

ISA Industrial Network Security Symposium
ISA Expo 2004 - October 4th, 5th, 6th and 7th, 2004
Houston, TX

Houston Industrial Network Security Activities – Overview

This Symposium provides the attendee with the latest practical, immediately applicable, information on security threats to manufacturing and control systems. In addition, it examines the synergies and applications of this information to the transportation and physical security domains. Leading experts from a wide range of industries, government (technology, regulatory, and research), academia, and manufacturing, control and security systems manufacturers will present the latest research and data on the threat; how it is changing and becoming more dangerous, what regulations and standards require now and where they are headed, and the steps end users, manufacturers, architect engineers, and constructors must take to reduce risks to acceptable levels. The attendee will learn how to justify expenditures in this critical area, how to cost effectively integrate these activities with other essential reliability, productivity, and control enhancements, and what technology, programs, and procedures are needed to harden their manufacturing and control systems to meet security challenges that are occurring more frequently and with more significant impacts.

ISA has published over 160 pages of guidance in the ISA Standards and Practices Manufacturing and Control Systems Security Committee's Technical Reports TR99.00.01 and TR99.00.02. The scope of these technical reports, and the work being done by SP99 takes the widest practical view of "manufacturing and control systems", including discrete and continuous processes, and all critical infrastructure industries that employ real time automation systems. This Symposium extends beyond that work, providing detailed information and training on how to apply the guidance to a wide variety of systems. In addition, expert users from major international companies will discuss what additional technologies and programs are needed from the manufacturers and how we can make security solutions more cost effective as we integrate into our routine design and operation activities.

Beyond the industries typically covered by past symposia and conferences, this symposium will include sessions covering the specifics of transportation automation systems security, and the opportunities to integrate physical security systems, automation upgrades, and the manufacturing and control systems network security that has been our focus in prior conferences.

Those interested and involved in this area should plan to attend the symposium, and the concurrent meetings of ISA SP99 working groups and the full SP99 committee; you will help to build the information presented in these sessions into additional practical guidance and standards which can be used by all stakeholders to improve the security of their manufacturing and control systems in the most cost effective manner.

THIS PROGRAM OUTLINE CONTAINS THE LATEST SUMMARY OF SESSION, AUTHOR AND STANDARDS MEETINGS, AND SOME ROOM NUMBERS - MAKE SURE TO CHECK THE ROOM NUMBERS LISTED HEREIN ONCE YOU ARE ON SITE – THINGS CHANGE!!

ISA Industrial Network Security Symposium
ISA Expo 2004 - October 4th, 5th, 6th and 7th, 2004
Houston, TX

Training, Papers, Panel discussions, Tutorial sessions, standards committee meetings planned for this conference include:

Monday, October 4 –

IC31C: Securing Industrial Networks: Cyber Protection for Automation, Control and SCADA Systems – A one day course in industrial networking from the security viewpoint – this course will be presented by its developer, Eric Byres, of British Columbia Institute of Technology. Eric is a leader in the research on manufacturing and control systems security threats and solutions, and has extensive experience in industrial networking. His extensive technical knowledge and outstanding presentation skills make this course a highly effective and enjoyable way to learn what must be done to secure your networks, both new and legacy systems.

Tuesday, October 5 – SP 99 Working Group 3 Meeting (8:00 AM – 5:30 PM)
SP-99 Part 1 – Models, Definitions, and Terminology (WG 3) – Reliant Center, Room 503/504

A lot of work has happened within this group in the past few months to generate ISA SP-99 Part 1 (DRAFT) of the standard. This will be a planning and content development session to drive towards completing this first part of the standard.

Tuesday, October 5 – Morning - 10:00 AM – 11:30 AM

Track 1 – Cyber Threats to your Automation Systems – Why worry? What to worry about? (P¹) – Session 122 – Session Developer – Eric Byres

Process control systems, with their reliance on proprietary networks and hardware, have long been considered immune to the network attacks that have wrecked so much havoc on corporate information systems. Unfortunately, new research indicates this complacency is misplaced – the move to open standards such as Ethernet, TCP/IP and web technologies has let hackers take advantage of the process industries ignorance. And the nature of the threat is changing. This session provides specific information on the changing nature of the threat, and a general overview of how one can deal with the threat. It sets the stage for detailed discussions on standards, regulations, government and academic work in this area,

¹ P – Paper, PL – Panel, T – Tutorial

ISA Industrial Network Security Symposium
ISA Expo 2004 - October 4th, 5th, 6th and 7th, 2004
Houston, TX

what the leaders of industry are doing today, and what they want from hardware and software vendors, to help them to further reduce the risks from cyber attacks.

- Understanding Security Vulnerabilities in SCADA Protocols – Eric Byres, BCIT
- Is Your Plant Vulnerable to Cyber-Attack? - Fabio Souza Terezinho, Product Manager at InduSoft, Austin, Texas
- Soft' Industrial Security - Donovan Tindill, Network Solutions Manager at Matrikon Inc., Edmonton, Canada

Track 2 – How to make sense of a “forest” of advice, and address the issues responsibly (P&T) – Session 123 – Session Developer – Eric Cosman

In the past two years, the security of manufacturing systems has moved from obscure to topical. Virtually all of the process industry sectors have activities underway to address this topic, and public awareness and interest has increased in response to media coverage and government activity. Those charged with addressing electronic security in their manufacturing operations are faced with a confusing list of groups, activities and initiatives. It is often difficult to determine where to go for the best guidance and direction, or how the various activities may be related.

- Hitchhiker's Guide to Cybersecurity Guidance - Eric Cosman, CIDX
- Control System Security - Understanding and Use of Current Skills and Technologies - Ernest Rakaczky, Invensys Process Systems, Canada, P236
- Automation Systems Security Reference Architectures - Darrin Miller, Technical Leader at Cisco Systems, San Jose, CA

Tuesday, October 5 – Luncheon Forum – 11:45 AM – 1:15 PM

Automation Systems – An Achilles’ Heel to our Critical Infrastructure ?? – Forum Leader – Eric Byres

Can cyber attackers impact our critical infrastructures such as power water and transportation? Eric Byres will lead with a summary of new information on the changing nature of the threat automation systems face. This will be followed by government representatives, who will tell us what they are doing about the threat, and how that integrates with other government and private sector activities.

Finally, audience can ask the panel on their perspective on what is needed from the government and other organizations.

Tuesday, October 5 – Afternoon - 2:00 PM – 3:30 PM

Track 1 – Security Standards – Those available today and future direction (P&PL) – Session 124 – Session Developer – Bryan Singer

- Standards and Regulation Overview – SP99, IEEE, ANSI, other

ISA Industrial Network Security Symposium
ISA Expo 2004 - October 4th, 5th, 6th and 7th, 2004
Houston, TX

- Power Industry Experience and Potential Impacts of the Draft NERC Cyber Security Standard on Power Plant Control Systems - Joe Weiss, KEMA, Inc, Cupertino, CA, P52
- Standard and guidance - similarities among different recommendations – Dick Oyen, ABB
- Panel Discussion on Standards

Tuesday, October 5 –Afternoon 3:45 PM – 5:15 PM

Track 1 – Manufacturing and Control Systems Security – Government Directions – Research, Regulation, and Requirements (PL) – Session 125 – Session Developer – Joe Weiss

Control system cyber security has been identified as an important need for critical infrastructure protection. Consequently, domestic and international governments and national laboratories are establishing programs and facilities to address control system cyber security. Substantial funding is being made available for these efforts. This session will include presentations by the US Department of Homeland Security (DHS), the US Department of Energy's (DOE's) Idaho, Pacific Northwest, and Sandia National Laboratories, the UK's National Infrastructure Security Coordinating Centre, and a status of selected international activities.

Track 2 – Performing a Risk Assessment (T) – Session 126 – Session Developer – Tom Good

This tutorial session will use a hypothetical chemical facility as a base, and walk through preparation of a risk assessment that will form the basis and justification for automation systems security enhancements.

Tuesday, October 5 – SP 99 Working Group 3 Meeting (8:00 AM – 5:30 PM)



Wednesday, October 6 – SP 99 Working Group 2 (Security Programs) meeting – 8:00 AM – 12:15 PM – Reliant Center, Room 503/504

Working Group 2 will be discussing the transition of ISA 99.00.02 (TR 2) into the second part of the ISA SP-99 Standard.

Wednesday, October 6 – Morning 10:00 – 11:30 AM

Track 1 – Users Define the Requirements for Manufacturers (P & PL) – Session 127 – Session Developer – John E. Allen

Detailed review of major users needs - Organized around types of technologies that are useful in establishing or improving automation systems security, this detailed discussion on users needs is more than a

ISA Industrial Network Security Symposium
ISA Expo 2004 - October 4th, 5th, 6th and 7th, 2004
Houston, TX

panel discussion. It provides specific, detailed advice from major industry users, on what they need from automation system and component vendors to make their jobs more effective – both from a technological and cost viewpoint.

- Authentication and Authorization Technologies – role based, password, challenge/response, physical/token, smart cards, biometrics, location based, device to device, and password management and distribution
- Filtering Blocking and Access Control Technologies – firewalls, VLANs, etc.
 - A SCADA-Aware Distributed Firewall - Eric J. Byres, John Karsch, Joel Carter, Darren Lissimore and Khai Lee Group for Advanced Information Technology, BCIT
- Encryption – symmetric key encryption, public key encryption and key distribution, private key signatures and digital certificates, and VPNs
 - Understanding TKIP; the Latest Ethernet Security - Jim Weikert, Locus, Incorporated, Madison, WI, P093
 - Cyber security tools for SCADA, John T. Tengdin, OPUS Publishing, San Clemente, CA, P136

Track 2 – Physical Security Systems – Exploring Their Interface with Secure Control Systems (PL) – Session 128 – Session Developer – Chuck Landis

Physical security systems in the manufacturing plant environment are rapidly evolving and becoming networked, including IP-based video cameras and access control devices, and also connecting in with corporate IT networks., Physical security devices are even being used within the traditional control system perimeter, for example - video cameras to monitor conditions inside a chemical reactor. This session will explore the interface between physical security systems and process control systems. Speakers will explore the following issues, among others.

Panel Speakers

Andy Acquarulo	IFS/GE
Erwin Icyan	Advanced Control & Engineering Solutions, Inc.
Rick Gross	Honeywell/Vindicator Security Solutions
Chuck Landis	Landis & Associates

Wednesday, October 6 – SP 99 Working Group 1 (Technologies) meeting – 1:00 PM – 5:15 PM – Reliant Center, Room 503/504

We will be discussing TR 1 and plans for the next revisions of this document. We expect to lay out additional sections and security technologies, as well as discussing inclusion of current Manufacturing and Control Systems security issues into this TR 1.

ISA Industrial Network Security Symposium
ISA Expo 2004 - October 4th, 5th, 6th and 7th, 2004
Houston, TX

Wednesday, October 6 –Afternoon 2:00 PM – 3:30 PM

Track 1 – Users Define the Requirements for Manufacturers – Part II (A continuation of the AM session, with discussions centering on these additional technology groups – (P & PL) – Session 129 – Session Developer – John E. Allen

Detailed review of major users needs - Organized around types of technologies that are useful in establishing or improving automation systems security, this detailed discussion on users needs is more than a panel discussion. It provides specific, detailed advice from major industry users, on what they need from automation system and component vendors to make their jobs more effective – both from a technological and cost viewpoint.

- Audit, Measurement, Monitoring, and Detection Tools – log auditing, malicious code and virus detection, intrusion detection, network vulnerability scanners, network forensics and analysis tools, host configuration management tools, automated software management tools
 - Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks - Author: Dale Peterson, Digital Bond, Inc., Sunrise, FL -- P 070
- Computer software – server and workstation operating systems, real time embedded operating systems, web and internet technologies
 - Better OS coordination – Richard Eisenach, Chevron Phillips Chemical Co., LP
 - OPC Security: Controlling Access to Critical System Data – Sean Leonard, Matrikon
- Physical Security Controls – physical protection, personnel security

Track 2 – Security for Transportation Control Systems (P) – Session 130 – Session Developer – Fred Woolsey, LTK Engineering

This session will continue the momentum generated at ISA’s July 14 and 15th Control and Transportation Security Conference in Philadelphia, which is the first ISA conference session exploring the interface between ISA’s manufacturing and control systems security activities and railway security.

- Physical and Cyber Threats Facing Rail Systems Mike Goldsmith, NWTC Inc, Fla.
- Sandia National Labs Programs in Rail Security Speaker TBA, Sandia National Labs, N.M.

Wednesday, October 6 –Afternoon – 3:45 – 5:15 PM

Track 1 – New Technologies for Manufacturing and Control System Security (P) - Session 131 – Session Developer – Tom Phinney, Honeywell

- Improving Survivability Of Complex Networks Safeguarding SCADA Systems: The Safeguard Project - Sandro Bologna, ENEA - The Italian National Agency for New Technology, Energy and the Environment, Rome, Italy P209

ISA Industrial Network Security Symposium
ISA Expo 2004 - October 4th, 5th, 6th and 7th, 2004
Houston, TX

- Steganography (abstract 2)
- Human Factors In Industrial Cyber Security - Paul Baybutt, Primatech Inc, Columbus, OH

**Track 2 – Session 132 – Electronic Security for Railway Systems (PL), -
Session Developer – Susan Howard, LTK Engineering**

This session will be a natural follow-on to the earlier Security for Transportation Control Systems session, and will look at specific security technologies applied within the transportation sector. Speakers will cover:

- Cybersecurity Considerations at Houston Metro Michael Lay, Houston Metro, TX
- Cryptographic applications to secure railway networks Peter Kofod, ARINC, Inc, N.C.

Thursday, October 7th - SP99 – Manufacturing and Control Systems Security – Full Committee Meeting 8:00 AM – 12:15 PM –Reliant Center, Room 204/205

The Agenda for this full committee meeting includes:

- General committee business (leadership announcements, votes, etc.)
- Quick update from each Working Group
- Discussion on the ISA-99 plan and proposed architecture for the standard – this will be a very important session as we will be discussing the future layout of the standard
- Guest Speakers – Dave Teumim is working on several guest speakers from government and industry groups to talk about security and importance of the ISA SP-99 activities.

Thursday, October 7th – Morning 8:30 AM – 9:45 AM

Keynote - Biometric Technology: Prime Time!

This keynote describes the growing role of Biometrics, as a key element of physical security

Thursday, October 7th – Morning 10:00 AM – 11:30 AM

Track 1 – Session 138 – Additional Technologies for Manufacturing and Control System Security (P&T) – Session 138 – Session Developer – Chuck Landis

This session will continue the discussion of new directions for security, and provide a tutorial on considerations and approaches for the use of wireless and fiber optics mediums.

ISA Industrial Network Security Symposium
ISA Expo 2004 - October 4th, 5th, 6th and 7th, 2004
Houston, TX

- Wireless Communications and Fiber Optics – Chuck Landis
- Linux Based RF Smart Card for Biometrics Security - Suhas Anandrao Desai of Walcand College Of Engineering, India

**Thursday, October 7th – 11:45 AM – 1:15 PM - Luncheon Forum -
Sensors & Wireless in Homeland Security**

Whether we want to admit it or not, it's on our minds nearly all of the time. It's Homeland Security - that simple phrase that essentially encompasses all aspects of the "prevent and protect" mantra seen on the sides of police cars. With so much national attention turned to this hydra, and the push for advanced technology to assist in the endeavor, the role of technology, specifically advanced sensors and wireless communications arises. It is within that context that this discussion is set, be it RFID-based asset tracking or integrated chem/bio/rad nanosensors with wireless telemetry or providing the information backbone for operations-level decision making. Initial presentations will be given by senior level executives representing the Dept. of Homeland Security, the National Institutes for Science and Technology, the hotel, travel and leisure industry, and an industrial perspective aimed at presenting the up-to-the-minute technical challenges and probable sensing, control, and security applications. A panel of experts will then discuss various perspectives on the governmental and commercial implications.

- Panel Moderator: Dr. Peter Fuhr, RAE Systems
- The panelists include: Dr. Kang Lee, NIST Dr. David Bolka, DHS-HSARPA Mr. David Shepherd, Exec. Dir of Security, The Venetian Hotel and Casino Dr. Jose Guterrez, Eaton Corp. Mr. Ian McPherson, Wireless Data Research Group Mr. Stephen Lambright, Vice President of Marketing, Savi Corp.