



**Process Control Systems  
Industry Conference**

# 2008 **INDUSTRY CONFERENCE**

*“Tactical & Strategic Solutions for the Control Systems Community”*

**CONFERENCE PROGRAM**

*HILTON LA JOLLA TORREY PINES  
LA JOLLA, CALIFORNIA*

**AUGUST 26 – 28**

# AT-A-GLANCE AGENDA

## MONDAY – AUGUST 25

	Fairway Pavilion I	Fairway Pavilion II	Fairway Pavilion IV
8:00 am – 12:00 noon	Intermediate Control Systems Security	Introduction to Control Systems Security for the IT Professional	Red Team for Program Managers (RTPM)
1:00 pm – 5:00 pm			Control System Wireless Security
3:00 pm – 7:00 pm	Registration: Grande Ballroom Foyer		

## TUESDAY – AUGUST 26

7:00 am – 7:45 am	Continental Breakfast: Parterre Gardens		
7:00 am – 5:00 pm	Registration: Grande Ballroom Foyer		
<b>PLENARY SESSION:</b> Salons A/B/C, Grande Ballroom			
8:00 am	Welcome and Opening Remarks		
8:30 am	Keynote Address		
9:30 am	Networking Break: Grande Ballroom Foyer		
10:00 am	Security Challenges Facing the Control Systems Environment <i>(Closed to the press)</i>		
11:15 am	Should We Be Scared-a SCADA? <i>(Closed to the press)</i>		
12:00 noon	Lunch – Updates from Energy Sector Roadmap and Water Sector Roadmap		
1:15 pm	Industry Consequences and Mitigation		
2:15 pm	Control System Cyber Incident Handling: A Law Enforcement Perspective Panel		
3:15 pm	Networking Break: Grande Ballroom Foyer		
3:45 pm	Responsible Vulnerability Disclosure		
5:30 pm	ISA Security Compliance Institute (ISCI) – ISA SP99: Salons D/E	Lemnos Interoperable Security Project Birds of a Feather Meeting: Scripps Ballroom II	Water Sector: Scripps Ballroom I

## WEDNESDAY – AUGUST 27

7:00 am – 7:45 am	Continental Breakfast: Parterre Gardens				
7:00 am – 5:00 pm	Registration: Grande Ballroom Foyer				
	R/OC – Scripps Ballroom	UR – Salons D/E	A/D – Salon C	D/C – Salons A/B	UR – Scripps Ballroom
8:00 am	A Trusted Framework for Managing Compliance Evidence	Are You Compliant or Liable? Achieving Solid Cross-Standard Compliance	When Good Traffic Goes Bad: When is Application Traffic Too Much?	Secure ICCP	
9:15 am	Vallourec & Mannesmann Tubes of Brasil: Business Systems and M&C Networks Segregation Project	The Repository for Industrial Security Incidents (RISI)	Design Techniques for Deployment of a Policy Based Network	Secure Access Control for Control System Operations	
10:15 am	Networking Break: Grande Ballroom Foyer				
10:45 am	Raising the Bar On Built-In Cyber Security	Control Systems Threat Awareness	Protecting Safety Instrumented Ssystems from Cyber Attack	Security Beyond Standards	
11:45 am	Lunch: Parterre Gardens				
12:45 pm		Control System Self Assessment and the Water Sector Roadmap	Unidirectional Connectivity – Novel Robust Method for Absolute Protection of Process Control Systems		AchillesINSIDE – Intelligent Cyber Security and Risk Management for Industrial Environment
2:15 pm	Networking Break: Grande Ballroom Foyer				
2:30 pm	Meeting 24x7 Managed Cyber Security for a Process Control Network	Supporting Risk Reduction Decisions Using Scenario-Based Modeling	Secure Access to Industrial Automation and Control Systems (IACS)		
3:30 pm	Intrusion Detection and Prevention Systems in the Industrial Automation and Control Systems Environment	A Hybrid Virtualization Environment for Process Control System Security		Intuitive, Easy, and Secure Provisioning and Configuration of Industrial Sensor and Control Networks	
4:30 pm – 8:30 pm	Solution Provider Evening: Fairway Pavilion (see page 19 for details)				

## THURSDAY – AUGUST 28

7:00 am – 7:45 am	Continental Breakfast: Parterre Gardens			
7:00 am – 4:00 pm	Registration: Grande Ballroom Foyer			
	Scripps Ballroom	Salons D/E	Salon C	Salons A/B
8:00 am	Bandolier: Auditing Control System Security Best Practice with the Nessus Vulnerability Scanner The Hallmark Project: A DOE Co-Operative Project The Lemnos Interoperable Security Project	Panel Session: State of Building Security In: Where Are We in That Process?	Survivability and Recovery of Process Control Systems RiskMAP: Translating ICS Risk Assessments into Corporate Terms The LOGIIC Consortium: A Sustainable Partnership	
9:30 am	Networking Break: Grande Ballroom Foyer			
10:00 am	Cyber Security Self-Assessment Panel	Cyber-Security Issues in Wireless Systems for Critical Infrastructure Protection Monitoring and Situational Awareness in PCS	Industrial Network Design Panel	
11:45 am	Lunch: Parterre Gardens			
1:00 pm	Responsible Vulnerability Disclosure WG	Education and Training WG	Metrics WG	Security Requirements WG
2:15 pm	Networking Break: Grande Ballroom Foyer			
2:45 pm - 4:30 pm	Closing Plenary Session: Salons A/B/C, Grande Ballroom			

**KEY:** R/OC: Requirements/Operational Considerations    UR: Understanding Risk    A/D: Architecture/Design    D/C: Devices/Components    WG: Working Group

# The Evolution of Public-Private Partnership and the Sharing of Intelligence in the Protection of Critical Infrastructure and Control Systems

**Phyllis A. Schneck, PhD**  
**Vice President, Research Integration, Secure Computing Corporation**  
**Chairman Emeritus, Board of Directors, InfraGard National Members Alliance**

*Electronics run our infrastructure and our world. Recently a top cyber agent at the FBI was quoted as saying “computers are everywhere. Most of you drove here in one.”*

Then consider Internet communication. Anyone, anywhere can send anything they wish to a recipient that has little to no control over whether or not the communication is received at the destination gateway. Traditional “viruses and worms” are mere symptoms of abuse of electronic communications resources, indicating the capability to control actions, and hinting of the very real potential for cyber action to cause consequences to physical infrastructure.

As control systems have been increasingly connected to traditional IT systems, exposing the electronics that control physical infrastructure to the vulnerabilities that plague communications, the danger grows. An effective approach to protection of cyber consequences to physical infrastructure requires a shared application of intelligence and expertise between government, industry and academia.

Government and private industry have worked for the past decade to create models for “information sharing.”

While factors such as the lack of protected information and lack of incentives to report or exchange information create a challenge to providing an environment where information can be productively shared, the core components we lack are trusted relationships and knowing who to call pre-crisis. This talk explores the evolution of “information sharing” in the context of cyber security as the nexus of infrastructure security over the past decade, from local community participation to State and Federal programs. We present a changing paradigm and the successes and failures that have led to the current progress, yet continued challenge in creating a trusted forum, with balanced private sector and government coordination, to identify and utilize subject matter expertise, transcending geographic and corporate boundaries.

Ten years ago, the concept of corporations building relationships with government and law enforcement was fairly new. The current environment includes a solid architecture and framework under the National Infrastructure Protection Plan (NIPP) that enables and fosters government-industry partnership. Programs such as the FBI’s InfraGard program extend information sharing to States and local communities, building trusted communities that connect, via relationships, to private sector colleagues and to local, state and Federal law enforcement and government. These local programs also connect horizontally to the vertical sector based programs within the NIPP.

As a nation, we must connect and leverage these for an efficient, cohesive and trusted operational environment for distributing and analyzing actionable information for preparedness, incident response, and the strategic growth of our infrastructures.

## DAILY EVENTS

### Registration – Grande Ballroom Foyer

Monday: 3:00 pm – 7:00 pm  
Tuesday and Wednesday: 7:00 am – 5:00 pm  
Thursday: 7:00 am – 4:00 pm

### Continental Breakfast – Parterre Gardens

Tuesday, Wednesday, and Thursday: 7:00 am – 7:45 am

### Lunch – Parterre Gardens

Wednesday and Thursday: 11:45 am – 12:45 pm

## MONDAY – AUGUST 25

### Introduction to Control Systems Security for the IT Professional

**Room:** Fairway Pavilion II      **Time:** 8:00 am – 5:00 pm  
**Sponsor:** US Department of Homeland Security, Control Systems Security Program

This course is directed to those with IT Security responsibilities or background but have no previous experience in critical infrastructure control systems and their relationship to modern IT networks. Four training sessions will guide attendees from basic definitions, components, and protocols to the major applications and architectures within critical infrastructure and key resources (CIKR). Control system network architectures, cyber threats and vulnerabilities, and mitigations will be presented. Current and emerging government and industry activities that are addressing the issue of risk reduction will be discussed.

### Intermediate Control Systems Security

**Room:** Fairway Pavilion I      **Time:** 8:00 am – 5:00 pm  
**Sponsor:** US Department of Energy, National SCADA Test Bed

This fast-paced, hands-on course is packed with information covering:

- General Security Observations and Pitfalls
- SCADA Network Communications Overview
- Potential SCADA Network Entry Points and Defenses
- SCADA Network Scanning and Vulnerability Identification (in a SAFE manner)
- Network Monitoring and Simple Intrusion Detection
- Dissecting SCADA Protocols
- Common Programming Pitfalls
- Modern Hardware and OS Mitigation Strategies
- Incident Response Essentials for the SCADA Community

This course is structured to help students not only understand exactly how attacks against SCADA systems could be launched and why they work, but also provides mitigation strategies to increase the cyber security posture of your control system network. Because it is hands-on, students get a deeper understanding of how the various tools work.

The hands-on character of this course requires that every student have a laptop computer they can configure and bring to the class. All students in this course should have already mastered networking fundamentals such as UDP vs TCP, MAC vs IP addresses, Layer 2 vs Layer 3 switches, and be comfortable with memory management and coding in C++, Java, or Assembly. In other words, it is a technical course. To be fair to the other students, we will not be able to slow this class to answer very basic questions, so if you are not comfortable with these topics, please take the Introductory SCADA Security Course where you will get much of the same material but without the technical details.

Accompanying this course is a sample SCADA network that will be used to demonstrate exploits used for unauthorized control of the SCADA system and mitigation solutions. This network will also be used during the course for the many hands-on exercises that will help you develop control system cyber security skills that you can apply when you return home.

### Red Team for Program Managers (RTPM)

**Room:** Fairway Pavilion IV      **Time:** 8:00 am – 12:00 noon  
**Sponsor:** US Department of Energy Office of Electricity Delivery and Energy Reliability (DOE/OE), National SCADA Test Bed

RTPM introduces program managers, analysts, and decision makers to a four-step approach designed to help focus effort, save time and energy, and avoid common difficulties in using adversary-based assessments. Red teaming or adversary-based assessment is a flexible tool that program managers use to understand threat and to deliver components and systems that achieve their mission in hostile environments. Red teaming methods apply across the full life-cycle from concept through retirement.

## Control System Wireless Security

**Room:** Fairway Pavilion IV      **Time:** 1:00 pm – 5:00 pm  
**Sponsor:** US Department of Energy, National SCADA Test Bed

Many misconceptions exist regarding wireless security. It is common to think that the control system is secure because they utilize licensed frequencies, deploy proprietary equipment, secure communication using encryption, or installed Yagi antennas. This course will show why these myths lead to insecure environment. In addition, hands-on activities with readily available tools will be used to educate asset owners on the tools and techniques available to adversaries, how to monitor and detect suspicious wireless communication, and how to secure wireless networks with a defense in depth approach. This course will address WiFi, Bluetooth, and SCADA Radio communication environments.

3:00 pm – 7:00 pm: Registration – Grande Ballroom Foyer

## TUESDAY – AUGUST 26

7:00 am – 7:45 am Continental Breakfast – Parterre Gardens

7:00 am – 5:00 pm Registration – Grande Ballroom Foyer

### PLENARY SESSION

**Room:** Salons A/B/C, Grande Ballroom

#### 8:00 am Welcome and Opening Remarks

**Presenters:** Michael Torppey, Manager, Noblis, Inc.  
 Governing Board

#### 8:30 am Keynote Address

**Presenter:** Phyllis A. Schneck, PhD, Vice President, Research Integration, Secure Computing Corporation and Chairman Emeritus, Board of Directors, InfraGard National Members Alliance

Networking Break – Grande Ballroom Foyer

#### 10:00 am Security Challenges Facing the Control Systems Environment *(Closed to the press)*

#### 11:15 am Should We Be Scared-a SCADA? *(Closed to the press)*

**Presenter:** Stephen Gill, Chief Scientist, Team Cymru

As a greater number of systems converge and interconnect over the Internet, the risks of increased outages and reduced reliability have never been so high. Technology has blurred the line between the physical and the electronic machine driving our infrastructure. The ones running our infrastructure may not be whom we expect, and the threat landscape is only getting worse.

Team Cymru will present some of their findings in a recent passive study done on the general use of SCADA traffic globally and some hard facts as to the state of the problem. They will suggest tactical and strategic ways to mitigate the risks associated with SCADA convergence, and staying ahead of the curve of what may some day become a monetized commodity in the miscreant underground economy.

#### 12:00 pm Lunch – Updates from the Energy Sector Roadmap and the Water Sector Roadmap

**Presenters:** David Edwards, CIO, Metropolitan Water District of Southern California  
 Seth Johnson, Chairperson, Water Sector Coordinating Council, Cyber Security Workgroup  
 David Norton, Program Manager-Transmission IT Security, Entergy

Mr. Edwards and Mr. Johnson will describe the strategy for implementing the “Roadmap to Secure Control Systems in the Water Sector” which was developed in 2007 – 2008 in accordance with the Department of Homeland Security’s (DHS) National Infrastructure Protection Plan (NIPP) partnership model by the Water Sector Coordinating Council’s (WSCC) Cyber Security Workgroup (CSWG). The Roadmap considers many variables for mitigating vulnerabilities and reducing risks to industrial control systems in the water sector.

Mr. Norton will discuss the Energy Sector Roadmap.

TUESDAY  
 AUGUST 26

### 1:15 pm **Industry Consequences and Mitigation**

**Presenter:** **Tim Roxey**, Technical Assistant to the Vice Chairman, Constellation Energy & Deputy Chairman, Nuclear Sector Coordinating Council

The Nuclear Sector has taken a proactive stance in the field of Cyber Security starting just before the Y2K roll over date. Over the next several years the Industry, working with NEI developed a program for Cyber Security for nuclear power plants and submitted this program to the NRC for endorsement.

Since those early efforts at developing the Program the Industry has completed two extensive sets of assessments. The first, covering Nuclear Significant systems, those deemed most essential to plant operations, were completed by May 1, 2007. The second covered all of the systems that could impact continuity of power and was completed this past May 1, 2008.

In June of 2007 the industry was made aware of a control system vulnerability and asked to implement a series of mitigation steps. One hundred percent of the nuclear power assets in the US completed mitigation within 60 days following the notifications.

This presentation explores how the vulnerability was presented to the sector, some of the mitigation work performed and some of the issues of vulnerability mitigation in general.

### 2:15 pm **Control System Cyber Incident Handling: A Law Enforcement Perspective Panel**

**Moderator:** **Mark Fabro**, President & Chief Security Scientist, Lofty Perch

**Panelists:** **Clint Baker**, Sergeant, Integrated Technological Crime Unit, Royal Canadian Mounted Police  
**Scot Huntsberry**, Supervisory Special Agent, Cyber Division/Computer Intrusion, Federal Bureau of Investigation  
**Jeff Morgan**, Process Control Systems Analyst, Cyber Division, Federal Bureau of Investigation

Over the last several years, the topic of cyber security for SCADA/Process Control Systems has been gaining considerable attention. With various intelligence agencies admitting that cyber attacks on infrastructure control systems have indeed been happening, initiatives have been tuned to accommodate for both incident response and forensics for SCADA and Process Control cyber incidents. As a key component to first responders, police and law enforcement cyber crime units have to prepare for incidents on SCADA and control systems.

This panel will provide some law enforcement insight into national and international perspectives on emerging issues regarding cyber incidents for critical infrastructure and control systems architectures. Issues such as incident response, forensics, public collaboration, as well as challenges and successes regarding how law enforcement is dealing with these very important issues will be discussed. This session will be a must-see for personnel who are tasked with critical infrastructure protection and cyber security for national assets and key resources.

3:15 pm *Networking Break – Grande Ballroom Foyer*

### 3:45 pm **Responsible Vulnerability Disclosure**

**Moderator:** **Zack Tudor**, Program Director, SRI International

**Panelists:** **Art Manion**, Internet Security Analyst, CERT Coordination Center  
**Yurie Ito**, Director of Technical Operation, JPCERT/Coordination Center  
**Bryan Singer**, Vice President of Security Services, Wurdtech™ Security Technologies  
**Al Rivero PE**, Director, Professional Services, Telvent  
**Ted Angevaare**, Global DACA Manager, Shell Global Solutions International BV, Global DACA Team Rijswijk, GSES  
**Kevin Sullivan**, Senior Security Strategist, Trustworthy Computing-Critical Infrastructure Protection, Microsoft  
**Ivan Arce**, Core Security Technologies

A responsible vulnerability management process for vulnerabilities related to control systems related serves a critical role in managing risk to our nation's critical infrastructure and key resources. This panel will include representatives from various types of process stakeholders including owners and operators, vendors, researchers, and government. The goal of the panel will be to address all stakeholders' perspectives in order to define a vulnerability management process, which appropriately and responsibly manages risk.

*Conclusion of the Plenary Session*

The following meetings are being co-located with the 2008 Industry Conference to provide maximum benefit for the control systems community and are open to all who wish to attend. You do not need to be registered for the 2008 Industry Conference to attend these events.

### ISA Security Compliance Institute (ISCI) – ISA SP99

**Room:** Salons D/E **Time:** 5:30 pm

Come join ISA and the ISA Security Compliance Institute (ISCI) for a Tuesday evening event where you will meet and get a better understanding of the current work underway within ISA SP99 and the ISCI. These two groups are working in-collaboration to provide not only a detailed set of Control Systems Standards but, as important, a clear set of compliance criteria for measuring, testing and validating Control system products, applications and vendor operating procedures. To ensure we are meeting the needed requirements, we need your guidance, please come and bring your questions, thoughts and most important your experiences...together we can make a difference.

### Water Sector Roadmap

**Room:** Scripps Ballroom I **Time:** 5:30 pm

### Lemnos Interoperable Security Project Birds of a Feather Meeting

**Room:** Scripps Ballroom II **Time:** 5:30 pm

## WEDNESDAY – AUGUST 27

7:00 am – 7:45 am Continental Breakfast – Parterre Gardens

7:00 am – 5:00 pm Registration – Grande Ballroom Foyer

### A Trusted Framework for Managing Compliance Evidence

**Solution Track:** Requirements/Operational Considerations

**Room:** Scripps Ballroom  
**Time:** 8:00 am – 9:00 am

**Presenter:** Jeff Kalibjian, HP Distinguished Technologist, HP Atalla Security Products, Hewlett Packard Corporation

Compliance evidence is very valuable information. It is not only information an auditor reviews to assess adherence to standards, but a detailed description of an organization's control system network, a unique view into business process and evidence that could clear an organization of wrongdoing should something go wrong. Consequently compliance evidence should be collected and managed with great care. This session will demonstrate how trust and accountability can be utilized in automated systems that can not only collect and manage compliance evidence but also provide a framework for external auditors to evaluate organizational compliance progress.

### Are You Compliant or Liable? Achieving Solid Cross-Standard Compliance

**Solution Track:** Understanding Risk

**Room:** Salons D/E  
**Time:** 8:00 am – 9:00 am

**Presenters:** Clint Bodungen, Founder/Principal Analyst, Critical Infrastructure Defense Group  
Chris Paul, Partner/Counsel, Joyce & Paul PLLC  
Jeff Whitney, Founder/Principal, Berkana Resources Corporation

With consistent communication issues lingering between traditional IT and control systems environments, along with the vast number of ambiguous security standards and guidelines available throughout the industry, asset owners and operators are challenged with becoming, or remaining, secure, and now at the same time, maintaining compliance. However, there is little absolution on exactly which standards to follow or which ones will be enforced. Even in more regulated industries such as Electric Utility, it is still uncertain whether or not you will actually end up maintaining security when it is all said and done due to the lack of technical and agreed upon guidance. Furthermore, many of the current standards and guidelines available only seem to address cyber-security issues more than anything, leaving physical attack vectors (which can also lead to control system cyber access) as well as legal issues by the wayside. In many cases, current industry accepted processes actually create liability.

This presentation will discuss a new approach to industrial security and compliance, which uses a cross-standard, holistic lifecycle model to address each of these issues thoroughly and cohesively, and helps minimize liability. Some of the concerning issues addressed are:

- Deciding which standards apply to you and eliminating gaps between them.
- Maintaining multi-standard compliance and solid security regardless of vague guidelines.
- How to become compliant with minimal change to your current processes and procedures.
- Establishing seamless due diligence to minimize incident liability and broad auditor interpretation.
- How to improve interdepartmental cohesion

WEDNESDAY  
AUGUST 27

## When Good Traffic Goes Bad: When is Application Traffic Too Much?

**Solution Track:** Architecture/Design

**Room:** Salon C  
**Time:** 8:00 am – 9:00 am

**Presenters:** **Kevin McGrath**, Scientist, ABB, Ltd.  
**Daniel Peck**, Offensive Security Researcher, Digital Bond, Inc.  
**Thomas Maufer**, Director, Technical Marketing, Mu Dynamics, Inc.

DoS is about much more than just intentional malicious attacks or simply overloading a link. When do ill effects set in? This presentation will illustrate DoS situations arising from both valid traffic (too much of a good thing!) or intentional attacks.

## Secure ICCP

**Solution Track:** Devices/Components

**Room:** Salons A/B  
**Time:** 8:00 am – 9:00 am

**Presenter:** **Ronald Lambert**, Lead Consultant, Integration Services, LiveData

ICCP/TASE2, Inter-Control Center Communications Protocol, is commonly used to exchange critical operations data between EMS/SCADA and other real time systems. ICCP is used over both LANs and WANs. In some cases, parts or all of the network paths are not secure or fully trustable. The original ICCP standard, now often referred to as insecure ICCP, does not provide secure communication or strong authentication. This leaves the data on those connections vulnerable. The new secure ICCP standard provides a solution.

Secure ICCP uses current SSL/TSL and X.509 certificate technology to secure ICCP data and provide strong authentication. The LiveData secure ICCP presentation will describe secure ICCP and the vulnerabilities it addresses.

## Vallourec & Mannesmann Tubes of Brasil: Business Systems and M&C Networks Segregation Project

**Solution Track:** Requirements/Operational Considerations

**Room:** Scripps Ballroom  
**Time:** 9:15 am – 10:15 am

**Presenter:** **Leandro Pflieger de Aguiar**, Computer Security Analyst/Network Specialist, Chemtech – A Siemens Company

Although the automation industry is often slow to adopt technological advances that appear in IT environments, with the development and popularization of Ethernet and TCP/IP and the strong adoption of these standards in M&C systems, the security needs also become essential to the industrial environment. One of the first steps towards creating a structure with secure and independent controls, able to meet the specific security requirements, is the segregation of the business systems and M&C environments, a recommended practice by ISA SP99.

This presentation aims to demonstrate the BUSINESS SYSTEMS AND M&C NETWORKS SEGREGATION project developed at V&M of Brazil between 2007 and 2008; the solutions adopted, the risks, the implementation difficulties and lessons learned during the implementation.

The presentation begins by showing the V&M M&C structure and managing models, highlighting historical problems that justified the project. After this, the technologies and practices that have been adopted to and in conjunction with the physical and logical separation of networks are described. The choices are related to recommendations from standards and security best practices. This section addresses topics such as used strategy for implementation of network elements and Firewall, implementation strategy for Active Directory authentication and authorization service, and weightings on automation systems needs for Information security technologies adoption.

The exposure continues with presentation of implementation methodology employed, especially planned to allow minimal interference over production processes. Finally, the main conclusions and obtained results in the project findings are highlighted with comments about important elements to consider by any interested parties on future similar implementation projects.

Project highlights:

- Highly Available new network model
- Network traffic characterization and firewall rules summarization
- Microsoft Active Directory: new Authentication and Authorization model
- Introduction of Server and Client Operating Systems Security Guidelines
- Antivirus and Operating System Updates
- Inventory and Documentation
- Running factory project: zero impact to production

## The Repository for Industrial Security Incidents (RISI)

### Solution Track: Understanding Risk

**Room:** Salons D/E  
**Time:** 9:15 am – 10:15 am

**Presenters:** **Eric Byres**, Chief Technology Officer, Byres Research Inc.  
**Mark Fabro**, President & Chief Security Scientist, Lofty Perch

One of the major challenges that control system professionals experience is obtaining accurate and up to date cyber security incident information on which to base risk analysis and financial decisions. The Repository for Industrial Security Incidents (RISI) provides a collection, analysis and reporting mechanism for cyber security events that impact industrial control and automation systems. This session will first present preliminary trends from the data collected to date. Next we will explain the process for submitting incidents to RISI system and the procedures and technology in place to carefully protect the identity of all submitters and their corporations. Options for obtaining incident analysis data will also be presented.

## Design Techniques for Deployment of a Policy Based Network

### Solution Track: Architecture/Design

**Room:** Salon C  
**Time:** 9:15 am – 10:15 am

**Presenter:** **Steve Hargis**, Director of Secure Networks, Enterasys Networks, Inc.

Industrial control systems have evolved significantly over the past several years with an increase in the use of Ethernet data communications networks and IP communications protocol. More and more critical infrastructure processes are being supported with underlying standards-based network communications technology. While the use of the standards-based Ethernet network has greatly increased the business and process interaction in industrial automation environments, there is also potential for increased security risks to critical infrastructure. It is imperative that clear and concise network security architecture be established as a foundational element to any network communications system involving the plant environment.

This presentation from Enterasys will explain how a networking architecture for process control can provide a highly manageable, scalable and adaptable communications infrastructure addressing the critical data and security concerns of the control systems environment. Leveraging a framework to establish, distribute and enforce access and network communications policies, process control environments are able to take advantage of modern data communications without sacrificing security.

## Secure Access Control for Control System Operations

### Solution Track: Devices/Components

**Room:** Salons A/B  
**Time:** 9:15 am – 10:15 am

**Presenter:** **Andrew Wright**, Chief Technology Officer, N-Dimension Solutions, Inc.

N-Dimension's Secure Access Control solution will provide uniform Authentication, Authorization, and Audit (AAA) controls across all aspects of a control system, including both IP-enabled and legacy equipment, at both control centers and remote field sites, and for local access, disconnected access, and remote access. Our solution adds several new capabilities to the N-Dimension N-Platform security appliance to provide the same AAA controls universally to every point of cyber access to the control system. The security appliances are deployed throughout the control system to mitigate access to control devices and networks, and synchronize with a central source of authentication and authorization information to ensure access control is up to date. Synchronization can be performed over both IP and dialup, and access control can be performed without a connection to the central source. In the future, we will be exploring multi-factor authentication, physical security integration, and access control agents for Windows-based control systems servers.

10:15 am *Networking Break – Grande Ballroom Foyer*

## Raising the Bar on Built-in Cyber Security

### Solution Track: Requirements/Operational Considerations

**Room:** Scripps Ballroom  
**Time:** 10:45 am – 11:45 am

**Presenters:** **Gary Finco**, Control System Cyber Security Researcher, Idaho National Laboratory  
**Robert McComber**, Product Security Specialist, Telvent  
**Larry Spoonmore**, IT Business Analyst, Southern Company Services  
**Rita Wells**, Energy Sector Lead, Idaho National Laboratory

The presenters will describe how the Department of Homeland Security Control Systems Security Program Procurement language document is being used to address control systems security and how asset owners are using this document in procurement of control systems.

WEDNESDAY  
AUGUST 27

## Control Systems Threat Awareness

**Solution Track: Understanding Risk**

**Room:** Salons D/E  
**Time:** 10:45 am – 11:45 am

**Presenters:** **Robert Huber**, Senior Cyber Security Researcher, Idaho National Laboratory  
**Sean McBride**, Cyber Security Researcher, Idaho National Laboratory

One of the primary tenets of security is to limit attacker knowledge. Researchers at the Idaho National Laboratory monitor the industrial control system threat environment to discern attacker interest, capability and opportunity. In this session the presenters will describe trends in vulnerability research and reporting applicable to control systems, give examples of events that demonstrate increasing attacker interest, capability and opportunity in control systems, and outline appropriate stakeholder responses.

## Protecting Safety Instrumented Systems from Cyber Attack

**Solution Track: Architecture/Design**

**Room:** Salon C  
**Time:** 10:45 am – 11:45 am

**Presenters:** **Eric Byres**, Chief Technology Officer, Byres Security Inc.  
**Kevin Staggs**, Engineering Fellow, Honeywell Process Solutions

Today there are many Safety Integrated Systems (SIS) that are interfaced to process control systems using either serial or Ethernet-based communications. This connection allows both systems to share information concerning the state of the process and provide better safety and operations management. However, it also introduces the possibility of security events (such as viruses or Denial of Service (DoS) attacks) migrating from one system to the other, especially in cases where personal computers are being used to program or manage either system. Addressing this risk requires a defense-in-depth solution, where a security firewall carefully monitors and controls all traffic, ensuring only appropriate control traffic is allowed to pass between systems.

This presentation describes how a petroleum refinery used the industrial firewall solution to provide secure communications between a Triconex™ Emergency Shutdown (ESD) system and a Honeywell Experion™ process control system. It also explains the use of the ISA-99 zone and conduit model for security design. A case history will discuss the use of firewalls in redundant networks, techniques for grouping large numbers of identical devices in “networks” and the management of nuisance alarms generated by unwanted multicast traffic.

## Security Beyond Standards

**Solution Track: Devices/Components**

**Room:** Salons A/B  
**Time:** 10:45 am – 11:45 am

**Presenter:** **Andrew Bartels**, Chief Technology Officer, Aegis Technologies, Inc.

This session will identify the most critical areas not addressed by security standards, the technologies/procedures necessary to secure them, and the potential impact of doing the minimum for compliance.

There is no silver bullet for securing a control system, but there are steps that can be taken to reduce the risk of a cyber event that could result in downtime and damage to critical infrastructure. The specific areas that we will look at are:

- Serial communications – while not covered in the CIPs, serial communication (or non-routable protocols) are still utilized by over 70 percent of the industry.
- Security framework – additional security measures such as encryption, key management, etc. are important steps to consider when implementing a security solution. With the industry moving towards IP communications, an entirely new set of vulnerabilities are encountered. According to the CVE list (common vulnerabilities and exposure), there are over 25,000 known IP network vulnerabilities. Solutions should address this trend and assist in a secure, seamless transition from a Serial network to IP.
- Next wave – AMI, Substation Automation. With the industry moving towards Automated Meter Infrastructure and Substation Automation, it is important to address security at the forefront of these waves.
- Additional areas outside of the reach of current security standards that should be addressed.

While this session will cover the gaps in current security standards, the focus will be on solutions to the problem. With the right procedures, methodologies, and technologies, utilities can prevent costly cyber events and proactively address areas that could very well be covered in the near future by the expansion of current standards.

11:45 am *Lunch – Parterre Gardens*

## Control System Self Assessment and the Water Sector Roadmap

### Solution Track: Understanding Risk

**Room:** Salons D/E  
**Time:** 12:45 pm – 2:15 pm

**Presenters:** **Candace Chan-Sands**, Program Manager, EMA, Inc.  
**Patrick Ellis**, IT Director/CISO, Broward County Water & Wastewater Services  
**Darren Hollifield**, Manager, Water Treatment & Control Systems, JEA

A control system self assessment tool set developed and specifically tested for use in the water and wastewater sector is available to assist asset owners in identifying cyber security vulnerabilities in their control system environment. The tool, known as the Control Systems Cyber Security Self-Assessment Tool (CS2SAT), was developed by the Department of Homeland Security Control Systems Security Program to assist control system users and vendors to assess the security of their systems against the database of categorized security requirements. This collaborative effort, between the Department of Homeland Security, US Environmental Protection Agency, Water Environment Research Foundation, the American Water Works Research Foundation, and Idaho National Laboratory collected the best available cyber security recommendations and guidance into a single database known as the Cyber Security Protection Framework.

The CS2SAT provides users with a systematic and repeatable approach for assessing the cyber security posture of their industrial control system networks. The CS2SAT is a desktop software tool which guides users through a step-by-step process to collect facility specific control system information and then makes appropriate recommendations for improving the system's cyber security posture. The tool pulls its recommendations from a database of the best available cyber security practices and standards, which have been adapted specifically for application to industry control system networks and components. Based on the user's cyber security configuration, the tool also identifies security gaps and appropriate requirements to meet the needed security assurance levels.

As the water sector implements its Cyber Security Roadmap, the CS2SAT will play an important tool in creating baseline information as well as for measuring improvements. The presentation will provide a summary of project activities, a demonstration of the tool, as well as a roll out plan.

## Unidirectional Connectivity – Novel Robust Method for Absolute Protection of Process Control Systems

### Solution Track: Architecture/Design

**Room:** Salon C  
**Time:** 12:45 pm – 2:15 pm

**Presenter:** **Avner Turniansky**, Director of Product Marketing, Waterfall Solutions, Ltd.

Process control systems obviously require protection, considering the assets they are part of. Their users require flexibility, ease of use and connectivity. Cyber hacking and data theft are the main dangers facing such systems and their users, and awareness to actual cyber-attacks which have already taken place is growing daily.

Existing network protection methods may be applied to protect process control systems and networks, such as a firewall or an intrusion detection system, but all have their limitations and shortcomings. A novel protection concept, unidirectional connectivity, is aimed at overcoming such limitations and is now being made available to system integrators, installers and users.

The unidirectional connectivity concept and its realization will be explained, showing its unique attributes and absolute security strength. Several relevant case-studies of unidirectional connectivity solutions, already operating in process control systems and in additional scenarios and architectures will be presented, aimed at giving the audience a wide view and full scope of the immense potential of employing unidirectional connectivity solutions for absolute security in process control systems and networks.

## AchillesINSIDE – Intelligent Cyber Security and Risk Management for Industrial Environment

### Solution Track: Understanding Risk

**Room:** Scripps Ballroom  
**Time:** 12:45 pm – 2:15 pm

**Presenters:** **Dr. Nate Kube**, Co-founder and Chief Technology Officer, Wurdtech™ Security Technologies  
**Bryan Singer**, Vice President of Security Services, Wurdtech™ Security Technologies

Currently, security solutions for control systems (SCADA, DCS, etc) are delivered through a small number of companies and disparate commercial products from vendors lacking crucial cyber-risk intelligence specific to industrial environments. The end result is a high degree of complexity, increased operational costs, limited visibility and reliance on incomplete data to make critical security decisions. For a majority of industrial organizations, the outcome is a sub-optimal security posture, inadequate demonstrations of regulatory compliance, and increased security management costs, which serve to promote security as a cost center as opposed to valued added service.

In our opinion, cyber security for ICS must focus on a system's resiliency to faults. Such resiliency is demonstrated by a system's ability to resist systematic failure (either intentional or non-intentional) while maintaining safe and constant control of a process, ensuring performance, quality, safety and (if appropriate) regulatory compliance.

*(continued next page)*

*(continued from previous page)*

Worldtech Security Technologies' Achilles product suite provides vendors, operators, system integrators, and service providers' unparalleled visibility into the reliability, safety and security of the systems and networks essential to the operation of the world's industrial infrastructure. AchillesINSIDE takes a step ahead empowering users to answer questions such as, How secure am I? Where should I focus my resources? and Am I taking appropriate measures to ensure the safety, and reliability of my operations. This session focuses on the AchillesINSIDE Security Model (metrics and analytics) along with real examples on how it may be employed and utilized. Key considerations and actionable conclusions from the collected resilience data will also be presented.

2:15 pm Networking Break – Grande Ballroom Foyer

## Meeting 24x7 Managed Cyber Security for a Process Control Network

**Solution Track: Requirements/Operational Considerations**

**Room:** Scripps Ballroom  
**Time:** 2:30 pm – 3:30 pm

**Presenters:** Clayton Coleman, Senior Consultant, Invensys Process Systems Global Consulting  
Kevin Nixon, Senior Director Americas, Integralis

Learn how Husky Energy is staying ahead of the security threat landscape – by addressing security risks before they become issues. Husky Energy will describe the unique challenges his organization was faced with and how Invensys augmented their available consulting services by leveraging a relationship with global managed security services provider, Integralis to provide a comprehensive suite of consulting, technology and managed services. We will walk through the process beginning with the security audit, recommendations, network design and implementation and finally the management of the new system. (Presentation prepared by Don Gilmore, Husky Energy)

## Supporting Risk Reduction Decisions Using Scenario-Based Modeling

**Solution Track: Understanding Risk**

**Room:** Salons D/E  
**Time:** 2:30 pm – 3:30 pm

**Presenter:** Mark Fabro, President & Chief Security Scientist, Lofty Perch

In order to effectively assess a Process Control Systems' (PCS) risk and reduce security concerns a more modern and robust approach to risk analysis is required. Using observed and measured vulnerabilities that have been collected during a tactical assessment, a scenario based activity can be used to help illustrate actual cyber incident consequences. This has been proven to provide exceptional focus for organizations looking to prioritize mitigation activities and provide more clarity in terms of self-assessment and security monitoring. PCS security discussions can quickly conjure up threats that are solely based on speculation and unidentifiable assumptions. To reduce confusion a scenario based threat model will create plausible and verifiable risk assessments that are both proactive and focused. This will empower stake holders with a deeper insight and a systematic way of identifying security risks.

## Secure Access to Industrial Automation and Control Systems (IACS)

**Solution Track: Architecture/Design**

**Room:** Salon C  
**Time:** 2:30 pm – 3:30 pm

**Presenters:** Paul Didier, Industrial Solutions Architect, Cisco  
Serhii Konovalov, Industrial Solutions Architect, Cisco  
Venkat Pothamsetty, Business Development Manager, Cisco

Remote access solution provides engineers or authorized contractors with the ability to get instant information or even tune parameters of an industrial automation and control system when they are out of the control room or other standard facility for such tasks. Also, it allows vendors to provide instant support, verify configuration and upgrade firmware, eliminating timely and costly visits to a physical site and responding immediately to emergencies. While visiting the site, employee can verify recent changes or notes in his or her assignment, identify the fault device by RFID and check its history or add new status records in the assets database. However, all of these should not be done without strict security in mind. Ability to verify identity of an authorized remote connection, limit access to only authorized systems or even subsystems, and finally, grant authorized access under the most secure control, mitigating risks of emerging viruses and worms – all of these are properties of "Secure Remote Access to Industrial Automation and Control Systems" solution. Technically, architecture of the solution combines virtualization, firewall technologies, virtual private networks and admission control.

## Intrusion Detection and Prevention Systems (IDPS) in the Industrial Automation and Control Systems Environment

### Solution Track: Requirements/Operational Considerations

**Room:** Scripps Ballroom  
**Time:** 3:30 pm – 4:30 pm

**Presenter:** Chris Martin, Senior Director Product Management, Industrial Defender, Inc.

This session will provide potential implementers or users of IDPS within the process control industry with an overview of IDPS technologies and implementation architectures. Various considerations will be explored that might prove useful during the analysis of IDPS technologies for use in the industrial automation and control systems environment, or at the boundary between industrial automation and control systems and business systems.

The implications discussed are categorized into three broad areas: planning considerations, implementation considerations and support considerations. Planning considerations such as the required organization for success, internal and supplier support considerations as well as implementation of a risk assessment are discussed. A comparison of host-based and network-based intrusion prevention systems will also be covered. Finally design considerations such as sensor placement will be suggested.

Implementation topics will include a discussion of how to perform a site survey as well as installation standards. These standards rely on using a baseline installation process which will be described in detail. Some important functions to support IDPS after implementation include best practice operations such as back-ups, testing and tuning. Also the procedure for getting regular signature updates to keep IDPS current and effective are covered. Next, event management technology, which IDPS usually feed into, is described as they are an integral part of a defense-in-depth strategy. The last topic to be discussed is the development of an incident response plan which is typically required for regulatory compliance.

## A Hybrid Virtualization Environment for Process Control System Security

### Solution Track: Understanding Risk

**Room:** Salons D/E  
**Time:** 3:30 pm – 4:30 pm

**Presenter:** David Kleidermacher, Chief Technology Officer, Green Hills Software, Inc.

General purpose operating systems and virtualization solutions such as Windows, Linux, and VMware are unsuitable for security assurance to the high levels required for protecting the computers and networks running critical control systems. We propose a hybrid operating environment that combines the utility of virtualization with the robustness of a high security real-time operating system that protects the control system and network from hostile and well-funded attackers while providing users with the familiar interfaces and applications available in legacy IT systems.

## Intuitive, Easy, and Secure Provisioning and Configuration of Industrial Sensor and Control Networks

### Solution Track: Devices/Components

**Room:** Salons A/B  
**Time:** 3:30 pm – 4:30 pm

**Presenter:** René Struik, Cryptographic Standards Specialist, Certicom Corporation

We present an intuitive, yet secure approach to provisioning and configuration of industrial sensor and control networks. The approach hides security details from the user, thus allowing ease of device and network setup and flexibility of trust lifecycle management, while doing away with security hassles that have plagued more conventional approaches.

The proposal uses public-key cryptography, a security technology that allows reduction of trust lifecycle management to the management of trusted device identities (via so-called certificates), and security policy enforcement techniques based on lifecycle management of device roles.

From a user's perspective, this results in a system where trusted lifecycle management appears to be the same as that of an unsecured network: it simply comes down to proper identification of devices (e.g., reading off a label of a physical module) and proper management of device roles (e.g., adding these to, resp. removing these from a white list, e.g., via a workstation GUI). No secret information is disclosed at any lifecycle stage of a device or a system, nor needs to be, since management relies completely on handling of public information. This greatly reduces the complexity of lifecycle management and, thereby, training requirements for operational personnel. Moreover, it virtually removes trust dependencies between different entities involved in the value chain, whether OEM, vendor, system integrator, installer, or user. Lastly, the approach has the benefit of allowing enforcement of standards compliance (by only issuing a certificate to devices from vendors that passed conformance testing).

The techniques will be exemplified using extensive deployment scenarios co-developed with and validated by end users in the ZigBee Alliance and ISA SP100 communities.

### Solution Provider Evening – Fairway Pavilion

4:30 pm – 8:30 pm  
 (see page 19 for details)

WEDNESDAY  
 AUGUST 27

## THURSDAY – AUGUST 28

7:00 am – 7:45 am Continental Breakfast – Parterre Gardens

7:00 am – 4:00 pm Registration – Grande Ballroom Foyer

### US Department of Energy (DOE) Public-Privately Funded Initiatives

**Room:** Scripps Ballroom  
**Time:** 8:00 am – 9:30 am

#### Bandolier: Auditing Control System Security Best Practice with the Nessus Vulnerability Scanner

**Presenter:** Jason Holcomb, Security Consultant and Researcher, Digital Bond, Inc.

Digital Bond will provide a description and demonstration of the DOE funded Bandolier project. Bandolier allows vendors to audit control system application configurations against a best security practice in a manner that has much less impact and risk to control system availability than traditional vulnerability scanning. The project leverages the policy compliance functionality in Nessus and will result in a security audit capability for at least twenty different control system applications.

Examples of the wide range of security settings that can be audited on Windows and UNIX systems will be provided. These include OS settings, common application settings, and control system specific application settings. After an explanation of the project and tool, a demonstration will show how to configure Nessus for use with the Bandolier audit files.

#### Hallmark Project: A DOE Co-Operative Project

**Presenters:** Mark Hadley, Cyber Security Research Scientist, Pacific Northwest National Laboratory  
Rhett Smith, GSEC, CISSP, Development Manager, Schweitzer Engineering Laboratories, Inc.

The Hallmark Project is a DOE Cooperative agreement involving Schweitzer Engineering Laboratories, Pacific Northwest National Laboratory, and CenterPoint Energy. This research and development project focuses on delivering an OEM FIPS 140-2 validated cryptographic card that can be used in products with serial communications. A bump-in-the-wire link module will also be developed that includes the cryptographic card allowing the Hallmark team to complete lab and field testing detailing the impact this technology has on control systems and the control system operators. These two reports will arm the industry with the technical details needed to understand what to expect when deploying this technology system wide and how to successfully deploy and maintain it.

#### The Lemnos Interoperable Security Project

**Presenters:** Darren Highfill, Utility Security Practice Lead, EnerNex Corporation  
David Teumim, Consultant, Teumim Technical, LLC

The Lemnos Interoperable Security Project is a two year government/industry R&D project sponsored by the Department of Energy's Office of Electricity Delivery and Energy Reliability Program. This project is designed to increase the availability and accessibility of cost-effective, interoperable security solutions for control systems with Internet Protocol (IP) based communications to utilities in the energy sector

At the PCSF session in 2007 for the OPSAID project (the predecessor to Lemnos), utility end-users overwhelmingly expressed preference for security solution interoperability. To this end, deliverables for 2008 involve defining the basic security functional units, building a reference implementation, a vendor implementation, and an interoperability test suite, while activities for 2009 include laboratory testing at TVA for the Lemnos reference and vendor implementation. Additionally an invitation to industry vendors to come and lab test interoperable solutions in 2009 at TVA, and then demonstrate interoperability with Lemnos implementations in a public venue, will be extended.

### Panel Session: State of Building Security In: Where Are We in That Process?

**Room:** Salons D/E  
**Time:** 8:00 am – 9:30 am

**Moderator:** David Norton, Program Manager-Transmission IT Security, Entergy

**Panelists:** Dr. Markus Braendle, ABB Corporate Research  
Penny Chen, Principal Systems Architect, Yokogawa IA Global Marketing Center (USMK)  
Robert McComber, Product Security Specialist, Project Manager-INL Testing, Telvent  
Jeff Potter, Security and IT Integration Manager, Emerson Process Management  
Ernest Rakaczky, Principal Security Consultant, Enterprise Architecture & Integration, Invensys Process Systems  
Paul M. Skare, Director, Security & Deployment, Siemens  
Kevin Staggs, Engineering Fellow, Honeywell

The Vendor Forum has been in existence for over two years and includes representatives from all of the major process control systems vendors. This panel of control systems vendors is a representative mix of the Vendor Forum where each panelist will have an opportunity to address the path their company is taking to build security into their products, outreach, and business approaches to accelerate the progress towards improving the security of control systems. This knowledge exchange will be designed to address questions and requirements from the user community and establish a new process by which the user community can communicate with the Vendor Forum on a continuous basis. Understandably information requests posed to a world class control systems vendor panel can be overwhelming with a wide variety of topic areas to cover. To refine the scope and make this exchange meaningful, valuable, and efficient for the asset owners and vendors we will open with a focus upon 'State of building security in, where are we at in that process?'

**Room:** Salon C, Grande Ballroom

**Time:** 8:00 am - 9:30 am

## Survivability and Recovery of Process Control Systems

**Presenter:** Ulf Lindqvist, Program Director, SRI International

The I3P is a collaborative R&D consortium that is implementing projects that will result in a new tool, a new concept, or a knowledge development report. Of the seven current projects in the PCS program, five of the projects are working on knowledge and tool development and two are researching knowledge and concept development:

### Knowledge and Tool Development

- 1) RiskMAP (MITRE) is used to identify corporate risks
- 2) DEADBOLT (MIT/LL) ensures that vendor supplied software has been rigorously tested for coding errors
- 3) SHARP (PNNL) provides an infrastructure-dependent, high-security drop-in appliance that limits access to sensitive data
- 4) APT (UIUC) helps ensure that PCS security policy is specified and implemented correctly
- 5) SecSS (Univ. of Tulsa) provides situational awareness and prevents misuses of Modbus

### Knowledge and Concept Development

- 6) The ROBUST concept (Sandia) helps plan for surviving through and responding to cyber disruption
- 7) Gap Analysis reports (USMA) document technology gaps and the Tech Transfer efforts (SRI) help in technology transition

## RiskMAP: Translating ICS Risk Assessments into Corporate Terms

*Sponsored by The Institute for Information Infrastructure Protection (I3P)*

**Presenter:** Jim Watters, Lead INFOSEC Engineer, The MITRE Corporation

The session will open by describing the twofold problem of (1) needing to identify and mitigate the risks facing ICS network nodes and (2) lacking the means to express these risks in terms meaningful to the corporate officers who hold the resources for risk mitigation. Following this is an explanation of RiskMAP and the way it addresses this need by uncovering dependencies between corporate business objectives, operational tasks, critical information assets and ICS network nodes. A live demonstration illustrates the use of RiskMAP to link risks facing a network node to risks facing key business objectives. The session will conclude with remarks by an end user with experience in using RiskMAP.

## The LOGIIC Consortium: A Sustainable Partnership

**Presenter:** Richard Jackson, Chief Information Protection Officer and General Manager of Global Information Risk Management, Chevron Corporation

The LOGIIC consortium (LOGIIC) is an ongoing collaboration of oil companies and the US Department of Homeland Security. LOGIIC was formed to facilitate cooperative research, development, test, and evaluation procedures to improve cyber security in the petroleum industry digital control systems. The consortium undertakes collaborative research and development projects to improve the level of cyber security in critical systems of interest to the oil and natural gas sector.

In a first project that was completed in 2006, the LOGIIC collaboration model was shown to be successful. The LOGIIC Correlation Project demonstrated an opportunity to reduce vulnerabilities of oil and gas process control environments by sensing, correlating and analyzing abnormal events to identify and prevent cyber security threats.

The LOGIIC Consortium now seeks to evaluate and improve the level of security of Safety Instrumented Systems (SIS) as these are increasingly integrated with process control systems. This is to be achieved by an evaluation process with results ultimately intended to support standards and certification, although these activities are outside of the scope of LOGIIC.

The LOGIIC SIS Project will result in security improvements to individual systems, characterization of residual risk, architectural recommendations to greatly increase the security of SIS/PCS integration, and confidence on the part of the sector that safety systems are verifiably secure. The LOGIIC effort will facilitate a robust and coordinated thought process involving vendors, end users, and experts in security and SIS applications, enabling improved architectures and future standards while decreasing duplication.

9:30 am Networking Break – Grande Ballroom Foyer

## Cyber Security Self Assessment Panel

**Room:** Scripps Ballroom  
**Time:** 10:00 am – 11:45 am

**Moderator:** Brian Isle, Chief of Operations, Adventium Labs

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

This panel will examine the need for improved methods and tools in two critical control system cyber self assessment areas: staff training and risk analysis. The panelists will review the state of the practice today and their view of the future, based on their extensive experiences and history of direct involvement. We will then open the discussion to the audience. The session goals are to validate the need for improved methods and tools, discuss what steps should be taken, and who should have responsibility for the improvements. This session builds on the efforts of the SCADA Cyber Self Assessment Working Group, which in 2005 began its effort to analyze self assessment requirements vs. existing tools and methods. The group concluded that these two requirements areas were the highest priority gaps. The session will begin with an overview of the working groups methods and results. (Note that the working group's written outputs have been provided on the memory device available to all conference participants.)

**Room:** Salons D/E, Grande Ballroom  
**Time:** 10:00 am – 11:45 am

## Cyber-Security Issues in Wireless Systems for Critical Infrastructure Protection

**Presenter:** Teja Kuruganti, R&D Staff Member, Modeling and Simulation Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory

There are several wireless technologies that are currently in use at the critical infrastructure facilities. The applications range from data acquisition and/or control extending from long-range links like cell phones, microwave links (several hundred kilometers) to short range wireless sensors (several meters). It appears that a problem, identified at critical infrastructure protection (CIP) sites, occurs at the nexus of regulatory constraints, legal implications, technological options, and corporate policy. NERC CIP-005 standard (issued by the North American Electric Reliability Corporation) defines the requirements in the electric power industry for identifying and securing the electronic security perimeter (ESP) within which all the cyber assets reside. The interpretation and subsequent implementation of that standard has uncovered potential conflicts with corporate policies. The CIP standards that are in place do not comprehensively address the new modes of vulnerabilities introduced by wireless devices.

This presentation will draw on an analysis done (with an end-user) over CIP 005 to provide secure implementation guidelines in the context of wireless networks. The presentation will introduce the existing and emerging standards in wireless for industrial automation. The presentation will further discuss the new modes of vulnerabilities in next generation control systems operating over discrete communication networks. An open source tool developed at ORNL will be introduced with a case study in power systems operation and control.

## Monitoring and Situational Awareness in PCS

**Presenter:** Al Valdes, Senior Computer Scientist, SRI International

Digital controls such as Supervisory Control and Data Acquisition (SCADA) systems have been universally adopted in the energy sector, and infrastructure systems such as electric power generation and distribution, oil and gas (O&G) refining, and pipelines are critically dependent on such controls. Adoption of standard protocols and platforms has increased functionality but has also potentially rendered infrastructure systems vulnerable to remote cyber attacks. The situation is exacerbated because, for a variety of reasons, control systems tend to lag behind corporate systems in security posture.

The DATES (Detection and Analysis of Threats to the Energy Sector) project seeks to address this challenge by developing a control-system-specific monitoring, event correlation, and threat information sharing capability. Our project will develop and demonstrate an effective, integrated monitoring control system solution with applicability in both electric power and oil and gas to complement perimeter defenses in such systems.

DATES is an R&D project exploring ubiquitous monitoring and situational awareness in Process Control Systems. In particular, we are developing model based and adaptive approaches exploiting regularity of protocols and communication patterns in PCS to provide a workable anomaly detection capability and potentially protect against zero-day exploits. This complements signature and misuse.

## Industrial Network Design Panel

**Room:** Salon C  
**Time:** 10:00 am – 11:45 am

**Moderator:** Craig Schiro, I&C/Secure Networks, Exxon-Mobil

**Panelists:** Eric C. Cosman, Engineering IT Consultant, The Dow Chemical Company  
 Steve Hargis, Director of Secure Networks™, Enterasys Networks, Inc.  
 Shawn Kirk, Cisco  
 Raphael Pereira, Security Officer, Chemtech – A Siemens Company  
 Steve Venema, The Boeing Company  
 Jules Vos, Program Manager, Shell Global Solutions BV

The 2008 Industry Conference program is stacked with a number of presentations from top Network Design solution providers and includes various levels of guidance and practical application techniques applied to theory, architecture, security, implementation and next generation designs. With the abundance of knowledge present the Industrial Network Design Panel will provide an opportunity for a deep dive into the technical details while offering a venue for sharing individual user requirements, opinions and recommendations. The panelists include a diverse group who will present and discuss various architecture layouts and the requirements that drive these designs while providing ample time to address the audiences top design objectives.

11:45 am Lunch – Parterre Gardens

## WORKING GROUPS

### Responsible Vulnerability Disclosure Working Group

**Room:** Scripps Ballroom  
**Time:** 1:00 pm – 2:15 pm

**Moderator:** Zach Tudor, Program Director, SRI International

A responsible vulnerability management process for vulnerabilities related to control systems related serves a critical role in managing risk to our nation's critical infrastructure and key resources. This panel will include representatives from various types of process stakeholders including owners and operators, vendors, researchers, and government. The goal of the panel will be to address all stakeholders' perspectives in order to define a vulnerability management process, which appropriately and responsibly manages risk.

### Education & Training Working Group

**Room:** Salons D/E  
**Time:** 1:00 pm – 2:15 pm

**Moderator:** Marty Edwards, Industry Liaison Lead, Idaho National Laboratory

This session is designed to attract interested participants in training to an informal roundtable to discuss the future direction and strategy for training needs in the control systems environment. Opinions, comments, ideas, requirements, interests are welcome from all participants including those who conduct the training, are planning on building training programs, attending future training classes, or are just interested in ensuring that sufficient training material is available to impact a large portion of the population who can improve the security of industrial control system environments. The Industry Conference provided several training courses prior to the start of the meeting and with a number of professionals from government-sponsored programs in attendance that are responsible for conducting and designing the training. The output from this discussion will be used by interested training stakeholders and posted to the Industry Conference website as a product for those interested in learning more about the training needs for the control systems security community.

### Metrics Working Group

#### Technical Metrics for Control System Cyber Security

**Room:** Salon C  
**Time:** 1:00 pm – 2:15 pm

**Presenter:** Wayne F. Boyer, PhD, Advisory Engineer/Scientist, Idaho National Laboratory

The session will describe a recommended framework for cyber security technical metrics and recent case studies, The Department of Homeland Security Control Systems Security Program supported development of a control system cyber security framework and a set of technical metrics to aid owner-operators in tracking control systems security. The framework defines seven relevant cyber security dimensions and provides the foundation for thinking about control system security. Based on the developed security framework, a set of ten technical metrics are recommended that allow control systems owner-operators to track improvements or degradations in their individual control systems security posture. A brief discussion of the metric support tool will also be provided with a focus on soliciting suggestions and user needs from the audience.

## Security Requirements Working Group

Room: Salons A/B  
Time: 1:00 pm – 2:15 pm

Presenters: Robert Evans, Engineer, Idaho National Laboratory  
David Teumim, Consultant, Teumim Technical, LLC

*The Catalog of Control Systems Security: Recommendations for Standards Developers* (Catalog) was developed by the DHS CSSP to assist organizations in the development and implementation of control system cyber security standards. This session provides an overview of the Catalog and an example of how the Catalog has been used by the Transportation sector in the development of a recommended practice for securing public transportation from cyber intrusions.

2:15 pm Networking Break – Grande Ballroom Foyer

## CLOSING PLENARY

Room: Salons A/B/C, Grande Ballroom  
Time: 2:45 pm – 4:30 pm

### Brief Updates

Working Group Report-outs  
Panel Report-outs  
Water Sector Roadmap  
PCS Forum Brasil

### Closing Comments

Conclusion of the 2008 Industry Conference

# Local Flavor

 Jazz at Croce's Restaurant and Jazz Bar (corner of 5th & F, downtown San Diego)

San Diego Padres vs Arizona Diamondbacks @ Petco Park 



Rockabilly or Blues at Henry's Pub (618 - 5th Avenue, San Diego)

A play at The Old Globe Theatre (Balboa Park, San Diego)



Relaxation at Spa Tiki (200 Harbor Drive, Suite 200, San Diego)

*You are cordially invited...*

## **SOLUTION PROVIDER EVENING**

August 27  
4:30 pm – 8:30 pm  
Fairway Pavilion

Certicom Corporation

Department of Homeland Security  
National Cyber Security Division  
Control Systems Security Program

Electric Power Research Institute (EPRI)

Enterasys Networks, Inc.

Industrial Defender, Inc.

Invensys Process Systems

The Institute for Information  
Infrastructure Protection (I3P)

MTL Instruments/Byres Security Inc.

On-Ramp Wireless, Inc.

Schweitzer Engineering Laboratories

Secure Computing

Waterfall Solutions, Ltd.

**A special Solution Provider Evening & Social Networking Event  
will allow attendees one-on-one time with  
Solution Providers**





## *Solution Providers*

### **Byres Security Inc.**

Byres Security Inc. develops industrial security technologies for critical infrastructure companies in the oil and gas, power, chemical and manufacturing sectors. Its sister company, Byres Research Inc. is a consulting and services company providing security guidance to government security agencies, major oil companies and power utilities on cyber protection for critical infrastructures and industrial processes.

### **Certicom Corporation**

Certicom manages and protects the value of content, applications and devices with government-approved security. Adopted by the National Security Agency (NSA) for government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the global leader in ECC, Certicom's security offerings are currently licensed to hundreds of multinational technology companies, including IBM, General Dynamics, Motorola, Oracle and Research In Motion. Founded in 1985, Certicom's corporate offices are in Mississauga, Ontario, Canada with worldwide sales and marketing headquarters in Reston, Virginia and offices in Europe and Asia. Visit [www.certicom.com](http://www.certicom.com)

### **Control Systems Security Program (CSSP), National Cyber Security Division, Department of Homeland Security**

The mission of the Control Systems Security Program (CSSP) is to strengthen the control system security posture by coordinating across government, private sector, and international organizations to reduce the risk. The CSSP objectives include building a culture of reliability, security and resilience, demonstrating value, addressing cross sector security interdependencies, and providing thought leadership.

### **Electric Power Research Institute (EPRI)**

The Electric Power Research Institute, Inc. (EPRI, [www.epri.com](http://www.epri.com)) conducts research and development for the global electricity sector. An independent, nonprofit organization, EPRI brings together experts from academia and industry as well as its own scientists and engineers to help address challenges in electricity generation, delivery and use, including health, safety and the environment. EPRI also provides technology, policy, and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent more than 90 percent of the electricity generated and delivered in the United States, and international participation extends to 40 countries. EPRI's principal offices and laboratories are located in Palo Alto, CA; Charlotte, NC; Knoxville, TN; and Lenox, MA.

### **Enterasys Networks, Inc.**

Enterasys Networks understands that industrial control systems have evolved over the years with a dramatic increase in the use of Ethernet networks and IP communications. While this transition has greatly enhanced business and process interaction, there are increased security risks to critical infrastructure. An Enterasys Secure Network offers a unique approach providing a highly manageable, scalable and adaptive network architecture that addresses the critical data communications needs and the security concerns of the process control environment.

### **Industrial Defender, Inc.**

Industrial Defender, Inc., the global leader in Cyber Risk Protection™, is the first company to offer a comprehensive cyber security solution designed to protect the real-time process control/SCADA environment. This comprehensive Cyber Risk Protection™ solution enables the efficient assessment, mitigation and management of cyber security risk for critical infrastructure industries.

### **The Institute for Information Infrastructure Protection (I3P)**

The Institute for Information Infrastructure Protection (I3P) is a national consortium of leading academic institutions, federally-funded labs, and non-profit organizations dedicated to strengthening the cyber infrastructure of the United States.

# Solution Providers

## Invensys Process Systems (IPS)

Invensys Process Systems (IPS), headquartered in Plano, Texas, is a global technology, software and consulting firm leading significant change in process manufacturing, plant optimization, business operations and enterprise performance. IPS clients are some of the world's most important industrial organizations — companies that operate large oil refineries; plants that process chemicals, gas, LNG, power, pharmaceutical and minerals; and pulp and paper mills. IPS solutions, used at over 50,000 locations across the globe, include field devices and controls from Foxboro and Triconex, advanced applications from SimSci-Esscor, operations management from Avantix, and the world's first truly open enterprise control system, InFusion™.

The company's nearly 7,000 employees integrate these capabilities to create solutions that impact and increase efficiency, boost productivity, and accelerate performance. These results help industrial companies run safer, operate more efficiently, and extract useful knowledge from their operations to make faster, better decisions. To learn more about IPS visit [www.ips.invensys.com](http://www.ips.invensys.com).

The Invensys Group ([www.invensys.com](http://www.invensys.com)) is headquartered in London and is listed on the London Stock Exchange (ISYS.L), with approximately 25,000 employees working in 60 countries.

## MTL Instruments

MTL Instruments, a part of Cooper Crouse-Hinds, is a world leader in the development and supply of electronic instrumentation and protection equipment for the process control and telecommunications industries. Many of the world's most critical processes are monitored, controlled or protected by MTL equipment and the Group is distinguished by the quality and reliability of its products, its global network of sales-and-support centres and its acknowledged position as a thought-leader in this high technology marketplace. With 36 dedicated sales centres in 13 countries and a further 137 MTL representatives in 64 countries, MTL's expertise in Intrinsic Safety, Industrial Networks, Surge Protection and Operator Displays/HMI is unsurpassed.

## On-Ramp Wireless, Inc.

On-Ramp Wireless Inc. is a San Diego based systems provider for low-power wide area scalable sensor networking and location tracking. The Company's revolutionary Ultra-Link Processing™ ("ULP") technology solves the main barriers to wide-scale deployments of wireless sensor networks and location tracking in challenging environments. On-Ramp's ULP can achieve a receive sensitivity of -145dBm which provides a 25x advantage in terms of range (2,000 miles free space; 12 floors indoors) and capacity (scalable up to 10,000 nodes) over competing free spectrum & cellular protocols enabling broad adoption of wireless sensors. Initial target applications are Industrial Sensor Networking, AMR/AMI, Building Control, Remote Monitoring, and Energy Management using the free 2.4 GHz and 900 MHz ISM bands. On-Ramp's hardware has successfully been tested at over an 11 mile range in the 2.4GHz Free ISM band while preserving low power operation with product availability later this year.

## Schweitzer Engineering Laboratories

SEL designs and manufactures complete solutions for the protection, monitoring, control, automation, metering, and communications security of electric power systems. Our dedication to research and product development, combined with our practical experience in power system protection, results in advanced, cost-effective products. SEL has unique and sophisticated model power system testing services to validate customer settings and protection practices.

## Secure Computing

Secure Computing® is a leading provider of enterprise security solutions. Powered by TrustedSource™ technology, our award-winning solutions proactively protect our customers' mission-critical business applications from all manner of Internet-borne threats. Our comprehensive portfolio of Secure Web, Secure Mail, and Secure Firewall solutions provide unmatched protection for the enterprise. We are proud to be the security solutions provider to many of the most mission-critical and sensitive environments in the world.

## Waterfall Solutions, Ltd.

Waterfall Solutions Ltd. delivers secure unidirectional connectivity for process control and SCADA systems, segregated networks, remotely monitored networks and systems and IP surveillance infrastructures, based on patent pending technologies. The hardware-based solution provides a physical strictly one-way connection and a proprietary communication protocol, to transfer data between a transmitter and a receiver through a single fiber optic cable. It is immune to on-line attacks and the risks of data leakage. Waterfall was initially developed in 2004 to meet the needs of the Israeli Ministry of Defense and has been deployed in many homeland security and critical national infrastructure organizations, as well as a large variety of financial and enterprise customers.





# *Solution Provider Evening*

## *Floor Plan*

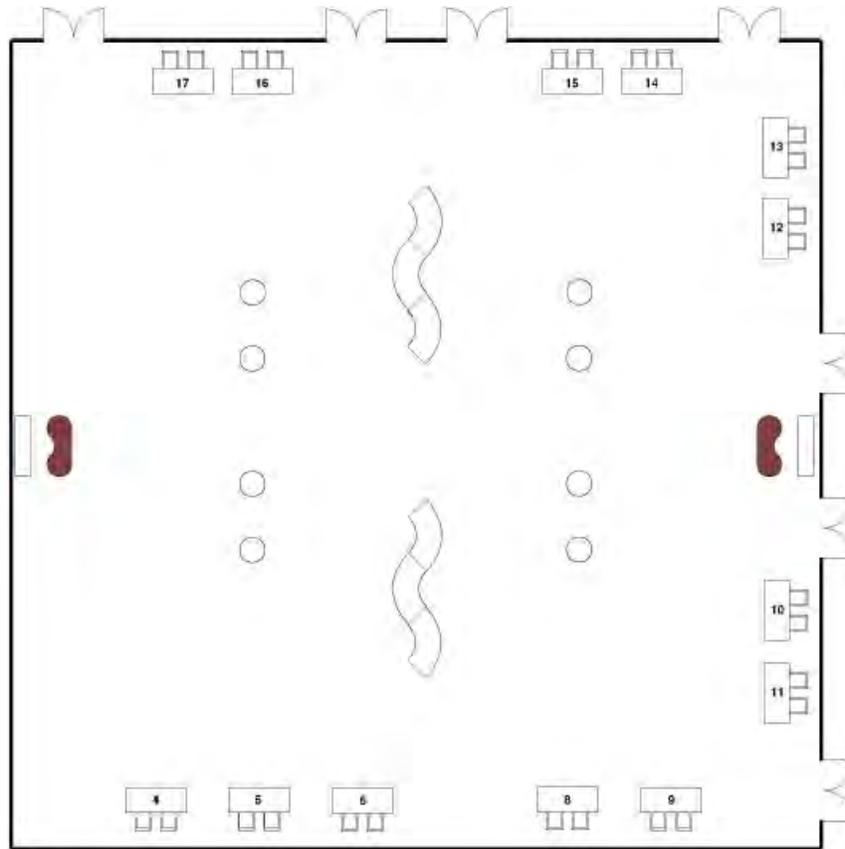
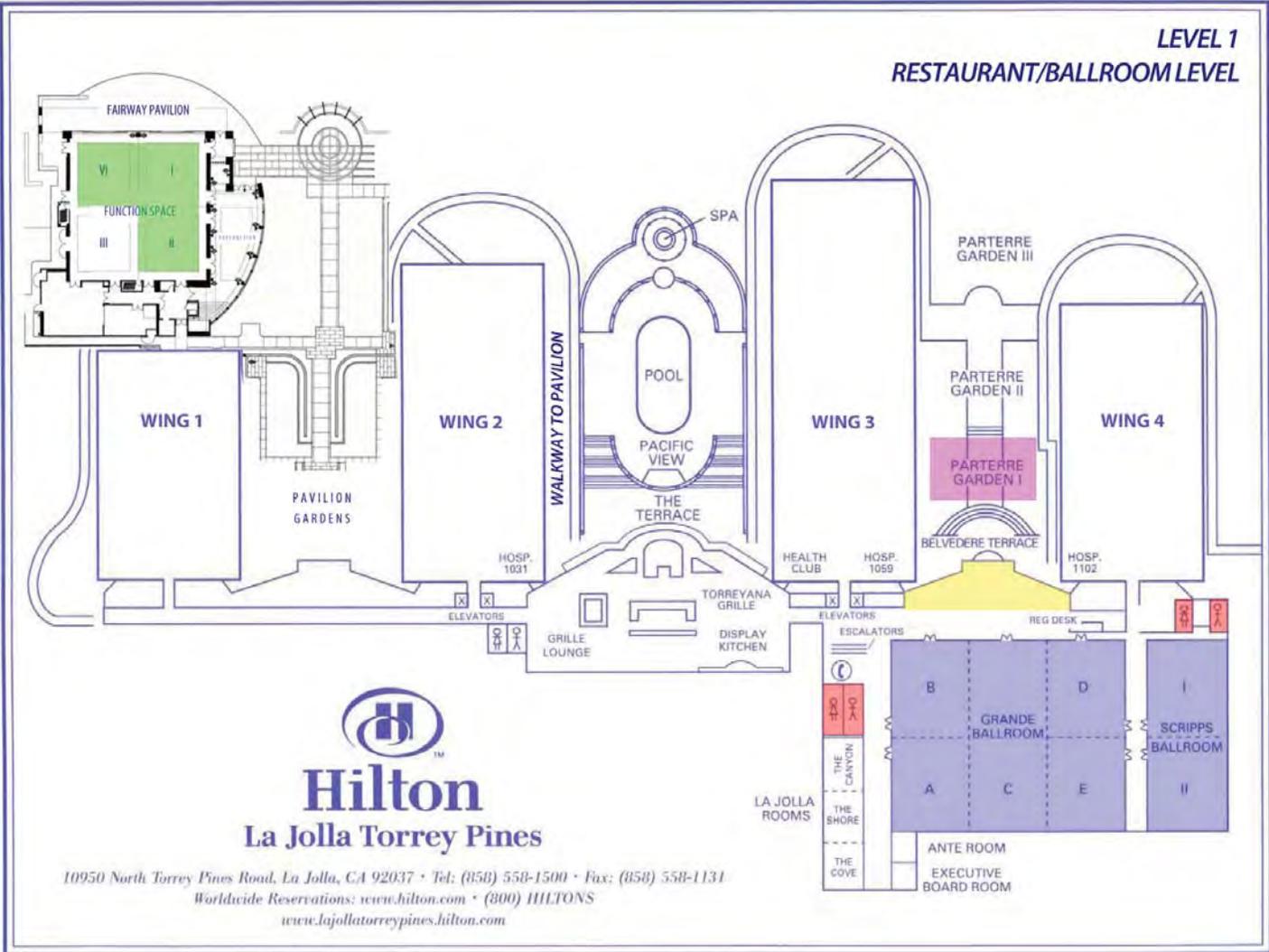


Table 4	Schweitzer Engineering Laboratories
Table 5	Waterfall Solutions, Ltd.
Table 6	On-Ramp Wireless, Inc.
Table 8	Secure Computing
Table 9	Electric Power Research Institute (EPRI)
Tables 10 & 11	The Institute for Information Infrastructure Protection (I3P)
Table 12	Control Systems Security Program, US DHS
Table 13	Invensys Process Systems
Table 14	Industrial Defender, Inc.
Table 15	Enterasys Networks, Inc.
Table 16	Certicom Corporation
Table 17	MTL Instruments/Byres Security Inc.

# *Notes*



**LEVEL 1  
RESTAURANT/BALLROOM LEVEL**



**KEY**

-  *Registration & Networking Breaks*
-  *Continental Breakfast & Lunch*
-  *Restrooms*
-  *Meetings Rooms*
-  *Training Sessions & Solution Provider Evening*



**Process Control Systems  
Industry Conference**

3150 Fairview Park Drive South, MS F310  
 Falls Church VA 22042  
[www.pcsforum.org](http://www.pcsforum.org)