?
- Should support contracts be required for end users to get security fixes?

**Moderator:** **Matt Franz**, Senior Security Consultant, Control Systems Security Practice, Digital Bond, Inc. – [Bio](#)

**Panelists:** **Eric Byres**, Director of Industrial Cyber Security, Wurdtech Analytics Inc. – [Bio](#)

**Ralph Mackiewicz**, Vice President, SISCO, Inc. – [Bio](#)

**Art Manion**, Internet Security Analyst, CERT Coordination Center – [Bio](#)

**Ernie Rakaczky**, Director of Control System Security, Invensys Systems Canada, Inc. & Member, PCSF Spring Meeting Design Team – [Bio](#)

**Francisco Ramirez**, Senior Security Consultant, Securicon, LLC – [Bio](#)

**Karl Williams**, Senior Security Adviser, National Infrastructure Security Coordination Centre (NISCC) – [Bio](#)

### Breakout Workgroup Sessions

On Wednesday, June 7, there will be two back-to-back work sessions for vendors/researchers, asset owners, and coordination centers to define an action plan for developing and enhancing procedures for responding to control system-specific vulnerabilities.

---

### Security Testing Panel

The move to open systems for SCADA and control systems has enabled multiple systems and applications to be integrated together into a more complete and efficient control system. This integration also has presented some significant security risks to those systems that are now interconnected. There is a need to develop a security standard that integrated SCADA and control systems are required to meet. Once

**2006 Spring Meeting  
June 6 – 7 • La Jolla, CA  
Sessions and Workshops**  
*Industrial Cyber Security Research Consortium: June 5  
PCSRF Meeting and I3P Workshop: June 8  
(As of May 11, 2006. Subject to change.)*

this standard is developed, a standard security test harness can be utilized to verify that integrated systems are meeting the security standard. This panel will propose a minimum technical security standard for integrated systems and the test tools and methodologies to test against this standard.

**Speakers:** **Eric Byres**, Director of Industrial Cyber Security, Wurdtech Analytics Inc. – [Bio](#)  
**Matt Franz, CISSP**, Senior Security Consultant, Control Systems Security Practice, Digital Bond, Inc. – [Bio](#)  
**Kevin Stags, CISSP**, Engineering Fellow & Control Systems Solution Planner, Honeywell Process Solutions – [Bio](#)

---

### **The CIGRE B5 WG 22 Survey-Based Study of Wi-Fi Use and Plans for Protection and Automation in Electric Power Substations**

The CIGRE B5 Committee has convened Working Group 22 to develop a tutorial document concerning the use of wireless (Wi-Fi) communications in electric power substations, under the chairmanship of Dennis Holstein. The Working Group (WG) members include representatives from the United States, Canada, and Europe.

To assist in documenting the current status of Wi-Fi use, the Newton-Evans Research Company—whose president, Charles Newton, is the secretary of this WG—has agreed to undertake a survey of world electric power utilities to determine current and planned usage of Wi-Fi in electric power substations.

The study findings presented to the PCSF include representation from scores of North American utilities as well as utilities from throughout Europe, the Asia-Pacific Region, Latin America, and the Middle East and Africa.

This presentation will review highlights of the study findings, covering issues such as current use and practices related to Wi-Fi and planned use of wireless communications usage in electric power substations.

**Speaker:** **Charles W. Newton**, President, Newton-Evans Research Company, Inc. – [Bio](#)

---

### **Progress on Antivirus for Control Systems: National SCADA Test Bed Report and Antivirus for Control Systems Vendor Workshop**

This session will present the results of the National SCADA Testbed Antivirus project, summarizing an antivirus test procedure and industry good practices. It will have mini-presentations from a panel of antivirus software vendors, control vendors, and end users. The panel session will continue during a vendor workshop in a breakout session on Wednesday, June 7, allowing for end-user Q & A and possible Interest Group formation.

**Moderator:** **David Teumim**, Independent Consultant, Teumim Technical, LLC – [Bio](#)

**Panelists:** **Richard Clark**, Information Security Analyst, Invensys Wonderware – [Bio](#)

**Mark Heard**, Engineering Associate, Eastman Chemical Company – [Bio](#)

**Jae D. Pudewell**, Senior Product Manager, McAfee, Inc. – [Bio](#)

**Ernie Rakaczky**, Director of Control System Security, Invensys Systems Canada, Inc. – [Bio](#)

**Richard Sutton**, Architect, Advisory Engineer, Symantec



2006 Spring Meeting  
June 6 – 7 • La Jolla, CA  
Sessions and Workshops  
*Industrial Cyber Security Research Consortium: June 5*  
*PCSRF Meeting and I3P Workshop: June 8*  
(As of May 11, 2006. Subject to change.)

## Wednesday, June 7, 2006

**7:00 am – 7:45 am: Continental Breakfast**

**7:00 am – 5:00 pm: Registration and Information Open**

**7:00 am – 5:00 pm: SAFETY Act and You**

David McWhorter of the Office of SAFETY Act Implementation (OSAI) will be available throughout the meeting to talk one-on-one with interested companies about 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.

**9:30 am – 10:00 am: Networking Break**

**12:00 pm – 12:45 pm: Lunch**

**3:00 pm – 3:30 pm: Networking Break**

### PLENARY SESSION

**8:00 am – 9:30 am**

#### **Control System Community Updates**

Latest news and research updates from I3P, National SCADA Test Bed (NSTB), Project LOGI<sup>2</sup>C, PCSRF, Office of SAFETY Act Implementation, National Labs, Government Programs, and others.

**Speakers:** **Richard Jackson**, Chevron Corporation

**Hank Kenchington**., Program Manager, Department of Energy – [Bio](#)

**Keith Stouffer**, Mechanical Engineer, National Institute of Standards and Technology – [Bio](#)

**Ronald Trelue**, Deputy Director, Information Systems Analysis Center, Sandia National Laboratories – [Bio](#)

### **BREAKOUT SESSIONS**

**10:00 am – 11:00 am**

#### **Expectations for Vendors & Researchers Workshop**

This one hour workshop is a follow-up to Tuesday's Vulnerability Disclosure Session for vendors/researchers, asset owners, and coordination centers to define an action plan for developing and enhancing procedures for responding to control system-specific vulnerabilities.

**10:00 am – 11:30 am**

#### **Safe Zone for Critical Information Sharing Interest Group Workshop**

The sanitized results of ten assessments on vendor equipment and onsite installations will be presented with a dashboard type of metric for the severity of the vulnerability and the ease of exploit. Mitigation suggestions will be provided for each vulnerability category. An analysis of findings of the assessments, which were sponsored by the U.S. Department of Homeland Security Control System Security Center

**Expectations for Vendors & Researchers Workshop  
(continued)**

**Moderator: Matt Franz, CISSP**, Senior Security Consultant,  
Control Systems Security Practice, Digital Bond, Inc.  
– [Bio](#)

**Panelists: Ernie Rakaczky**, Director of Control System  
Security, Invensys Systems Canada, Inc. – [Bio](#)

**Eric Byres**, Director of Industrial Cyber Security,  
Wurldtech Analytics Inc. – [Bio](#)

**Ralph Mackiewicz**, Vice President, SISCO, Inc.  
– [Bio](#)

**Safe Zone for Critical Information Sharing Interest Group  
Workshop (continued)**

and the U.S. Department of Energy National SCADA Test Bed,  
resulted in common vulnerabilities that can be discussed without  
attribution back to the specific vendor equipment or location of the  
installation. For additional information on this Interest Group, please  
visit: <https://www.pcsforum.org/groups/64>.

**Chair: Rita Wells**, Critical Infrastructure Assurance,  
Idaho National Laboratory – [Bio](#)

10:00 am – 12:00 pm

**SCADA Cyber Self-Assessment (SCySAG) Working  
Group**

This Working Group is assisting the development and adoption of  
the next generation of self-administered tools and methodologies  
for the assessment of the cyber security readiness of control  
systems. The SCySAG will hold a workshop that will focus on  
advancing the deliverables of the Group:

- Identify and publish a compendium of existing SCADA  
self-assessment efforts/resources available to operators  
to assist them in performing a self-assessment.
- Gather and distill unique characteristics of the control  
system environment versus the generic IT environment,  
identifying the variation of characteristics for the various  
infrastructure sectors. This information will provide a  
framework to 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.

For additional information on this Working Group, please visit:  
<https://www.pcsforum.org/groups/68>.

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

10:00 am – 12:00 pm

**Congress of Chairs (CoC) Working Group Workshop**

This Working Group raises awareness of work in progress on  
standards and related projects that impact the process control  
systems community. Through information sharing and the  
development of tools, the goal is to improve the quality and  
efficiency of all such standards. The CoC will hold a workshop to  
demonstrate the Standards Assessment Database and Combined  
Glossary. The database is an information resource built upon input  
provided by standards (or study group) chairs and structured to  
address asset owner requirements. The Combined Glossary Project  
collects and analyzes glossaries from as many process control-  
related standards groups as possible and combines them. The project  
has demonstrated positive results for contributors and users by  
helping to reduce duplication of effort, simplify standards  
development work, and avoid the emergence of incompatible or  
conflicting terms during the development of various standards.

For additional information on this Working Group, please visit:  
<https://www.pcsforum.org/groups/59>.

**Chair: Bill Rush**  
Institute Physicist, Gas Technology Institute &  
PCSF Vice Chair – [Bio](#)

**11:00 am – 12:00 pm**

**Distribution Guideline for Coordination Centers Workshop**

This one hour workshops is a follow-up to Tuesday's Vulnerability Disclosure Session for vendors/researchers, asset owners, and coordination centers to define an action plan for developing and enhancing procedures for responding to control system-specific vulnerabilities.

**Moderator:** **Matt Franz, CISSP**, Senior Security Consultant, Control Systems Security Practice, Digital Bond, Inc. – [Bio](#)

**Panelists:** **Art Manion**, Internet Security Analyst, CERT Coordination Center – [Bio](#)

**Francisco Ramirez**, Senior Security Consultant, Securicon, LLC – [Bio](#)

**Karl Williams**, Senior Security Adviser, National Infrastructure Security Coordination Centre (NISCC) – [Bio](#)

**1:00 pm – 2:00 pm**

**Progress on Antivirus for Control Systems: National SCADA Test Bed Report and Antivirus for Control Systems Vendor Workshop**

*(This session is a continuation of Tuesday's presentation.)*

This session will feature antivirus vendors McAfee and Symantec, control system vendors, government personnel, representatives from Microsoft, and end users, talking about using antivirus software without disrupting control system operation. This discussion is the culmination of a two-year government research project involving Sandia National Laboratory and National Institute of Standards and Technology.

**Moderator:** **David Teumim**, Independent Consultant, Teumim Technical, LLC – [Bio](#)

**Panelists:** **Richard Clark**, Information Security Analyst, Invensys Wonderware – [Bio](#)

**Mark Heard**, Engineering Associate, Eastman Chemical Company – [Bio](#)

**Jae D. Pudewell**, Senior Product Manager, McAfee, Inc. – [Bio](#)

**Ernie Rakaczky**, Director of Control System Security, Invensys Systems Canada Inc. – [Bio](#)

**Richard Sutton**, Architect, Advisory Engineer, Symantec

**1:00 pm – 3:00 pm**

**US-CERT Control System Security Center Industry Group Interest Group Workshop**

The primary focus of this meeting is to ensure that the Control Systems Security Program (CSSP) products, tools, and outreach efforts are aligned with the needs of industry. This interactive session will present the CSSP strategy, goals, and plan. The CSSP will utilize the input received in this meeting to help guide priorities and promote industry awareness, and to evaluate the Program's effectiveness.

**1:00 pm – 3:00 pm**

**Key Management Infrastructure – The Challenge of Managing Large-scale Cyber Security Presentation**

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 stovepipe 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. It also must take into account the trend to outsource critical operational functions, such as protection device



2006 Spring Meeting  
June 6 – 7 • La Jolla, CA  
Sessions and Workshops  
*Industrial Cyber Security Research Consortium: June 5*  
*PCSRF Meeting and I3P Workshop: June 8*  
(As of May 11, 2006. Subject to change.)

### US-CERT Control System Security Center Industry Group Interest Group Workshop (continued)

For additional information on this Interest Group, please visit:  
<https://www.pcsforum.org/groups/71>.

**Chair:** **Jeffrey Hahn**, Industry Outreach Lead, Idaho National Laboratory – [Bio](#)

settings, to third parties. The hot-button crypto-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!

**Moderator:** **Dennis Holstein**  
Publisher, OPUS Publishing – [Bio](#)

**Panelists:** **Gus K. Lott**, Principal Engineer, YarCom, Inc. – [Bio](#)

**Paul M. Skare**, Product Manager, Siemens Power Transmission & Distribution, Energy Management and Automation Division – [Bio](#)

**Jay Wack**, Chief Evangelist, TecSec – [Bio](#)

**Andrew Wright**, Critical Infrastructure Researcher, Critical Infrastructure Insurance Group (Cisco) – [Bio](#)

1:00 pm – 3:30 pm

### Control Systems Research Interest Group Workshop

This session will be a collaborative discussion designed to: share and document information on current and needed research; identify liaison and outreach opportunities; finalize charter, deliverables, and plan of action; and solicit input to expand and improve the Group's content area on the PCSF Web site  
<https://www.pcsforum.org/groups/65>.

**Chair:** **Ann Miller**, Cynthia Tang Missouri Distinguished Professor of Computer Engineering, University of Missouri-Rolla – [Bio](#)

2:00 pm – 3:00 pm

### Security Testing Panel Workshop

*(This session is a continuation of Tuesday's presentation.)*

The move to open systems for SCADA and control systems has enabled multiple systems and applications to be integrated together into a more complete and efficient control system. This integration also has presented some significant security risks to those systems that are now interconnected. There is a need to develop a security standard that integrated SCADA and control systems are required to meet. Once this standard is developed, a standard security test harness can be utilized to verify that integrated systems are meeting the security standard. This panel will propose a minimum technical security standard for integrated systems and the test tools and methodologies to test against this standard.

2006 Spring Meeting  
June 6 – 7 • La Jolla, CA  
Sessions and Workshops  
*Industrial Cyber Security Research Consortium: June 5  
PCSRF Meeting and I3P Workshop: June 8  
(As of May 11, 2006. Subject to change.)*

**Security Testing Panel Workshop (continued)**

**Speakers:** **Eric Byres**, Director of Industrial Cyber Security, Wurdtech Analytics Inc. – [Bio](#)

**Matt Franz, CISSP**, Senior Security Consultant, Control Systems Security Practice Digital Bond, Inc. – [Bio](#)

**Kevin Staggs, CISSP**, Engineering Fellow, & Control Systems Solution Planner, Honeywell Process Solutions – [Bio](#)

**2:00 pm – 4:30 pm**

**Control System Event Monitoring Working Group Workshop**

This workshop will progress the Security Event Monitoring (SEM) Working Group’s two projects: collecting and correlating control system attack statistics and integrating control system application logs in SEM products. Real world results will be demonstrated, and work to improve and broaden the solution will be debated. For additional information on this Working Group, please visit: <https://www.pcsforum.org/groups/66>.

**Chair:** **Dale Peterson**, Director, Digital Bond, Inc. – [Bio](#)

**3:30 pm – 5:30 pm**

**Control System Technical Security Metrics Interest Group Workshop**

This session will focus on industry needs in development and application of technical security metrics. Additionally, it will gauge interest in developing improved security metrics for estimating the strength of control system components and networks against cyber attacks.

The possible metrics of interest will relate to quantitatively estimating a variety of attributes, including component susceptibility to attacks through both known and unknown vulnerabilities, defensive mechanism effectiveness, and system risk estimation.

For additional information on this Interest Group, please visit: <https://www.pcsforum.org/groups/73>.

**Chair:** **Miles McQueen**, INL Principal Investigator and Computer Science Graduate Faculty, University of Idaho, Idaho Falls – [Bio](#)

**Speakers:** **Eric Byres**, Director of Industrial Cyber Security, Wurdtech Analytics Inc. – [Bio](#)

**Dr. Paul Dorey**, Vice President of Digital Security & Chief Information Security Officer, BP p.l.c. – [Bio](#)

**Clifford Glantz**, Chief Scientist, Pacific Northwest National Laboratory

**Ann Miller**, Cynthia Tang Missouri Distinguished Professor of Computer Engineering, University of Missouri-Rolla – [Bio](#)

**3:30 pm – 5:30 pm**

**Business Case Development Interest Group Workshop**

**Building a Business Case for a Control System Cyber Security Program**

In today’s environment, the implementation of a defined cyber security program is both critical and imperative. Today we see progress as slow and without question very challenging. One of these challenges is the task of building a business case that would support the needed investments. Through this Interest Group, we will work together to identify those elements that are focused on data value, and the three value types to build a solid business case: 1) economic value, 2) operational value, and 3) technical value.

Within these three value elements, we will build a strong message of “Total Benefit of Ownership” rather than the traditional cost of ownership that many—especially key financial decision makers—so commonly hear. During this session, we will work together to develop a methodology that builds on Economic Value Creation. Desired outcomes of this Interest Group session include:

- Defining Key Performance Indicators (KPIs)
- Identify and/or define security enabled communication for strategic improvement
- Defining the value of the currently connected control data
- Identifying what impact loss of that data would have on current revenue stream
- Setting continuation schedule and members

For additional information on this Interest Group, please visit:  
<https://www.pcsforum.org/groups/72>.

**Chair: Ernie Rakaczky**, Director of Control System Security, Invensys Systems Canada Inc. – [Bio](#)

**3:30 pm – 5:30 pm**

**System Analysis and Modeling (SA&M) Interest Group Workshop**

This Interest Group is working to identify and characterize logical domains that form the security boundaries to be protected from cyber attack, and to describe the level of security needed to effectively mitigate the most probable attacks. Session attendees should be familiar with the techniques used to develop organizational, functional, and object models to support system-level requirements analysis. Issues to be reviewed and possibly addressed include the overlapping of organizational responsibilities, role-based access control to restrict access to and use of data down to the level of any named object, cyber-security requirements to establish DMZs where needed, and the system requirements to effectively manage the cyber-security systems throughout the enterprise. During the session, the SA&M Interest Group will define additional issues and determine the scope of analysis needed to address each issue.

For additional information on this Interest Group, please visit:  
<https://www.pcsforum.org/groups/70>.

**Chair: Dennis Holstein**, Publisher, OPUS Publishing – [Bio](#)

**6:00 pm – 7:00 pm**

**PCSF Interim Governing Board Meeting**  
*(by invitation only)*

The PCSF Interim Governing Board will meet at the conclusion of the Workshops.

## Thursday, June 8, 2006

**8:00 am – 1:00 pm**

### **PCSRF Meeting**

The Process Control Security Requirements Forum (PCSRF) will hold a face-to-face meeting on Thursday, June 8, in conjunction with the PCSF Spring Meeting. The main objectives of this meeting will be to review the developed SCADA Field Device Protection Profile and to discuss future direction/objectives. There is no cost to attend the PCSRF meeting. For additional information, please visit <http://www.isd.mel.nist.gov/projects/processcontrol/>.

**Facilitator: Keith Stouffer**, Mechanical Engineer, National Institute of Standards and Technology – [Bio](#)

**8:00 am – 5:00 pm**

### **I3P Workshop**

As part of its major PCS and SCADA security research initiative, the Institute for Information Infrastructure Protection (I3P) will hold its second security workshop on Thursday, June 8, in conjunction with the PCSF Spring Meeting. The workshop will be used to showcase research results generated as part of the project and to demonstrate new tools and technologies that can be used by industry to help secure control systems in the oil and gas sectors and other infrastructures.

I3P Workshop attendance is free when registering in conjunction with the June 5-7 PCSF Spring Meeting. If you will attend only the I3P workshop, the cost is \$100 and you will need to register from the I3P Web site at <http://www.thei3p.org/>. If you will attend both the PCSF meeting and I3P workshop, please register with PCSF as outlined above. Additional information on the I3P workshop is available from <http://www.thei3p.org/>.