



**PROCESS CONTROL  
SYSTEMS FORUM**  
*Collaborating to Advance  
Control System Security*

# **ANNUAL MEETING 2007**

## **MEETING PROGRAM**

*Sheraton Atlanta Hotel  
Atlanta, Georgia*

**March 6–8**

**SOLUTIONS**

*FOR THE CONTROL SYSTEMS COMMUNITY*

Dear PCSF Participants,

Since our formation in early 2005, the PCSF has established a reputation for raising awareness about programs and activities responsible for introducing/improving technologies, driving research, and pursuing unique approaches to solving control system security issues. The PCSF continues to succeed in bringing diverse communities together to identify common issues, plan direction, and produce deliverables leading to improvements in the security posture of industrial control systems.

The Annual Meeting Design Team has taken a different approach towards this year's meeting structure, activities, and objectives. Traditional mainstays such as industry updates, Interest Group discussions, Working Group focused actions, and external organizational gatherings remain an essential part of the program. The new "value add" is SOLUTIONS. The control systems security community has matured since 2005 and continues the positive trend towards improving secure environments across sectors; therefore it is appropriate to narrow the divide between solution seekers and solution providers.

The PCSF Annual Meeting should not be confused with a trade show. The "Solution Day" provides end-users with tactical and strategic solutions to their most pressing control system security concerns. Solutions will be presented through a variety of means, including: presentations; demonstrations; labs; tabletop exercises; training workshops; and case studies with vendors and their customers to provide insight into the circumstances driving solution adoption, planning, implementation, and lessons learned, as well as technical and operational considerations.

The final day of the meeting completes the experience by having participants share feedback and goals while establishing baseline metrics to evaluate success and refine our future objectives.

Regardless of whether you are here as a solution seeker, a solution provider, policy maker, researcher, or are just generally interested in securing our vital control systems, you will be able to immediately apply the information gathered from this meeting to situations you face wherever you call home.

We look forward to your continued participation and welcome you to the PCSF 2007 Annual Meeting.

Sincerely,

The PCSF 2007 Annual Meeting Design Team

MONDAY, MARCH 5					
12:00 pm - 7:00 pm	PCSF Registration and Information: Georgia Pre-Function, Level One				
8:00 am - 5:00 pm	DHS Control Systems Security Program Vendor Forum (Closed-Door Meeting): Georgia 2, Level One				
8:00 am - 5:30 pm	International Electrotechnical Commission (IEC) TC65/WG10 Meeting , Georgia 3, Level One				
5:00 pm - 5:30 pm	PCSF Orientation, Georgia 4, Level One				
TUESDAY, MARCH 6					
7:00 am - 5:00 pm	PCSF Registration and Information: Georgia Pre-Function, Level One				
7:00 am - 8:00 am	Continental Breakfast: Georgia Pre-Function, Level One				
Plenary Session: Georgia 4, 5, & 6, Level One					
8:00 am	Opening Remarks				
8:30 am	Keynote Presentation				
9:00 am	PCSF, Working, and Interest Group Updates				
9:30 am	Networking Break: Georgia Pre-Function, Level One				
10:00 am	Industry Updates				
12:00 pm	Lunch: Garden Courtyard, Level Two				
WORKSHOPS AND DEMONSTRATIONS					
	Georgia 3 & 4	Georgia 5 & 6	Georgia 7 & 8	Georgia 9 & 10	Georgia 11 & 12
1:00 pm	Control System Technical Security Metrics Interest Group	Congress of Chairs Working Group	SCySAG PCS Cyber Security Assessment Requirements Workshop	Education & Training Interest Group	
2:00 pm					
3:00 pm	Networking Break: Georgia Pre-Function, Level One				
3:30 pm	Control Systems Research Interest Group (session concludes at 5:00 pm)			Anti-Virus on Control Systems Interest Group	
4:30 pm					
5:30 pm					
6:00 pm - 8:00 pm	Welcome Reception: Garden Courtyard, Level Two				
WEDNESDAY, MARCH 7					
7:00 am - 5:00 pm	PCSF Registration and Information: Georgia Pre-Function, Level One				
7:00 am - 8:00 am	Continental Breakfast: Georgia Pre-Function, Level One				
WORKSHOPS AND DEMONSTRATIONS					
	Georgia 3 & 4	Georgia 5 & 6	Georgia 7 & 8	Georgia 9 & 10	Georgia 11 & 12
8:00 am		The Mind of the Hacker – Understanding Vulnerabilities, Exploits, and Hacker Methods	Securing Remote Modem and SCADA Scans Across Existing Communication Networks	LOGIIC Correlation Project Solution	
9:30 am	Networking Break: Georgia Pre-Function, Level One				
10:00 am		OPSAID – Interoperable IP-Based PCS Security Architecture (A DOE National SCADA Testbed Project)	Industrial Plants Un-Wired!	SABESP Water Supply Operation Control System – Security Design and Implementation	Real World Security Certifications and Achilles
11:00 am			Smarter Business: Driven by Regulation, Enabled by Standards	Managing Compliance Evidence: Establishing a Trusted Cost Effective Framework for Managing Data and Performing Successful Audits	
12:00 pm	Lunch: Garden Courtyard, Level Two				
1:00 pm	Making the Control System Intrinsically Secure (Defense in Depth for Legacy Systems)	CS2SAT: Control Systems Cyber Security Self Assessment Tool (ends at 3:00pm)	Assessing Security Policies and Procedures - Featuring Process Control IT Incident Management	Cutting Edge Defense Techniques for SCADA, DCS, and other Critical Systems	
2:30 pm	Networking Break: Georgia Pre-Function, Level One				
3:00 pm	Secure Network Architectures for Control Systems	CS2SAT: Control Systems Cyber Security Self Assessment Tool	Creating a Secure Zone for Control Systems Communications	Securing Dial Up Modems into Substations for Engineering Access	
4:10 pm	I3P Security Tools		Implementing and Managing a Secure Wireless Infrastructure	Recommended Practices Program	
5:10 pm	Day Concludes				
THURSDAY, MARCH 8					
7:00 am - 1:00 pm	PCSF Registration and Information: Georgia Pre-Function, Level One				
7:00 am - 8:00 am	Continental Breakfast: Georgia Pre-Function, Level One				
8:00 am	Plenary Session: Georgia 4, 5, & 6, Level One				
8:45 am	Solution Track Breakout Sessions				
	Georgia 4, 5, & 6: Architecture/Design Georgia 7 & 8: Device/Components Georgia 9 & 10: Requirements/Operational Considerations Georgia 11 & 12: Understanding Risk				
10:45 am	Networking Break: Georgia Pre-Function, Level One				
11:00 am	Closing Plenary Session: Georgia 4, 5, & 6, Level One				
12:00 pm	PCSF Annual Meeting Concludes - Lunch Available				
2:00 pm - 6:00 pm	International Electrotechnical Commission (IEC) TC65/WG10 Meeting , Georgia 9 & 10, Level One				
2:00 pm - 6:00 pm	Solutions for Process Control Security Training Course, Georgia 13				
FRIDAY, MARCH 9					
8:00 am - 3:00 pm	International Electrotechnical Commission (IEC) TC65/WG10 Meeting , Georgia 9, Level One				
8:00 am - 5:00 pm	Intermediate Control Systems Security Training Course, Georgia 13				

## DAILY EVENTS

### Registration and Information

**Location:** Georgia Pre-Function, Level One

**Monday, March 5 ~ 12:00 pm – 7:00 pm**

**Tuesday, March 6 ~ 7:00 am – 5:00 pm**

**Wednesday, March 7 ~ 7:00 am – 5:00 pm**

**Thursday, March 8 ~ 7:00 am – 1:00 pm**

### Control Systems Security Program Booth

**Location:** Georgia Pre-Function, Level One

**Tuesday, March 6 ~ 7:00 am – 5:00 pm**

**Wednesday, March 7 ~ 7:00 am – 5:00 pm**

**Thursday, March 8 ~ 7:00 am – 1:00 pm**

To reduce control system risks within and across all critical infrastructure sectors, the Department of Homeland Security's National Cyber Security Division (NCSA) established the Control Systems Security Program (CSSP) to coordinate efforts among federal, state, local, and tribal governments, as well as control systems owners, operators, and vendors. The CSSP coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities. CSSP staff will be on hand to provide additional information on the program and answer any questions throughout the PCSF Annual Meeting.

### National SCADA Test Bed Booth

**Location:** Georgia Pre-Function, Level One

**Tuesday, March 6 ~ 7:00 am – 5:00 pm**

**Wednesday, March 7 ~ 7:00 am – 5:00 pm**

**Thursday, March 8 ~ 7:00 am – 1:00 pm**

The National SCADA Test Bed (NSTB) booth highlights activities that address industry-defined priorities for enhancing control system security in the energy sector. This multi-laboratory partnership under the U.S. Department of Energy works with industry partners to identify and correct critical security flaws in control systems and equipment through system assessments, training, standards, and technology advancement. Stop by to learn more and make sure your organization's activities are reflected in the new, online, interactive Roadmap to Secure Control Systems in the Energy Sector.

### Technology Demonstrations and Q&A with the I3P Research Team Booth

**Location:** Georgia Pre-Function, Level One

**Tuesday, March 6 ~ 7:00 am – 5:00 pm**

**Wednesday, March 7 ~ 7:00 am – 5:00 pm**

**Thursday, March 8 ~ 7:00 am – 1:00 pm**

For the past two years, researchers funded by The Institute for Information Infrastructure Protection (I3P) have been collaborating to develop new findings and technical solutions addressing the control system security challenges facing the oil and gas sector and other critical applications of control systems. The results of this effort will be showcased in the I3P demo booth, where members of the research team will be available to demonstrate technologies, answer your questions, and provide you with additional material. In particular, the team will demonstrate solutions for platform security (SHARP) and control system network monitoring (EMERALD) presented in the solution track, using a portable test bed.

# MONDAY, MARCH 5

## Department of Homeland Security – Control Systems Security Program Vendor Forum

**Room:** Georgia 2, Level One

**Time:** 8:00 am – 5:00 pm

The CSSP Vendor Program is a closed-door meeting. For more information, please contact Jeff Hahn at Jeffrey.Hahn@inl.gov or 208.526.6178.

## International Electrotechnical Commission (IEC) TC65/WG10 Meeting

**Room:** Georgia 3, Level One

**Time:** 8:30 am – 5:30 pm

The International Electrotechnical Commission (IEC) TC65/WG10 is writing a three-part international standard on system and network security for industrial process measurement and control systems:

- IEC 62443-1, Framework and Threat-Risk Analysis
- IEC 62443-2, Security Assurance: Principles, Policy, and Practice
- IEC/TS 62443-3, Sets of Security Requirements for Security Elements in Typical Scenarios

The IEC standards Working Group meetings are open to all observers, who will be permitted to participate in discussions.

## PCSF Orientation

**Room:** Georgia 4, Level One

**Time:** 5:00 pm – 5:30 pm

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

Those new to the PCSF are encouraged to attend this useful introductory session to gain an understanding of the unique value, goals, and objectives the Forum brings to the control systems community, as well as the tools and information resources available to participants.

## TUESDAY, MARCH 6

**Continental Breakfast**  
Georgia Pre-Function, Level One  
7:00 am – 8:00 am

## PLENARY SESSION

Georgia 4, 5, & 6, Level One

### 8:00 am – 8:30 am: Opening Remarks

**Speakers:** **Michael Torppey**, PCSF Technical Manager & Senior Principal, Noblis  
**Perry A. Pederson**, Director, Control Systems Security Program, National Cyber Security Division, U.S. Department of Homeland Security

### 8:30 am – 9:00 am: Keynote Presentation

**Speaker:** **Mr. Bruce Landis**, U.S. Department of Homeland Security Deputy Assistant Secretary for Cyber Security and Telecommunications

### 9:00 am – 9:30 am: PCSF Update and Working & 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 Tuesday afternoon.

**Networking Break**  
Location: Georgia Pre-Function, Level One  
9:30 am – 10:00 am

### 10:00 am – 12:00 pm: Control System Community Updates

- **Analysis and Coordination of Software Vulnerabilities Update** – The CERT Coordination Center will present an overview of the vulnerability coordination process, describe how the process may be applied to control systems vulnerabilities, and identify gaps in the process with respect to control systems. Questions, discussion, and feedback are welcome, particularly from stakeholders such as vendors, owner/operators, and researchers. The mission of the CERT Coordination Center Vulnerability Analysis Team is to reduce the number of, and threat posed by, software vulnerabilities. To this end, CERT/CC collects and analyzes vulnerability reports and coordinates vulnerability information with vendors, researchers, trusted collaborators, those responsible for critical infrastructure protection, and the general public.  
**Presenter:** **Art Manion**, Vulnerability Analysis Team Lead, CERT Coordination Center
- **Control Systems Security Certification Organization** – The presenters will review the status of a proposed organization to oversee creation of well-engineered specifications and processes for the security testing and certification of critical control systems and products.  
**Presenters:** **Eric Byres**, CEO, Byres Security Inc. and **T.S. Lee**, Director, Publishing Services, ISA
- **Cyber Security Procurement Language for Control Systems Guide:** The momentum and industry desire for the Procurement Language guide was recognized during the SANS SCADA/Control System Security Summit in Orlando, FL (March 2006). The most important driver for this project is the recognition by asset owners, vendors, industry organizations, and government stakeholders of the importance of security risks. The Department of Homeland Security is taking advantage of this reality and is focused on developing and supporting risk reduction tools and related projects. The agency has joined with owners, vendors, and other government stakeholders to develop this "tool kit" or guide to give asset owners an understanding of what they can and should ask for from their vendors to ensure that cyber security is designed and built into the systems they purchase.  
**Presenter:** **Gary J. Finco**, SCADA Security Researcher, Idaho National Laboratory

## 10:00 am – 12:00 pm: Control System Community Updates (continued)

- Industrial Control System Security: Applying NIST 800-53, Revision 1 to Industrial Control Systems (ICSs)** - Industrial and process control systems (hereafter referred to as ICSs) are an integral part of the critical infrastructure and the protection of those systems is a priority for the federal government. From air traffic control systems to the systems managing the nation's largest electric power grids, ICSs are playing an increasingly important role in the economic and national security interests of the United States. Until recently, ICSs had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems are integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems while still maintaining their unique operational attributes. While the change in industrial control system architecture supports new information system capabilities, it introduces many of the same vulnerabilities that exist in current networked information systems. There are a number of standards and industry activities now focused on securing ICSs with little coordination occurring. Additionally, there are certain federal security requirements (e.g., NIST SP 800-53, Revision 1) that apply to all federal agency computing systems including control systems. Since some of the security controls contained in SP 800-53, Revision 1 were not directly applicable to ICSs, NIST initiated an effort to develop an interpretation of NIST SP 800-53, Revision 1 specifically for ICSs (800-53 ICS). The development included a comparison of SP 800-53, Revision 1 security requirements with those found in other industry standards-- in particular the NERC CIP cyber security standards. This session addresses the status of 800-53 ICS, NIST's plans to introduce it into the federal ICS community, and NIST's plans to work with the ICS standards community to foster convergence on a common set of ICS cyber security standards for all ICS communities (e.g., electric, water, gas, manufacturing).

**Presenters:** **Stuart W. Katzke, Ph.D.**, Senior Research Scientist, National Institute of Standards and Technology  
**Joe Weiss**, Managing Partner, Applied Control Solutions, LLC

- Securing Control Systems in the Energy Sector** – This presentation will update attendees on a unique public-private partnership to secure control systems in the energy sector. The partnership is guided by the Roadmap to Secure Control Systems in the Energy Sector, which serves as a tool for aligning and integrating resources in industry, academia, and government. The U.S. Department of Energy will discuss recent achievements and exciting new developments, including the recent NIAC recommendations, new partnering opportunities, and a new on-line tool for tracking current projects that address Roadmap needs.

**Presenter:** **Henry (Hank) S. Kenchington**, Program Manager, Department of Energy

- Status and Accomplishments of the I3P's Process Control Systems Security Research Project** – The Institute for Information Infrastructure Protection (I3P) established its Process Control Systems Security Research Project in the spring of 2005. This ambitious project brought together ten I3P member institutions from across the country to collaborate on the development and demonstration of novel solutions for the control system security challenges facing the oil and gas and other infrastructure sectors. This presentation will highlight new insights, methodologies, and tools developed by the I3P team to improve the characterization, assessment, and mitigation of control system security risks. The I3P's plans for future work in control system security research also will be outlined.

**Presenter:** **John Cummings, Ph.D.**, Director, I3P PCS Security Research Project, Sandia National Laboratories

### Lunch

Garden Courtyard, Level Two  
 12:00 pm - 1:00 pm

## Control System Technical Security Metrics Interest Group

**Room:** Georgia 3 & 4, Level One

**Time:** 1:00 pm – 3:00 pm

**Presenters:** **Wayne Boyer**, Advisory Engineer/Scientist, Idaho National Laboratory

**Eric Byres**, CEO, Byres Security Inc.

**Cliff Glantz**, Senior Staff Scientist, Pacific Northwest National Laboratory

**Miles McQueen**, Principal Investigator, Idaho National Laboratory, & Chair, Control System Technical Security Metrics InterestGroup

This session is a continuation of the Control System Technical Security Metrics Interest Group that began at the PCSF 2006 Spring Meeting. The Interest Group focuses on applied research and application of technical security metrics. Industry and owner/operators are responding to demands for security improvements, but there is a need to provide quantitative measures of the effectiveness of security-related activities.

We will review the current state of cyber security technical metrics, present a set of recommended technical security metrics for use by owners/operators of control systems and solicit input from participants in support of the Group's goal to advance the state of the art and the state of the practice in security metrics for control systems.

### Control System Technical Security Metrics Interest Group (continued)

**Session topics include:**

- Recent work by the I3P project related to security metrics will be presented including: framework for metrics development and use, currently available metric tools and how security metrics can be used to make cost-effective cyber security decisions.
- The Application of Security Metrics in Process Control System Environments will be presented from the perspective of the National SCADA Test Bed Project. A metrics taxonomy with an Automated Systems Reference Model will also be presented and discussed.
- The Control System Security Program (CSSP) has recently investigated the cyber security technical metrics that have previously been defined by various standards and by industry. The results of this study indicate that the currently defined metrics have serious weaknesses. An ideal set of metrics would be comprehensive, few in number, easy to understand and measure, and strongly related to the real level of control systems security. The CSSP has proposed seven high-level concepts/ideals from which metrics can be defined. For each of the seven ideals, one or more metrics are proposed.

### Congress of Chairs Working Group Workshop

**Room:** Georgia 5 & 6, Level One

**Time:** 1:00 pm – 3:00 pm

**Presenter:** William Rush, Rush Cyber Security

During this workshop, the CoC will demonstrate the latest version of the “Standards Assessment Database” which contains information pertaining to Control Systems Standards, Guidelines and Reports. This database will be utilized by the CIGRE Study Committee B5, who are examining the impact of implementing security requirements in IEC 61850. The CoC will also review the updated Common Glossary and will hold discussions pertaining to effective collaboration and awareness among standards organizations. This will include an update on AGA-12 and IEEE working together on adopting technical components of the respective organizations work, as well as updates on many of the standards under development.

### SCySAG PCS Cyber Security Assessment Requirements Workshop

**Room:** Georgia 7 & 8, Level One

**Time:** 1:00 pm – 3:00 pm

**Presenter:** Brian Isle, Chief of Operations, Adventium Labs, & Chair, SCADA Cyber Self-Assessment Working Group

The SCySAG Working Group will hold a workshop to further efforts to identify cyber security assessment requirements for process control systems. This workshop will provide a review of the work to date, including the cyber assessment tools reviewed and analysis of requirements coverage. The workshop will gather feedback on the work completed and prioritize the future SCySAG efforts.

### Education & Training Interest Group

**Room:** Georgia 9 & 10, Level One

**Time:** 2:00 pm – 3:00 pm

**Presenter:** Brian Lopez, Leader, Vulnerability & Risk Assessment Program, Lawrence Livermore National Laboratory and Chair, Education and Training Interest Group

**This year’s PCSF Education & Training Interest Group session will:**

1. Provide an overview of the brand new “Critical Infrastructure and Control Systems Security Curriculum” developed by a multi-disciplinary group under DHS sponsorship. This curriculum includes six modules focused on: Vulnerability, Engineering Approaches, Managing Organizations and Risk, Securing Networks of Enterprises, Creating Markets, and Building Trust – Public/Private Policy.  
Each module provides objectives, key questions, and supporting readings. An annotated bibliography also is provided to guide further investigation. The entire curriculum, including all supporting materials, will be made available to all attendees.
2. Discuss ways to leverage the curriculum for a variety of objectives (e.g. corporate training as background to get up-to-speed on issues, academic teaching, etc).
3. Brainstorm future efforts and the most important needs in the education and training arena, ranking potential efforts for the coming year and determining pathways to achieve them.

**Networking Break**

**Location:** Georgia Pre-Function, Level One  
**3:00 pm - 3:30 pm**

## Control Systems Research Interest Group

**Room:** Georgia 3 & 4, Level One

**Time:** 3:30 pm – 5:00 pm

**Presenter:** Dr. Ann Miller, Professor, University of Missouri-Rolla, & Chair, Control Systems Research Interest Group

This discussion and collaboration session to share information about current and needed research is open to all who are interested in control systems research. Following introductions, there will be a brief update on progress to date, short presentations, and then discussion of a workshop proposal. Our goal is to migrate to a Working Group whose Web site is the “one-stop shop” for information about control systems research, with links to relevant government, industry, and academic Web sites.

## Anti-Virus on Control Systems Interest Group Meeting

**Room:** Georgia 9 & 10, Level One

**Time:** 3:30 pm – 5:30 pm

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

The purpose of this session will be to look at the requirements for anti-virus software on control systems. The session will drive to evaluate the holistic needs of anti-virus and anti-intrusion capabilities for control systems. Not only will technology be addressed, but also policies and procedures with regard to usage of control systems. Discussion will include architectures that mitigate the risk of virus, worm, and malware infection of control systems. One of the objectives of this session will be to define a proactive approach to malware prevention. This session will include discussions from end-users and vendors of control systems to understand the approach and costs of integrating anti-virus software into control systems.

**Some of the IT topics to be discussed include:**

- How does IT work with A/V vendors?
- How does IT qualify A/V for their enterprise?
- Is there a different A/V approach for servers vs. desktops?
- What is the approximate IT cost for A/V qualification?
- How closely does IT track A/V major updates?
- Is anti-spyware installed on tightly controlled servers?

**Vendors should be prepared to address topics such as:**

- Special A/V requirements from the vendor perspective
- Approximate A/V software qualification costs
- A/V tradeoffs and resulting risk

### Welcome Reception

Garden Courtyard, Level Two

6:00 pm - 8:00 pm

Enjoy an evening reception by the pool, including an assortment of delicious food, excellent conversation, and a two-hour hosted soft drink, beer, and wine bar.

*Tuesday*  
*March 6*

## WEDNESDAY, MARCH 7

**Continental Breakfast**  
Georgia Pre-Function, Level One  
7:00 am – 8:00 am

## WORKSHOPS & DEMONSTRATIONS

### The Mind of the Hacker – Understanding Vulnerabilities, Exploits, and Hacker Methods

**Room:** Georgia 5 & 6, Level One  
**Time:** 8:00 am – 9:30 am

**Presenter:** Clint Bodungen, President, Critical Infrastructure Institute (USA)

**Solution Track:** Understanding Risk

What makes industrial systems vulnerable to attack? How do hackers take advantage of these vulnerabilities? What, exactly, is a buffer overflow? What's the difference between a threat, a vulnerability, an exploit, and risk? These questions, and many questions like these, must be understood and properly answered in order to safeguard your systems effectively. This tutorial will explore the mind of the hacker, his motivations, and his methods. It takes a technical look at vulnerabilities and proper safeguards.

### Securing Remote Modem and SCADA Scans Across Existing Communication Networks

**Room:** Georgia 7 & 8, Level One  
**Time:** 8:00 am – 9:30 am

**Presenters:** Andrew Bartels, Senior Vice President & CTO, Aegis Technologies, Inc.  
Robert Sill, CEO & President, Aegis Technologies, Inc.  
William Winters, EMS Manager, Arizona Public Service

**Solution Track:** Devices/Components

Many utilities have contemplated a number of projects and investments to improve the reliability and performance of their control systems communications networks as well as secure their networks from hackers and cyber attack. Implementing multiple solutions from multiple vendors would be counterproductive to one of the utilities' main objectives – improving network performance. The Odyssey™ Solution is the only solution that provides several operational benefits in addition to SCADA system security and, at the same time, can be scaled to minimize the cost of future expansions. Odyssey™ can retrofit to the existing SCADA network to provide enhanced performance benefits, improved diagnostics tools to Control Center operators, and provide a security package that will secure the entire electronic perimeter of the control system network. A pilot program with a major investor-owned utility is currently in progress.

A protocol-independent solution designed for legacy and newer control systems, the Odyssey™ Solution is comprised of three unique feature sets:

- OptiBit™ Performance Suite
- PinPointer™ Diagnostics Suite
- SCADAsafe™ Security Suite

### LOGIIC Correlation Project Solution

**Room:** Georgia 9 & 10, Level One  
**Time:** 8:00 am – 9:30 am

**Presenters:** Leeanna Demers, Senior Sales Engineer, ArchSight, Inc.  
Raymond Parks, Sandia National Laboratory

**Solution Track:** Architecture/Design

This session will be comprised of three parts including: an explanation of LOGIIC, the project structure, and the results of the work; a discussion of the threat basis of the project and of the technical details; and a vendor will explain how their product integrates into the overall solution.

**Networking Break**  
**Georgia Pre-Function, Level One**  
**9:30 am – 10:00 am**

### Industrial Plants Un-Wired!

**Room:** Georgia 7 & 8, Level One

**Time:** 10:00 am – 11:00 am

**Presenter:** William Miller, President, Maximum Control Technologies (MaCT)

**Solution Track: Devices/Components**

This session will introduce attendees to maximizing routing performance and design factors for optimal route selection, including discussion of the following topics:

- Layer 2 (L2) Multi-Layer Switching
- New Metric (Time vs. Hop)
- New Proactive Routing Protocol
- Advanced Encryption
- Sophisticated Key Management

### SABESP Water Supply Operation Control System – Security Design and Implementation

**Room:** Georgia 9 & 10, Level One

**Time:** 10:00 am – 11:00 am

**Presenter:** Raphael Gomes Pereira, Security Officer, Chemtech

**Solution Track: Requirements/Operational Considerations**

This session will demonstrate all the security concerns during the project design and implementation in some security domains, like network and system security, physical security, access control, and penetration tests.

The original concept was based on two premises: (1) segregation of duties and (2) network/environment segregation. The challenge consisted of integrating Automation network to Corporate Office network, providing real-time information to users of both networks.

This project has a three-tier automation system solution with a SCADA System (automation), PIMS (process data), and a water supply management system, along with operational intelligence and data visualization (management). All these systems are protected with controls implemented by layers.

The first layer is the physical security controls, which use biometrics to control access to the Control Room and a CFTV system to monitor physical access.

The second layer is the network layer. All components in this layer are clustered / redundant. The solution also uses Firewalls, Switches layer 2 and 3. All these components are monitored by a management system and use a single-user database for authentication, authorization, and accounting. Other controls implemented in this layer include VLANs, Port Security, 802.1x, Trunking, VPN, and others.

The third layer is the system security. The SCADA System is deployed in a cluster environment, reducing its downtime. The other systems also are implemented using security best practices. All applications authenticate their users by using a unique database. Other controls in this layer include Antivirus, Host IDS, Time Servers, and others.

### OPSAID – Interoperable IP-Based PCS Security Architecture (A DOE National SCADA Test Bed Project)

**Room:** Georgia 5 & 6, Level One

**Time:** 10:00 am – 12:00 pm

**Presenters:** Ori Artman, CTO, Teltone Corporation

David L. Norton, CISSP, Program Manager – Transmission IT Security, Entergy – New Orleans and Member, PCSF Board of Governors

Rhett Smith, Applications Engineer, Schweitzer Engineering Laboratories

Jason Stamp, Ph.D., OPSAID Program Lead, Sandia National Laboratories

David J. Teumim, CISSP, Teumim Technical, LLC

**Solution Track: Architecture/Design**

### **OPSAID – Interoperable IP-Based PCS Security Architecture (A DOE National SCADA Test Bed Project) (continued)**

OPSAID is an open process control system security architecture for IP-based PCS networks based on open source security software to promote interoperability. The project is being led by Sandia National Laboratories under the Department of Energy's National SCADA Test Bed (NSTB) program, and includes end-users and industrial networking vendors.

The session will describe the project and industry partnership opportunities, cover the deliverables to industry such as the OPSAID reference design and field test data, and feature an end-user's view of the need to accelerate interoperable IP security solutions for automation technology. The session also will demonstrate constituent technology, like firewall, VPN, IDS, and access control capabilities. Finally, two vendors will describe their experience with the project, concluding with an audience Q&A session for the overall panel.

### **Real World Security Certifications and Achilles**

**Room:** Georgia 11 & 12, Level One  
**Time:** 10:00 am – 12:00 pm

**Presenters:** **Nate Kube**, CTO, Wurdtech Security Technologies  
**Dale Peterson**, Director, Digital Bond, Inc.

#### **Solution Track: Understanding Risk**

The Achilles Vulnerability Assessment Platform is the first automated, comprehensive testing product for systematically assessing network stack robustness and locating zero-day vulnerabilities in industrial control devices. Many of the large Vendors are currently using Achilles testing as the means to demonstrate, to their security-conscious customers, the network robustness of their flagship controllers.

The first portion of this session will introduce attendees to the commercial offering of Achilles and have them execute, step-by-step, their own Achilles tests against representative controllers. Attendees of this session will learn how real world vulnerabilities are found, what they actually look like, and how easily they may be packaged into maladies such as viruses.

The second portion of this session will introduce the Achilles certification program, describe the test cases and test criteria for the initial certification, and reveal a sample of the certification results that will be publicly available to the control systems community.

### **Smarter Business: Driven by Regulation, Enabled by Standards**

**Room:** Georgia 7 & 8, Level One  
**Time:** 11:00 am – 12:00 pm

**Presenter:** **Darren Reece Highfill**, CISSP, Software Engineer, EnerNex Corporation

#### **Solution Track: Requirements/Operational Considerations, Architecture/Design, Device/Components**

It wasn't very long ago that devices were dumb and connections were costly. Obscure, proprietary protocols and truly isolated systems fostered complex and inflexible solutions. We built a world that brought us robust functionality through meager resources, but left us strategically vulnerable when it came to doing business.

The landscape has changed, and those days are gone. Today's offering of Intelligent Electronic Devices (IED) includes many capable of serving large amounts of high resolution data from multiple functional domains. Use of standard protocols and IP communications makes available a wide array of inexpensive and easily deployed transport mechanisms, and issues of compliance and corporate responsibility bring overall system security into the spotlight. The objective of this presentation is to delineate the manners in which EnerNex Corporation is supporting the Tennessee Valley Authority (TVA) in making remote field data securely available to the enterprise in this new information era.

This presentation will use three significant projects to illustrate TVA's efforts to secure IED-to-enterprise, or "end-to-end" data, communications:

- The PowerWAN Security Policy addresses TVA's new, wide-area IP-based network for real-time remote device and data access.
- The Remote Device Access Solution integrates corporate identity and access management for engineers and applications communicating with devices and data in the field.
- The Bradley County 500kV Substation is a fully automated, next generation environment implementing IEC 61850 capable devices supplied by multiple vendors.

Together, these projects represent a major piece of the future for managing TVA's remote resources through a robust, scalable, secure, and maintainable solution while enabling TVA to meet the incoming NERC Critical Infrastructure Protection (CIP) Security Standards.

## Managing Compliance Evidence: Establishing a Trusted, Cost Effective Framework for Managing Data and Performing Successful Audits

**Room:** Georgia 9 & 10, Level One  
**Time:** 11:00 am – 12:00 pm

**Presenter:** Jeff Kalibjian, Senior Security Architect, Hewlett Packard Corporation

**Solution Track:** Requirements/Operational Considerations

Compliance initiatives are generally dual faceted, presenting an organization challenges in deploying process and procedures to meet compliance directives, as well as specifying requirements for demonstrating compliance adherence (e.g., NERC CIP). This session will demonstrate how trust and accountability can be utilized in automated systems that cannot only collect and manage compliance evidence but also provide a framework for external auditors to evaluate organizational compliance progress.

**Lunch**  
 Garden Courtyard, Level Two  
 12:00 pm – 1:00 pm

## Making the Control System Inherently Secure (Defense in Depth for Legacy Systems)

**Room:** Georgia 3 & 4, Level One  
**Time:** 1:00 pm – 2:30 pm

**Presenter:** Eric Byres, CEO, Byres Security Inc.

**Solution Track:** Architecture/Design

Despite industry's best efforts to isolate our control systems from the outside world, the statistics show that the bad guys (and bugs) are still getting in. Traditional firewalls are too complex for most security professionals to configure correctly and are even harder to set up properly on the plant floor. And once a virus or hacker gets past the control system firewall, the typical HMI, PLC, or DCS is an easy target for attack.

The bottom line is that companies cannot rely solely on a "Great Wall of China" firewall architecture: They need a defense-in-depth solution for both new and legacy control systems. In addition, they need an open security platform that is designed from the ground up with the environment, staff capabilities, and needs of industry in mind.

This session demonstrates a possible solution for a control security platform that uses a number of unique features developed at the BCIT Research Labs, including:

- Zero configuration field deployment that makes it simple for electricians and instrumentation mechanics to install the system without any training.
- Central management based on standard control systems concepts (such as PLC programming and Fieldbus configuration tools), allowing an industrial controls practitioner, rather than the security specialist, to commission and manage security for the plant floor.
- "Device-Focused Rule Creation" so that the firewall rule sets are automatically created with the needs of the device to be protected in mind, not with the design of the firewall in mind.

Finally, the presentation will close with an interactive session designed to discover how companies might deploy this type of open platform in real-life situations and what types of security modules (e.g., AGA-12 Encryption, ProfiNet Filtering, etc.) end users really need and would encourage the control systems vendors and security industry to create.

## CS<sup>2</sup>SAT: Control Systems Cyber Security Self Assessment Tool

**Room:** Georgia 5 & 6, Level One  
**Time:** 1:00 pm – 3:00 pm

**Presenter:** Jeffrey Tebbe, R&D Scientist/Engineer, Idaho National Laboratory

**Solution Track:** Understanding Risk

Development of the CS<sup>2</sup>SAT was funded by the Department of Homeland Security to provide owner/operators with a tool to assess the strength of control system cyber security implementation. The tool is a desktop application that walks users through a series of questions that assess security posture and provide recommendation for areas identified as potential weaknesses. Benefits of the tool include its repeatability to allow for baselining posture and measuring improvement over time. Because the tool is based on recognized standards, gaps also can be identified through standards-specific reporting to help identify potential problems with standards compliance.

**Please note that each participant must bring a laptop computer running Windows 2000 or XP and must have administrator rights to the computer to install Java 1.5 release 6 or higher, if not already installed before this training session begins.**

### **Assessing Security Policies and Procedures - Featuring Process Control IT Incident Management**

**Room:** Georgia 7 & 8, Level One

**Time:** 1:00 pm – 2:30 pm

**Presenters:** Chris Sandford, Principle Consultant, International Network Services (INS)

**Solution Track:** Understanding Risk

It is difficult to assess non-technical aspects of security. This session will show that assessing the security policies and procedures will demonstrate compliance or non-compliance to a security program. Using a tool and completing regular audits will indicate the particular strengths and weaknesses within a business unit, manufacturing plant, and the company. If a company is aware of its security weaknesses, it will be able to react and remediate the identified issues.

This session also will highlight the incident management plan and how the plan can be integrated.

### **Cutting Edge Defense Techniques for SCADA, DCS, and other Critical Systems**

**Room:** Georgia 9 & 10, Level One

**Time:** 1:00 pm – 2:30 pm

**Presenters:** Clint Bodungen, President, Critical Infrastructure Institute (USA)  
Jonathan Pollet, Vice President, PlantData Technologies, A division of Verano

**Solution Track:** Architecture/Design, Device/Components

As SCADA, Control Systems, and other critical systems converge with IP networks, they are plagued by new threats. However, it is possible that the mitigation could turn out to be more disastrous than the risk itself, due to unforeseen system impacts. Sometimes, systems, applications, or code may be so proprietary or vendor-dependent that it is not possible to apply the necessary patches or safeguards. So, how does one remain secure and compliant? How does one remain secure without hindering others' ability to function efficiently? This presentation examines creative, safe, cutting edge defense techniques that cost nearly nothing. This is a must-see presentation for any security professional or engineer facing the complexities of security, regulation, compliance, and interoperability.

**Networking Break**  
Georgia Pre-Function, Level One  
2:30 pm - 3:00 pm

### **Secure Network Architectures for Control Systems**

**Room:** Georgia 3 & 4, Level One

**Time:** 3:00 pm – 4:00 pm

**Presenter:** Andrew Wright, Technical Leader, Cisco Systems, Inc.

**Solution Track:** Architecture/Design

Cisco Systems is developing a set of architectures and design guides for building secure control systems based on Ethernet technologies. The architectures exploit the Cisco Self-Defending Network technologies to deliver a secure control system network that provides not only strong perimeter defense, but also security throughout the network core that can adapt and defend against new threats and attacks as they arise. The design guides will provide specific guidance on firewall configuration, VLAN organization and management, L2 and L3 security, access control, wireless configuration, and redundancy, as well as recommendations for specific Cisco products to achieve particular levels of performance.

## Creating a Secure Zone for Control Systems Communications

**Room:** Georgia 7 & 8, Level One  
**Time:** 3:00 pm – 4:00 pm

**Presenter:** Clayton L. Coleman, Solutions Architect, Invensys Process Systems

**Solution Track:** Architecture/Design

In this session, Invensys will describe techniques for creating a secure control system data acquisition architecture, describe an example customer environment, and the steps taken to solve their needs. The customer's need is to share process data, provide remote access, and at the same time prevent the flow of virus, worm, or malicious hacking traffic from entering their control system. The Invensys team will walk through the processes of assessing the customer environment, creating a security policy, and implementing the right technologies to enforce that policy, in a step-by-step manner. Session attendees will obtain an understanding of Invensys' approach.

## Securing Dial Up Modems into Substations for Engineering Access

**Room:** Georgia 9 & 10, Level One  
**Time:** 3:00 pm – 4:00 pm

**Presenter:** Dwight Anderson, Marketing Engineer, Schweitzer Engineering Laboratories

**Solution Track:** Devices/Components

This session will present a real example of securing remote access of the critical infrastructure. Southern Company is using encryption and session authentication to secure dial-up engineering access of remote and geographically dispersed monitoring and control systems of bulk power protection equipment located in electric power substations. This same type of equipment could be used to secure remote access of water, chemical, gas, or other infrastructures dependent on the need for remote access via telephone or even spread spectrum radios.

## CS<sup>2</sup>SAT: Control Systems Cyber Security Self Assessment Tool

**Room:** Georgia 5 & 6, Level One  
**Time:** 3:00 pm – 5:00 pm

**Presenter:** Jeffrey Tebbe, R&D Scientist/Engineer, Idaho National Laboratory

**Solution Track:** Understanding Risk

Development of the CS<sup>2</sup>SAT was funded by the Department of Homeland Security to provide owner/operators with a tool to assess the strength of control system cyber security implementation. The tool is a desktop application that walks users through a series of questions that assess security posture and provide recommendation for areas identified as potential weaknesses. Benefits of the tool include its repeatability to allow for baselining posture and measuring improvement over time. Because the tool is based on recognized standards, gaps also can be identified through standards-specific reporting to help identify potential problems with standards compliance.

**Please note that each participant must bring a laptop computer running Windows 2000 or XP and must have administrator rights to the computer to install Java 1.5 release 6 or higher, if not already installed before this training session begins.**

## I3P Security Tools

**Room:** Georgia 3 & 4, Level One  
**Time:** 4:10 pm – 5:10 pm

**Presenters:** Cliff Glantz, Senior Staff Scientist, Pacific Northwest National Laboratory  
 R. Eric Robinson, Senior Scientist, Pacific Northwest National Laboratory  
 Alfonso Valdes, Senior Computer Scientist, SRI International

**Solution Track:** Requirements/Operational Considerations, Architecture/Design, Devices/Components

**Advanced Security Technologies:** This session will describe the I3P team's research in new solutions for platform security and control system network monitoring. For platform security, the Security-Hardened Attack Resistant Platform (SHARP) provides a vendor an infrastructure-independent, high security environment for process control network systems. The SHARP is designed to be a drop-in component that securely monitors and controls access to legacy process control investments. For network monitoring, the EMERALD network intrusion detection and correlation framework consists of multiple sensors and a correlation framework in an appliance form factor. This system has been extended and adapted for process control networks, including the incorporation of an adapted Modbus rule set to detect attacks against PCs and the commodity hardware and software platforms on which modern control systems are built.

### **Implementing and Managing a Secure Wireless Infrastructure**

**Room:** Georgia 7 & 8, Level One

**Time:** 4:10 pm – 5:10 pm

**Presenter:** Greg Burns, Solution Architect, Enterprise Networks and Security Practice, Invensys Process Systems

**Solution Track:** Architecture/Design

Attendees will learn how to manage multiple wireless technologies safely, securely, and easily within an industrial facility. The session will discuss the benefits of the Invensys (control system independent) wireless technology and how companies are securely managing solutions such as the mobile operator, condition monitoring, asset performance optimization, flexible communications, video for safety and process management, incremental process measurements, and many others at their facilities. A case study of LCRA will be presented.

### **Recommended Practices Program**

**Room:** Georgia 9 & 10, Level One

**Time:** 4:10 pm – 5:10 pm

**Presenters:** David Kuipers, CSSP, Principle Engineer/Scientist, Idaho National Laboratory

Trent Nelson, CSSP, Principle Engineer/Scientist, Idaho National Laboratory

**Solution Track:** Architecture/Design

This program provides a current information resource to help industry understand and prepare for ongoing and emerging control systems cyber security issues, vulnerabilities, and mitigation strategies.

The CSSP works with the control systems community to ensure that recommended practices that are made available have been vetted by subject-matter experts in industry before being made available publicly in support of this program.

Recommended practices are developed to help users reduce their exposure and susceptibility to cyber attacks. These recommendations are based on understanding the cyber threats, control systems vulnerabilities, and attack paths, and control systems engineering.

The practices recommended in the program are focused to increase security awareness and provide security practices that have been recommended by industry to aid in a secure architecture. Additional recommended practices and supporting documents that cover specific issues and associated mitigations will continue to be added on a regular basis.

# THURSDAY, MARCH 8

## Continental Breakfast

Georgia Pre-Function, Level One  
7:00 am – 8:00 am

## PLENARY SESSION

Georgia 4, 5 & 6, Level One  
8:00 am – 8:40 am

During the morning plenary session, attendees will be introduced to the planned activities for the remainder of the day. The breakout sessions that immediately follow will work towards obtaining opinions on met expectations, missing features, recognition of requirements, and other tangible information related to the solution tracks. Attendees will collaborate towards consensus on outstanding issues and identify specific action items and associated benchmarks.

### Solution Track Breakout Sessions

Room: Georgia 4, 5, & 6: Architecture/Design  
Georgia 7 & 8: Device/Components  
Georgia 9 & 10: Requirements/Operational Considerations  
Georgia 11 & 12: Understanding Risk  
Time: 8:45 am – 10:45 am

## Networking Break

Georgia Pre-Function, Level One  
10:45 am – 11:00 am

## PLENARY SESSION

Georgia 4, 5 & 6, Level One  
11:00 am – 12:00 pm

A closing plenary session will provide an opportunity for attendees to make an immediate impact on progress by jointly identifying commonalities, sharing best practices, and identifying and prioritizing next steps.

## Lunch

Garden Courtyard, Level Two  
12:00 pm – 1:00 pm

### **International Electrotechnical Commission (IEC) TC65/WG10 Meeting**

**Room:** Georgia 9 & 10, Level One  
**Time:** 2:00 pm - 6:00 pm

The International Electrotechnical Commission (IEC) TC65/WG10 is writing a three-part international standard on system and network security for industrial process measurement and control systems:

- IEC 62443-1, Framework and Threat-Risk Analysis
- IEC 62443-2, Security Assurance: Principles, Policy, and Practice
- IEC/TS 62443-3, Sets of Security Requirements for Security Elements in Typical Scenarios

IEC standards Working Group meetings are open to all observers, who will be permitted to participate in discussions.

### **Solutions for Process Control Security (4 hours)**

**Room:** Georgia 13, Level One  
**Time:** 2:00 pm – 6:00 pm

**PRE-REGISTRATION REQUIRED – PLEASE VISIT THE CSSP BOOTH TO REGISTER**

#### **Who should attend?**

Managers, engineers, IT staff and operators of process control systems

#### **Course Description:**

The Solution for Process Control Security training is a fast-paced course covering general control systems cyber security challenges. The training objectives include helping participants understand how attacks against control systems can be launched, identifying targets of opportunity, and providing mitigation strategies. Participants will gain an understanding of how to increase the cyber security posture of their control systems networks.

#### **Topics Covered**

- Process control network communications overview
- Common vulnerabilities of control systems
- Inadequate policies and procedures
- Poorly designed control systems networks
- Misconfigured or unpatched operating systems and embedded devices
- Inappropriate use of wireless communication
- Inadequate authentication of control systems communications
- Inadequate identification and control of access to control systems
- Lack of detection and logging of intrusions
- Dual use of control systems networks
- Lack of security checking of control systems software/applications
- Lack of change management/change control procedures and agreements
- Potential mitigation strategies based on multiple levels of implementation
- Cyber-security awareness demonstration video

# FRIDAY, MARCH 9

## International Electrotechnical Commission (IEC) TC65/WG10 Meeting

**Room:** Georgia 9, Level One  
**Time:** 8:00 am – 3:00 pm

The International Electrotechnical Commission (IEC) TC65/WG10 is writing a three-part international standard on system and network security for industrial process measurement and control systems:

- IEC 62443-1, Framework and Threat-Risk Analysis
- IEC 62443-2, Security Assurance: Principles, Policy, and Practice
- IEC/TS 62443-3, Sets of Security Requirements for Security Elements in Typical Scenarios

IEC standards Working Group meetings are open to all observers, who will be permitted to participate in discussions.

## Intermediate Control Systems Security (8 hours)

**Room:** Georgia 13, Level One  
**Time:** 8:00 am – 5:00 pm

**THIS CLASS IS CURRENTLY FULL. PLEASE VISIT THE CSSP BOOTH FOR ADDITIONAL INFORMATION.**

### Who should attend?

Technical staff responsible for securing process control and SCADA systems

### Course Description

This hands-on course is structured to help students understand exactly how attacks against process control systems could be launched and why they work, and to provide mitigation strategies to increase the cyber security posture of their control systems networks.

Because this course is hands-on, students will get a deeper understanding of how the various tools work. Accompanying this course is a sample process control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network also is used during the course for the many hands-on exercises that will help the students develop control systems cyber-security skills they can apply when they return to their jobs.

### Topics Covered

- General security observations and pitfalls
- Process control network communications overview
- Potential process control network entry points and defenses
- Process control network scanning and vulnerability identification (in a safe manner)
- Network monitoring and simple intrusion detection
- Dissecting process control protocols
- Common programming pitfalls
- Modern hardware and OS mitigation strategies
- Incident response essentials for the control systems community

***Every student attending this course must bring a laptop computer on which they have administrator rights. All students should have basic coding skills, a working knowledge of Linux, and a deep understanding of networking. Students who do not meet these requirements should consider the four-hour "Solutions for Process Control Security" course as an alternative.***

## *Keynote Biography*

### **Bruce Landis**

Mr. Landis was appointed Deputy Assistant Secretary for Cyber Security and Telecommunications (CS&T) for the Department of Homeland Security (DHS), within the Preparedness Directorate in January 2007. CS&T works to enhance the security, resiliency, and reliability of the Nation's cyber and communications infrastructure in collaboration with multiple public, private, and international entities.

Prior to joining CS&T, Mr. Landis served at DHS as the Deputy Director, Contingency Planning and Field Based Preparedness for the National Preparedness Task Force. In this role, he managed a range of DHS planning activities responsive to the national homeland security planning requirements, including scenarios for catastrophic hurricanes, terrorist attacks and pandemic disease. Mr. Landis was responsible for the planning of and support to DHS field-based preparedness capabilities, including the nomination, training, and exercise of Principal Federal Officials and their support teams.

Before joining DHS in December 2004, Mr. Landis was a professional cryptologist and held a number of intelligence analyst and management positions spanning more than two decades at the National Security Agency.

In 1998, Mr. Landis served as a Congressional Fellow on Senator Dan Coats' staff. He is a distinguished graduate of the Naval War College, and received his Baccalaureate from the University of Wisconsin - Milwaukee.

## *Speaker Biographies*

### **Dwight Anderson**

Mr. Anderson is the security product manager for Schweitzer Engineering Laboratories located in Pullman, Washington. Prior to joining Schweitzer in 2005, he worked twenty years at Hewlett-Packard as an aerospace and defense business development manager and systems engineer working on projects ranging from electronic warfare countermeasures to SCADA system programming. He recently published an article in the UTC Journal regarding the effect to SCADA channel bandwidth when adding encryption. He received his Bachelor's degree in Electrical Engineering from Stevens Institute of Technology.

### **Ori Artman**

Mr. Artman is the chief technology officer for Teltone Corporation and is responsible for product vision and full product cycle, including development, product management, and support. Prior to joining Teltone in 2003, Mr. Artman served as vice president of technology at MTS LTD, a publicly traded telecommunication software ISV, where he headed the Product Management group; and held similar assignments in New York, New Jersey, Israel and Washington. Mr. Artman was part of the team that led to a successful IPO. While at MTS, Mr. Artman played a major role in transitioning applications from DOS to Windows as well as a similar transition to the Web paradigm. Applications ranged from world class call accounting solutions and voice and data billing to OEM solutions and more.

### **Andrew Bartels**

Mr. Bartels is the chief technology officer for Aegis Technology, Inc. He is a leading expert in designing, engineering, and implementing technology for the financial industry. He developed encryption and security solutions for electronic and Internet transactions in the banking industry, led the development of high-speed financial inquiry systems, and managed open system solutions for financial services, retailers, governments, and other businesses worldwide.

### **Clint Bodungen**

Mr. Bodungen is the president of the Critical Infrastructure Institute – USA and the vice president of the ISA Houston Section – Industrial Computing and Control Systems Subsection. He began his professional career as a computer systems security officer and operational security manager in the United States Air Force. Following the Air Force, he was employed by Symantec to test Network Intrusion Detection Systems (IDS), including authoring several custom IDS evasion and penetration testing tools. Over the past decade, Mr. Bodungen has built corporate security departments from the ground up, led numerous security audits and penetration testing teams, and has played a key role in securing some of the nation's top organizations within the heart of our critical infrastructure and SCADA industries including the Department of Defense, top Fortune 500 oil and gas companies, financial institutions, transportation agencies, utility companies, healthcare organizations, and Fortune 500 telecommunications companies. He now continues his efforts in helping to secure our nation's critical infrastructure environments through research and instruction at the Critical Infrastructure Institute.

### Wayne Boyer

Mr. Boyer is an advisory engineer/scientist at the Idaho National Laboratory (INL) in Idaho Falls, Idaho and a computer science instructor for the University of Idaho in Idaho Falls. Mr. Boyer received a B.S. degree in electrical engineering from Brigham Young University; his M. S. degree in electrical engineering from Stevens Institute of Technology, and his Ph.D. in computer science from the University of Idaho. Before joining the Idaho National Laboratory, he was a member of the technical staff and technical supervisor at AT&T Bell Laboratories in Whippany, New Jersey and Denver, Colorado. He has extensive experience in real time software development. His current research interests are in parallel computing and network security for control systems.

### Greg Burns

Mr. Burns is a solution architect for the Enterprise and Networks Services Practice at Invensys Process Systems. He has been working in computer networking since 1979. He has experience as a system engineer, network engineer and solution architect for companies including IBM, Wang Laboratories, Digital Equipment Corporation, VideoServer, Compaq, Nortel Networks, and Unisys. Mr. Burns has a B.S. degree from Northeastern University.

### Eric Byres

Recognized as one of the world's leading experts in the field of critical infrastructure security, Eric Byres has been responsible for numerous standards, best practices, and innovations for data communications/controls systems security in industrial environments.

Mr. Byres' work in industrial cyber security spans both the academic and industry domains. As the founder of the BCIT Critical Infrastructure Security Centre, he shaped it into one of North America's leading academic facilities in the field of SCADA cyber-security, culminating in a SANS Institute Security Leadership Award in 2006. At the same time, he has provided security guidance to government security agencies and major energy companies on cyber protection for critical infrastructures. Mr. Byres also is the chair of the ISA SP-99 Security Technologies Working Group and is the Canadian representative for IEC TC65/WG13, a standards effort focusing on an international framework for the protection of process facilities from cyber attack.

Mr. Byres' achievements include testifying to the U.S. Congress on the "Security of Industrial Control Systems in National Critical Infrastructures" as well as receiving awards from international organizations. These include the IEEE Outstanding Industry Applications Article prize in September 2000, the 2004 Donald P. Eckman Education Award, and the 2005 Keith Otto Award presented by the Instrumentation, Systems, and Automation Society (ISA).

### Clayton L. Coleman

Mr. Coleman is currently a solutions architect at Invensys Process Systems. He has been working in the process controls industry for eight years, primarily focused on industrial security and information technology. He holds both CISSP and SANS certifications. In the past three years, he has been the principal in over twenty security assessments at critical infrastructure facilities.

### John Cummings, Ph.D.

Dr. Cummings is a senior manager in the Advanced Concepts Group (a small think tank) at Sandia National Laboratories in Albuquerque, NM. He also serves as the director of a project on process control systems security research for the Institute for Information Infrastructure Protection (I3P). Dr. Cummings was on assignment from Sandia in Washington, DC for three years, as the director of the R&D program for critical infrastructure protection for the Science and Technology Directorate of the Department of Homeland Security. While at DHS, he was the chair of the Infrastructure Subcommittee (of the National Science and Technology Council) and led an interagency effort to create the first National Plan for Research and Development in Support of Critical Infrastructure Protection. Before his position with DHS, he was the deputy to the chief technology officer at Sandia. He has worked at Sandia for over 30 years in a wide variety of technical staff and management positions. His technical work includes research in experimental fluid mechanics, combustion, and the use of laser-based instrumentation.

Before coming to Sandia, Dr. Cummings was employed by the Engineering Sciences Department at TRW Systems, Inc., where he conducted studies of HF and DF chemical lasers. Dr. Cummings serves on the Science Advisory Committee of the Homeland Security Center for Risk and Economic Analysis of Terrorism Events (CREATE), located at the University of Southern California. He is a member of the American Physical Society Division of Fluid Dynamics, and he served as the U.S. representative to the International Atomic Energy Agency working on the mitigation of hydrogen combustion hazards in nuclear power plants.

Dr. Cummings received his B.S., M.S., and Ph.D. (1973) degrees from Caltech. His Ph.D. research involved the development of a cryogenic shock tube and the study of strong shock waves in gaseous and liquid helium. He is the author or coauthor of over 50 technical publications and reports.

## **Gary J. Finco**

Mr. Finco is a member of the Critical Infrastructure Protection/Reliability directorate at the Idaho National Laboratory (INL). He is the deputy project manager for the National SCADA TestBed Program (NSTB) established by the Department of Energy (DOE-OE) and a senior advisory engineer for the Control System Security Program (CSSP), a Department of Homeland Security (DHS) effort. He is one of the authors of the Cyber Security Procurement Language Guide for Control Systems, a project funded by DHS.

Mr. Finco has 28 years of experience in real-time data acquisition (22 of those with SCADA and EMS systems). He has worked for Texas Instruments, Abbott Laboratories, DataLab Inc., and ABB Inc. before joining INL in February of 2005. While at ABB, Mr. Finco was the project manager for the first SCADA/EMS system to be tested under the NSTB project. Mr. Finco graduated from the Milwaukee School of Engineering with a B.S. degree in electrical engineering technology and an A.S. degree in computer engineering technology.

## **Clifford Glantz**

Mr. Glantz is a senior staff scientist with Pacific Northwest National Laboratory, where he manages projects and conducts research in consequence assessment modeling, emergency response and preparedness, and critical infrastructure protection.

Currently, he is leading the Security Metrics Team for the Institute for Information Infrastructure Protection's (I3P) PCS Security Project. In the recent past, he also has tackled cyber security risk assessment and risk management issues for the Nuclear Regulatory Commission and the North American Electric Reliability Council. Mr. Glantz is a member of the PCSF SCADA Cyber Security Self-Assessment Working Group (SCySAG) and the chair of the Department of Energy's Subcommittee on Consequence Assessment and Protective Actions.

## **Darren Reece Highfill**

Mr. Highfill is a Software Engineer and the information security architecture expert for EnerNex Corporation. He is one of the system architects for the PowerWAN – TVA's new wide-area IP-communications network – and has been heavily involved in the integration of the Bradley County 500kV Substation. He is the primary author of the overall security policy for the PowerWAN as well as many other reference documents and specifications for both the PowerWAN and Bradley Substation projects.

He also serves as the information security expert for EnerNex in support of Southern California Edison's Advanced Metering Infrastructure Project. He has developed the information security framework that will be used to manage risk, write policy, and produce specifications for SCE, and has adapted this framework for broader reference by the UtilityAMI forum.

Mr. Highfill is a Certified Information Systems Security Professional (CISSP) and holds Bachelor's and Master's degrees in Engineering Technology from East Tennessee State University.

## **Brian Isle**

Mr. Isle is the chief of operations and a member of the technical staff at Adventium Labs. His current technical focus is in assessment of critical infrastructure safety and security. Mr. Isle is a key member of the Air Force Association's Critical Infrastructure Team, which is responsible for creating the threat scenario-based Vulnerability Assessment and Prioritization Methodology and the application to Minnesota's homeland security effort. Mr. Isle currently is supporting a Department of Defense program developing approaches for automating aspects of vulnerability assessment for force protection at military bases and a Department of Homeland Security program to apply advanced cyber protection technology to control systems for critical infrastructure. He recently supported the onsite demonstration of a next-generation cyber security technology at the Joint Warrior Interoperability Demonstration at U.S. Northern Command. As an engineer, his technical accomplishments range from low-cost home automation systems to fiber optic communication systems for NASA's space station development. He has been awarded four patents and has published over 20 papers. Mr. Isle is Chair of the Process Control Systems Forum SCADA Cyber Self-Assessment Working Group for manufacturing and process control systems.

## **Jeff Kalibjian**

Mr. Kalibjian is currently a senior security architect in Hewlett Packard's Atalla Security Products. Atalla Security Products has been a leader in hardware-based security for over thirty years. He is lead architect for HP's new energy compliance product: the Trusted Compliance Solution for Energy. He has been on the senior management teams of two security start-ups and has had his own security consulting company. Prior to working in the public sector, Mr. Kalibjian spent twelve years at the Lawrence Livermore National Laboratory, where he was involved in pioneering work in such fields as missile defense, automated design and manufacture, and electronic commerce. He has a B.S. in electrical engineering and computer science from UC Berkeley and is chairman of the IEEE East Bay Computer Society.

### **Stu W. Katzke, Ph.D.**

Dr. Katzke began his second career at NIST as a senior research scientist in July 2001. In that role, he provides technical advice to the Computer Security Division (CSD), establishes government-industry partnerships for the purpose of improving the security of critical infrastructure IT systems, and works on NIST's FISMA implementation project. He currently leads an effort to improve the security of industrial control/SCADA systems that are operated by or for federal agencies. In January 2000, Stu joined NSA as chief scientist of the Information Assurance Solutions Group. Prior to joining NSA, Stu was Chief of the Computer Security Division in the Information Technology Laboratory at NIST from 1987 - 2000. During his 29-year career at NIST, Stu initiated and participated in the Common Criteria Project, conceived and established the National Information Assurance Partnership, and authored numerous publications. He has received a Bronze and Silver Medal from the Department of Commerce and the 2003 Award for Outstanding Contributions in the Field of Mathematics and Computer Science from the Washington Academy of Sciences.

### **Henry "Hank" Kenchington**

Mr. Kenchington is a senior manager with the United States Department of Energy's Office of Electricity Delivery and Energy Reliability (OE). OE leads the Department's efforts to ensure a secure and reliable flow of energy to the nation. His current responsibilities include strategic planning and program management for OE's activities in control systems security, including the National SCADA Test Bed. With the Department since 1996, he has also served as director of technology implementation in the Office of Industrial Technologies.

Mr. Kenchington was vice president of an engineering consulting firm and manager of a strategic business unit for a major industrial manufacturer. He holds a bachelor's degree in mechanical and nuclear engineering from Virginia Polytechnic Institute and a master's degree in engineering management from the George Washington University.

### **Nate Kube**

Mr. Kube received the honors B.Sc. degree in mathematics and computer science from the University of Victoria in 2002. With a national scholarship, he entered UVIC's Ph.D. program in computer science. While in the doctoral program, he worked at BCIT's Critical Infrastructure Protection Lab with the acclaimed industrial security researcher Eric J. Byres. Among other industrial security projects, Mr. Kube played an integral role in the design and architecture of the Achilles project, an innovative vulnerability assessment tool for industrial controllers. He currently is defending his Ph.D. work on vulnerability testing protocol implementations in SCADA/DCS devices.

In 2006, Mr. Kube co-founded Wurdtech Security Technologies, where he currently holds the position of CTO. He is responsible for the management of industrial security testing and product development operations, including Wurdtech's flagship product, Achilles. He and his team specialize in formal methods for software testing, operations research / statistical modeling, critical infrastructure protection, and embedded systems design and testing.

### **David G. Kuipers**

Mr. Kuipers is currently a principle engineer/scientist with a bachelor's degree in Industrial Technology (Computer Electronics and I&C). He has been working in operations and design of instrumentation & control systems (DCS, SCADA, and Hybrid) for 30 years. He started his career in nuclear power plant operations with the U.S. Navy, then at the Idaho National Laboratory (INL). He has worked as a control systems engineer for 17 years. Mr. Kuipers is currently the Test Bed Coordinator for the INL control systems test bed. His responsibilities include test bed management and operations, vulnerability assessment project principle investigator, training developer, and design lead for the CSSP recommended practices project. He has been assigned to projects requiring control systems expertise in development of test plans, vulnerability assessments, and information gathering efforts to identify threat vectors, and mitigations to unsecured systems.

### **T.S. "Chip" Lee**

A corrosion engineer by education and training, Mr. Lee has been in engineering society management for over 20 years. He currently directs the InTech and book publishing activity of ISA. He also directs the standards development activities of the Society including management of the recently created Automation Standards Compliance Institute.

### **Brian Lopez**

Mr. Lopez is a computer scientist at Lawrence Livermore National Laboratory (LLNL). For the past decade, he has led LLNL's Vulnerability and Risk Assessment Program (VRAP), which provides in-depth, multi-disciplinary assessments of threat, vulnerability, and consequence. Past projects include work in 28 U.S. states and internationally across sectors, including electric power, oil, gas, water, chemical, aviation, rail, maritime, telecommunications, national icons, and classified sites. He assembled and led security teams for the 2002 Winter Olympics, California Energy Crisis, and 9/11 response. He is a co-author of the recent book *Seeds of Disaster* (Cambridge University Press) regarding critical infrastructure security.

## Art Manion

Mr. Manion leads the Vulnerability Analysis Team at the CERT Coordination Center (CERT/CC) at Carnegie Mellon University. In this role, he supervises technical analysis, interactions with stakeholders, and coordination and disclosure of vulnerability information. Mr. Manion has written advisories, alerts, and vulnerability notes for CERT/CC and US-CERT. He also researches new ways to manage vulnerability information, decision making, economic factors of vulnerability disclosure, and ways to improve software quality and security. Prior to working at the CERT/CC, Mr. Manion was the director of network infrastructure at Juniata College. He received a B.S. degree from Penn State University in quantitative business analysis.

## Miles McQueen

Mr. McQueen is a principal investigator with Idaho National Labs (INL) and is on the computer science graduate faculty at the University of Idaho, Idaho Falls. He has over twenty-five years of experience in complex system-level analysis and design, including real-time systems, sensors, simulations, and security, and he has more than twenty peer-reviewed publications in the area of survivable systems and computer security. In addition, he has done advanced work in computer science and economics, where his emphasis was in micro-economics. Mr. McQueen currently teaches classes in analysis of algorithms, computer security, and software engineering metrics. He holds degrees in computer science, mathematics, and economics.

## Dr. Ann Miller

Dr. Miller is the Cynthia Tang Missouri Distinguished Professor of Computer Engineering at the University of Missouri – Rolla. Previously, she was the deputy assistant secretary of the Navy for command, control, communications, computing, intelligence, electronic warfare, and space. For a portion of that time, she also served as the Department of the Navy's chief information officer (CIO). Dr. Miller also served as director for information technologies with the U. S. Department of Defense, Research and Engineering. Prior experience includes over 12 years with Motorola, Inc., where she held a variety of technical and managerial positions, including chief software engineer for Motorola's Tactical Secure Communications Office and for the company's Satellite Communications Division.

Dr. Miller holds a U.S. patent in satellite communications, has co-authored four books, and is the author of more than five dozen articles and monographs. Her research involves the security, reliability, and survivability of large-scale networked systems, including SCADA systems. She currently chairs the NATO Information Systems Technology Panel. She is a senior member of IEEE and a member of the IEEE Communications, Computer, and Reliability societies. Her research interests are in the security and reliability of networked systems, including process control systems.

## William Miller

Mr. Miller is president of Maximum Control Technologies (MaCT), which has offices in the U.S., Canada, and Hong Kong. He is a graduate of Pennsylvania State University with a degree in electrical engineering and telecommunications and has over 27 years of experience in systems integration and design of process control systems for the power, pulp and paper, chemical, and cement industries. He is active in a number of U.S. government forums for the development of security standards for industrial process control systems, wireless systems, information assurance, supply chain, and enterprise integration.

## Trent Nelson

Mr. Nelson is currently a principle engineer/scientist at Idaho National Laboratory and has a bachelor's degree in computer information systems (CIS). He has been working with computers and CIS systems for 15 years. Currently, he is the cyber security assessment lead within the Control Systems Security Center (CSSC) organization. His responsibilities include cyber tools, testing, and evaluation of critical infrastructure. He also is assigned as the technical lead within the Communications and Cyber Security Resources Department at the Idaho National Laboratory (INL). He manages a core cyber technical staff of 10 employees. Mr. Nelson has been assigned to multiple projects that have required the development of test plans, vulnerability assessments, and information gathering efforts to identify threat vectors, and mitigations to unsecured systems.

## David L. Norton, CISSP

Mr. Norton currently holds the Electric Sector seat on the DHS Process Control Systems Forum Board of Governors. He is a Certified Information Systems Security Professional (CISSP) with 30+ years experience in technical leadership positions in information technology, manufacturing automation, electric sector EMS/SCADA, and real-time military and intelligence environments. He was one of the drafters of the CIP Cyber Security Standards, and in compliment has played a leadership role on the SERC Cyber Security Compliance Review Subcommittee engaged in compliance measurement of the CIP Standards he helped develop. Within Entergy, he is leading implementation of a next generation high-speed digital communications networking architecture of his design to support substation automation (e.g., IEC 61850) and a move to new EMS/SCADA platforms. This experience has brought an end-user perspective to the Sandia OPSAID project aimed at creating a reference implementation of next generation TCP/IP protocols and related security improvements for PCS/DCS environs. Finally, Mr. Norton has actively worked with authorities at the local level to identify lessons learned and needed improvements to first-responder command and control systems in the wake of Hurricanes Katrina and Rita.

## Raymond Parks

Mr. Parks is a core team member of Sandia National Laboratories' Information Design Assurance Red Team (IDART), a senior member of the technical staff in Sandia's Information Operations, Red Teaming and Assessments (IORTA) Department, and architect of the Center for SCADA Security Test Bed and Virtual Control System Environment. He has worked on assessments of control systems security and taught that assessment methodology to industry and government. Mr. Parks recently has led tests to measure the effects of boundary layer controllers on SCADA communications and is preparing the CSS Test Bed for assessment of new security technologies.

## Perry A. Pederson

Perry currently leads the DHS effort to reduce cyber risk to control systems as the Director of the Control Systems Security Program within the National Cyber Security Division (NCSD). Perry holds a bachelors degree in information systems and a masters in information security. Perry has held a number of IT security positions in the private sector as well as the government, and prior to joining NCSD he served as the Infrastructure Protection Program Manager for the Technical Support Working Group (TSWG) at DoD. At the TSWG, he was responsible for R&D and new technology programs to improve critical infrastructure protection and cyber security.

## Raphael Gomes Pereira

Mr. Pereira is currently head of information security for Chemtech–The Siemens Company, Rio de Janeiro, Brazil. His responsibilities include the internal Security Office, protecting internal information assets and reports to the organization board. Additionally, he is the manager of internal implementation of Information Security Management System compliance for ISO:IEC 27001:2005.

## Dale Peterson

Mr. Peterson has been in the information security industry for 20 years. He began his career with the National Security Agency (NSA), where he was an award-winning and certified cryptanalyst. In 1998, he started Digital Bond, where he leads the SCADA Security Consulting and Research Practice. He has performed SCADA cyber security assessment, architecture and policy engagements for water, oil and gas, electric, and other control system markets.

In the area of SCADA security research, Dale Peterson and Digital Bond developed the SCADA plug-ins for the Nessus Vulnerability Scanner, SCADA IDS signatures that are deployed by almost all IDS vendors, and a SCADA Honeynet. Digital Bond provided the first SCADA vulnerabilities to US-CERT / CERT-CC. Mr. Peterson also is the program chair and proceedings editor for Digital Bond's SCADA Security Scientific Symposium (S4).

## Jonathan Pollet

Jonathan Pollet, founder of PlantData Technologies, has a blended history of over 10 years of experience in SCADA systems, custom software development, and cyber security. In addition to developing and growing PlantData Technologies as a solid Industrial Consulting firm, Mr. Pollet also led a blend of physical and cyber security teams on over 50 SCADA and DCS vulnerability assessments for critical infrastructure facilities. In addition, he led several covert red team penetration tests performed for U.S. and Canadian utility and energy companies with SCADA and real-time control systems. PlantData Technologies also consults with energy companies in areas relating to SCADA, data integration, and software integration issues.

Prior to founding PlantData Technologies, Mr. Pollet was the director of operations for a Systems Integration and SCADA Design firm in Bakersfield, California. He also worked as an automation engineer for Chevron USA Production Company, where he designed and implemented SCADA Systems for both offshore and onshore oil and gas production fields in Louisiana and California.

Mr. Pollet graduated from the University of New Orleans with honors, and earned a B.S. degree in electrical engineering. Throughout his career, he has been actively involved with the IEEE, ISA, ISSA, UTC, CSIA, and other professional societies. Mr. Pollet has given several presentations and training sessions on SCADA systems, systems integration, and SCADA security to the FBI, the Department of Homeland Security, and the United Telecom Council, and he has spoken at many other conferences and workshops for government and professional organizations.

## R. Eric Robinson

Mr. Robinson is a senior scientist in the Cyber Security group at Pacific Northwest National Laboratory. His research focuses on providing database and network security capabilities that adapt to novel threats and errors autonomously. Recent work in this area includes the development of REBOUND, an artificial homeostatic framework, and SHARP, a dynamic environment that better secures process control network systems.

## **Chris Sandford**

Mr. Sandford currently is a principle consultant with International Network Services (INS) and has worked in the IT industry for over 15 years, specializing in critical infrastructure and security. Over the last seven years, he has worked with INS on projects with a major oil and gas company, Global telecom provider, power company, and within the airline industry. He has conducted risk assessments on process control networks, designed large scale secure networks, and has been part of a team that created, planned, and designed a global process control network architecture and associated processes. He also has worked in the space and satellite industry and with a major food manufacturer.

## **Robert Sill**

An industry pioneer, Mr. Sill has more than twenty years of leadership experience in business, manufacturing, and technology, including extensive experience in utilities. He specializes in growing companies, Aegis being his fourth. Currently, he is president and CEO of Aegis Technology, Inc.

He is a leader in the integration of engineered products with computer technology. Mr. Sill has spearheaded the development of lean manufacturing techniques in the automotive industry, managed global purchasing, and patented engineering solutions that have revolutionized industrial systems.

## **Rhett Smith**

Mr. Smith received his engineering degree in 1999 and is GSEC certified. He is currently an applications engineer in the time & communications group at Schweitzer Engineering Laboratories.

## **Jason Stamp, Ph.D.**

Dr. Stamp is a principal member of the technical staff at Sandia National Laboratories in Albuquerque, New Mexico. His research areas include the development of improved tools for information security and the integration of network technology into security architectures for infrastructure, homeland security, and the military. Dr. Stamp regularly participates in information security assessments for government and infrastructure, including electric power transmission and distribution, hydroelectric dams, water treatment and distribution, and petroleum storage and refineries. He was a member of the task force that investigated and analyzed the August 2003 power outage in the United States, and has presented at several conferences for SCADA and automation security.

Dr. Stamp has been at Sandia for over seven years, working in the field of information systems and national security. He also is an active researcher in the field of electric power. He received a bachelor of science degree in electrical engineering from the Rose-Hulman Institute of Technology in Terre Haute, Indiana in 1995 and his Ph.D. in electrical engineering from Clemson University in 1998. Dr. Stamp is an active member of the Power Engineering Society of the IEEE.

## **David J. Teumim**

Mr. Teumim is an independent consultant specializing in control systems security. He has taught seminars and chaired conferences for ISA in this area, and he has written the first book on this subject, *Industrial Network Security*, which was published in 2004 by ISA Press. Mr. Teumim has a master's degree in chemical engineering and is certified as a CISSP. Recently, he has focused on the application of control security to the area of rail transit.

## **Michael Torppey**

Mike Torppey is a senior principal with Noblis and technical manager of the Process Control Systems Forum (PCSF). He has more than ten years of information technology management experience and is an accomplished software engineer. As director of operations with Victory Springs, Inc., he directed the development, production and testing, and maintenance programs behind Smart E-Records™, a Web-enabled medical records portal application.

Mr. Torppey has presented at numerous meetings and symposia on topics including information technology, requirements planning, application design, health-care technology, and the Process Control Systems Forum. He holds a bachelor of arts degree in economics from Rutgers University.

### **Alfonso Valdes**

Mr. Valdes is a senior computer scientist at the Computer Sciences Laboratory at SRI and has led several projects in information security for such clients as the Defense Advanced Research Projects Agency (DARPA) and the Advanced Research and Development Activity (ARDA), and the Department of Homeland Security. He has coordinated the insertion of technology components from these and other projects into exercises with the U.S. Army and Navy. Mr. Valdes is an expert on statistical algorithms for detection and modeling and the application of such techniques in the information security arena. He has led statistical algorithm development in SRI's Next-Generation Intrusion Detection Expert System (NIDES) and, later, EMERALD. Mr. Valdes has implemented a high-speed Bayes component to detect network intrusions, as well as an innovative probabilistic approach to correlation of reports from heterogeneous intrusion detection sensors. In the EMERALD project, he has developed and improved algorithms from the standpoint of detection performance, false alarm rate, and computational efficiency. He holds two patents in the field of computer intrusion detection.

Mr. Valdes also is an expert on a wide variety of statistical and classification techniques, including likelihood theory, decision analysis, neural networks, simulation, and Bayesian formalisms. He has applied these methods with great success in a number of problem domains, including signal processing and environmental and medical sciences, in addition to information security.

More recently, he has introduced ultra-scalable methods to visualize unusual or potentially malicious activity at very high levels in computer networks. Over the last two years, Mr. Valdes has taken an interest in critical infrastructure systems such as the distributed control and SCADA systems that operate refineries and pipelines in the oil and gas sector.

### **Joe Weiss**

Mr. Weiss is an industry expert on control systems and electronic security of control systems, with more than 30 years of experience in the energy industry. Mr. Weiss spent more than 14 years at the Electric Power Research Institute (EPRI) where he led a variety of programs including the Nuclear Plant Instrumentation and Diagnostics Program, the Fossil Plant Instrumentation & Controls Program, the Y2K Embedded Systems Program and, the cyber security for digital control systems. As Technical Manager, Enterprise Infrastructure Security (EIS) Program, he provided technical and outreach leadership for the energy industry's critical infrastructure protection (CIP) program. He was responsible for developing many utility industry security primers and implementation guidelines. He was also the EPRI Exploratory Research lead on instrumentation, controls, and communications.

Mr. Weiss serves as a member of numerous organizations related to control system security. These include the North American Electric Reliability Council (NERC) Critical Infrastructure Protection Committee (CIPC), the International Electrotechnical Commission (IEC) Technical Committee (TC) 57 Working Group 15 - Data and Communication Security, the Process Controls Security Requirements Forum, CIGRÉ Joint Working Group D2/B3/C2 01- Security for Information Systems and Intranets in Electric Power Systems, and other industry working groups. He serves as the Task Force Lead for review of information security impacts on IEEE standards. He is also a Director on ISA's Standards and Practices Board. Mr. Weiss was involved in the development of, and participated in, the April 2002 White House Conference on CIP - "Developing Secure Digital/Electronic Process Control Systems for the Nation's Critical Infrastructures." He was an invited speaker at the NIST/NSA Information Security Summit and provided testimony before two Congressional subcommittees. He is also an invited speaker at many industry and vendor user group security conferences, has chaired numerous panel sessions on control system security, and is often quoted throughout the industry.

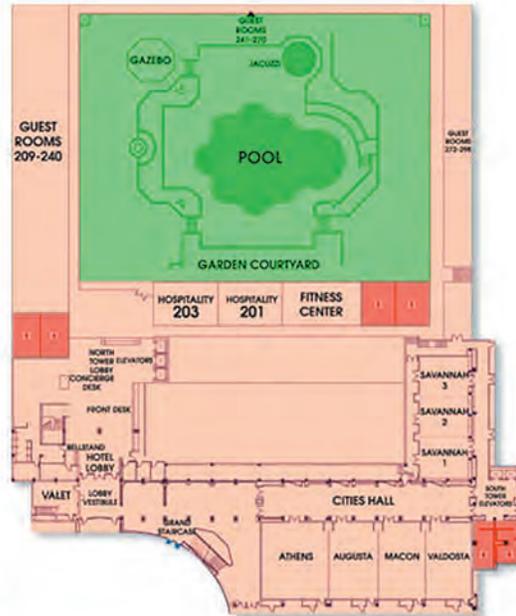
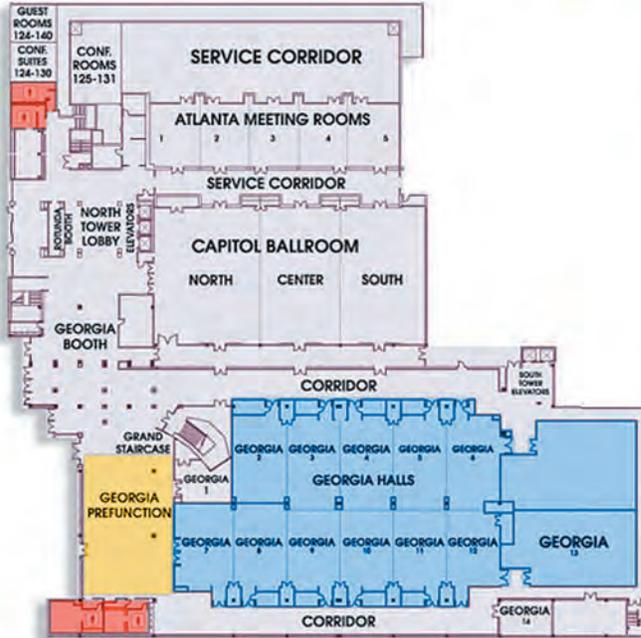
He holds two patents and has published over 60 papers on instrumentation, controls, and diagnostics including a chapter on cyber security for Electric Power Substations Engineering. Mr. Weiss has conducted several SCADA, substation, plant control system, and water systems vulnerability and risk assessments and conducted short courses on control system security. He also established and chairs the annual KEMA Control System Cyber Security Workshop and established the International Standards Coordination Meeting on Control System Cyber Security. Mr. Weiss has received numerous industry awards, including EPRI Presidents Award (2002) and is an ISA Fellow and a member of the ISA Engineering, Science, and Technology Policy Committee. He is a registered professional engineer in the State of California and a Certified Information Security Manager.

### **Andrew Wright, Ph.D.**

Dr. Wright is a research staff member in the Critical Infrastructure Assurance Group at Cisco Systems. His expertise lies in the areas of security, applied cryptography, digital rights management, and programming languages. Currently, he is working with members of the automation, oil and gas, and electric industries on network architectures for secure control systems. Previously, he contributed significantly to the design of AGA-12, a cryptographic protocol for protecting serial SCADA communications, and developed ScadaSafe, an open source implementation of AGA 12. His background includes over 10 years in various industrial research positions and a Ph.D. in computer science from Rice University.



**Sheraton Atlanta**  
HOTEL



## *Legend*

 Registration and Information  
Tuesday/Wednesday/Thursday  
Breakfast

 Restrooms

 Meeting Rooms

 Tuesday Reception  
Tuesday/Wednesday/Thursday  
Lunch



3150 Fairview Park Drive South, MS F310  
Falls Church VA 22042

[www.pcsforum.org](http://www.pcsforum.org)