In this Issue
- Director’s Message
- Spotlight on a Members Paper
- Honors & Awards
- 61st International Instrumentation Symposium Report
- Scholarship Awards
- New Members

Upcoming Events
Nov 9-12 Process Control & Safety Symposium
Houston Marriott Westchase, Houston, TX

DIRECTOR
Edward Naranjo
Emerson Process Management
952-204-6270
Edward.Naranjo@Emerson.com

DIRECTOR-ELECT & SYMPOSIUM CONTACT
Sohail Iftikhar
Honeywell Process Solutions
713-376-0143
sohair.iftikhar@honeywell.com

PAST DIRECTOR, HONORS & AWARDS AND PROCESS CONTROL & SAFETY
GENERAL CHAIR
Fateh (T.J.) Tajani
UniversalPegasus International
713-354-6522
fateh.ali.tajani@universalpegasus.com

SECRETARY
Michael Hilton
Dynamic Controls & Sensors
281-812-9844
mike@precisionvalves.net

MARKETING CHAIR
Ardis Bartle
Apex Measurement
713-446-1902
ardisbartle@earthlink.com

WEBMASTER
Sandeep Kumar Raju Vysyaraju
Searles Valley Minerals
760-372-2435
vysarya@ostateemail.okstate.edu

STAFF LIAISON
Rodney Jones
919-990-9418
rjones@isa.org

NEWSLETTER EDITOR
Rick Williams
Siemens
281-435-0475
rwill74018@aol.com

ASSISTANT NEWSLETTER EDITOR
Mary Carmichael
Texas Steam & Instrumentation
713-464-9055
mcarmichael@steamsolutions.com

SCHOLARSHIP ADMINISTRATOR
Murtaza Gandhi
Baker Engineering & Risk Consultants
281 822-3100
MGandhi@BakerRisk.com

SECTION-DIVISION LIAISON
Nikesh Regmi
Burns & McDonnell
816-333-9400 x6154
nregmi@burnsmcd.com

DIVISION PAPER REVIEW CHAIR
Otto Friedrich
otto_friedrich@mail.utexas.edu

PROCESS CONTROL & SAFETY SYMPOSIUM
TECHNICAL PROGRAM CHAIRMAN
Kash Behdinan
PLC Plus International
661-654-7196
kbehdinan@bkppi.com

FACILITATOR
Ken Belteau
Spectra Energy
713-627-4467
kbelteau@spectraenergy.com
Process measurement and control have played a critical role on improving efficiencies in the process industries. It seems only fitting then that the ISA Process Measurement and Control Division (PMCD) organizes events that foster collaboration among industrial instrumentation professionals and serve as a forum for disseminating technological advancements. Below are some of the activities PMCD has carried out over the last year to provide education and training and improve technical competency among its members:

60th International Instrumentation Symposium
The 60th IIS was hosted by the Test & Measurement Division in London, UK, during the week of June 24 to 26, 2014. Ardis Bartle served as PMCD exhibits chair and Kash Behdinan served as PMCD papers chair. The 60th IIS was organized jointly with the Institution of Engineering and Technology (IET) and proved a successful event in a country with long industrial instrumentation tradition.

2014 Process Control & Safety Symposium
The first Process Control & Safety Symposium illustrated the power of collaboration across divisions. Aside from PMCD, Safety & Security, Communications, Education, Chemical & Petroleum, and Pulp & Paper Industry Divisions participated in the event. Fateh (T.J.) Tajani served as the symposium’s general chairman, while Ardis Bartle and Kash Behdinan volunteered as PMCD exhibits and technical papers chair respectively.

61st International Instrumentation Symposium
The 61st IIS was sponsored by the PMCD and jointly developed with the Machinery Failure Prevention Technology (MFPT) Society. The event was held on May 12 to 14 at the Westin Hotel in Huntsville, Alabama. Kash Behdinan was symposium general chair and Edward Naranjo served as PMCD papers chair.

PMCD Scholarship Program
The scholarship program provides funds to college students with outstanding qualifications and who express interest in pursuing the industrial instrumentation profession. Several scholarships were awarded in 2014-2015 as Scholarship Administrator Murtaza Gandhi reports in this newsletter. Requirements for nominating scholarship candidates and selecting recipients are published in the PMCD website.

Succession Plan: I will continue to serve as PMCD director until December 31, 2015. Sohail Iftikhar has been selected by the ISA Automation and Technology Department to become division director in 2016.

Newsletter: Rick Williams and Mary Carmichael are serving as newsletter editor and assistant editor respectively. Newsletters are available in electronic format at the ISA PMCD website. As in past years, the division will notify the PMCD membership when the newsletter is available for download. Please review your ISA profile in isa.org to ensure your email address is current.

Nominations and Honors & Awards
Past director T.J. Tajani chairs the nominations and honors & awards committees.

Leader Training: Division leaders attended the Spring Leaders Meeting at the Marriott City Center in Raleigh, North Carolina, from June 13 to 16, 2015.

With several activities ahead, including the organization of the 2015 Process Control & Safety Symposium, this is an opportune time to volunteer on the PMCD board. If you are searching for involvement to further your own profession, gain insights into instrumentation and control, and establish stronger bonds with your peers, you need look no further. Please call or write me; I would be thrilled to discuss volunteer opportunities with you.

Yours sincerely,

Edward Naranjo
Director, PMCD
Cross-Domain Cybersecurity for Industrial Control Systems

By Robert E. Lindeman
Aerospace Testing Alliance

KEYWORDS: cyber security, cross domain solution, defense in depth

INTRODUCTION
Meeting cybersecurity requirements for industrial control systems is a real challenge for automation engineers. As part of a Defense in Depth approach, the automation engineer must rely on multiple tools and procedures. The Department of Defense has been dealing with similar issues for many years and has led the development of a category of devices known as cross domain solutions (CDSs). Designed to meet national security needs and allow interoperability between differing security domains and even between different nations, these devices offer the commercial world another tool in its arsenal to securely and safely interconnect business and control networks in order to more efficiently control and manage key processes while protecting the integrity of the systems. This paper provides an overview of the technologies available and their application as part of a cybersecurity solution for industrial control systems.

THE PROBLEM
We are bombarded daily with news of actual and potential cyberattacks on control systems used to support key infrastructure processes associated with water, power, manufacturing, and transportation systems. The need to tightly integrate business and control processes only serves to highlight the risks and consequences of cyberattacks. The typical business system is tasked with day-to-day operations relying heavily on back-office systems that must interface to the Internet to support decision-making critical for peak performance. Real-time data from the various manufacturing and process control systems play a key role in providing the timely and accurate information managers require. Doing so requires information sharing between the business and control networks while protecting both from cyberattacks.

Murray McKay, Principal Application Engineer, Siemens Industry, Inc. (Ref 1) provides an excellent summary of the challenges with control systems:

- Control systems are usually optimized for system availability, not security. Product trends in the last decade have been toward easier and more open network access, reducing historical “air gap” security.
- Control sensors and actuators frequently have no security features at all, but will supply their information and take commands from any device that correctly addresses them and communicates with the correct protocol.
- Field control devices (PLCs, motion controllers, DCS nodes, RTUs, etc.) usually have some security features such as passwords, but these features are underutilized.
- HMI devices must have control capability over field control devices in order to be useful. Most HMIs can be remotely modified to allow control engineers to modify their programs. These features can be disabled, but usually are not.
- HMI and field control device communications are seldom encrypted.
- SCADA systems use commercial-off-the-shelf (COTS) computers and operating systems, so they inherit the vulnerabilities of these systems.
- PCs functioning as elements of a control system frequently do not have their software regularly updated to close security vulnerabilities. This is because changing the software to close security holes often changes the behavior of the system, causing the control system to malfunction. However, this also makes them more vulnerable to cyberattacks.
- Some older control system software is incompatible with security software such as virus scanners.
- Control systems are usually connected to plant operations networks for MIS/MES data acquisition.
- Control systems are frequently connected to the Internet for remote access and troubleshooting.
- Control system PCs are often used for office functions such as email access. This makes them vulnerable to phishing attacks.
• Programming terminals frequently have administrative privileges with detailed knowledge of the control system and are not kept updated with the latest security patches.

James Lyne, global head of security research for Sophos, the biggest European-based computer security firm (Ref 2) states: “Industrial Control Systems (ICS) are typically 10 years or more behind the mainstream in terms of security. Over the next couple of years we anticipate more serious flaws exposed and used by attackers as opportunities vacillate between state-sponsored attacks and financially motivated ones. In short, it is an area of significant risk.”

Figure 1 provides a realistic representation of the complexities of a typical system. Vulnerabilities abound from the external world via the internet. Linkage to business systems exposes the control system to a variety of risks. Internal security weaknesses inherent within the control system itself compound the issue. And one should not forget the single biggest risk – people. Disgruntled employees out for revenge, improperly trained operators taking incorrect action, overworked staffs making mistakes – the list goes on and on.

Figure 1: Overview of Cyber Vulnerabilities (Ref 3)

So what do we do? ISA/IEC-62443 Security for Industrial Automation and Control Systems (IACS) (Reference 4) and NIST 800-82 Industrial Control System (ICS) Security (Reference 5) provide excellent answers. It is clear that the best approach to meeting these demands is the Defense in Depth methodology. A combination of enforced and monitored policies and procedures; physical, network, and application security practices; computer and device hardening; and training and awareness are required to provide what is needed to reduce the risks to systems.

Firewalls and air gaps are typically used in an attempt to protect control systems. The use of firewalls from multiple vendors is recommended in IEC 62443 and is good practice. Firewalls play an important role in a Defense in Depth design, but they are not fool proof. They can be wrongly configured and are susceptible to being bypassed.

Air gaps are another story. Besides the fact that they impede the real-time sharing of information, they simply do not work.

Eric Byre (Ref 6) states: “For effective ICS and SCADA security, the entire industry needs to move past the myth of air gaps and learn to deal with the reality: control systems are connected to the outside world – they may not be directly connected to the outside world, but they are certainly connected to networks that are. You can cut the network connection, but the bits and bytes will still move to and from the control system. Cyber security countermeasures must face up to this fact.”

Austin Scott (Ref 7) says it this way: “If you believe in the so called control system "Air Gap" then I have a unicorn farm run by leprechauns I would love to sell you.”

This paper addresses a class of devices known as cross domain solutions. A cross domain solution (CDS) is a form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains (Reference 8).

As shown in Table 1, these devices address several of the vulnerabilities in control systems. These were developed to meet Department of Defense requirements to interface networks of different security levels while maintaining the integrity of and protecting classified information. Their use in a commercial industrial environment is examined as a potential tool for automation engineers in connecting business systems to industrial control systems.

CDSs are available for unidirectional or bidirectional applications.

Table 1: Vulnerabilities & Mitigations for Control Systems (Ref 1)

<table>
<thead>
<tr>
<th>Venerabilities/Attacks</th>
<th>CDS (Data Diode)</th>
<th>Software Updates</th>
<th>Physical Access Control</th>
<th>Social Engineering</th>
<th>Security Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Storage modification</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Memory modification</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Overloading</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Data encryption</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Host-based authentication</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Role-based authorization</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Data encryption</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Virus scanners</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Firewalls</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Whitelisting</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Network intrusion detection</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Phishing</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Social engineering</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
<tr>
<td>Physical access control</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
<td>❑</td>
</tr>
</tbody>
</table>

CROSS-DOMAIN SOLUTIONS
Unidirectional CDSs, commonly referred to as data diodes, provide one-way communications between two networks. Analogous in function to diodes in electronics circuits, they allow data to be sent in one direction only from the process control systems to the business system, providing real-time information. This gives the business network access to valuable process information helpful in financial, quality, performance monitoring, maintenance, and operational decision making. Since no information can flow to the process systems, cyberthreats experienced by business systems are prevented from reaching the process systems.

Implementations of data diodes range from hardware-only solutions to more sophisticated combinations of hardware and software.

Hardware-only data diodes consist of a fiber optic interface with the send and receive transceivers physically removed for one direction. Since this configuration contains no decision logic, software, or firmware, the risk of cyberattack or of being configured incorrectly is nil. The downside of this is that TCP/IP communications are not supported over a hardware data diode, and there is no way for the process system to ensure that a successful data transfer occurred. Furthermore, hardware data diodes do not prevent viruses from reaching business systems.

A more comprehensive data diode system includes proxy servers and specialized software. These additions allow for virus protection, TCP/IP communications implementation, improved data integrity, error detection and correction, security auditing, event logging, and administration.

Multiple vendors offer data diodes, including Nexor, GeNUGate, Fox, Owl Technologies, Vado, BAE Systems, Waterfall, and Minerva.

For applications requiring information flow between process systems and business systems, bidirectional CDSs are required. These devices allow managed communication between process and business networks by actively controlling the information flow between them.

While the internal workings of these types of systems are proprietary and vary between different suppliers, a typical bidirectional CDS consists of specialized IP servers to interface to the process network and the business network, a dedicated computer using a trusted operating system different from the operating systems used in the process and business systems, and user-configurable software to perform the secure receipt and transmission of selected data. RISC processors, Linux operating systems, single-board, or single-chip IP servers and sophisticated software packaged in hardened, tamper-resistant housings provide compact solutions.

Functions provided include the following:

- Content filtering
- Security policy rules set
- Tamper resistance
- IP interface
- Log and audit capability
- Data flow validation – ensures the content is well-structured and contains user-defined good values only
- Operates automatically at power-up with no user interaction required
- All network configurations, filters and rule sets are completely configurable
- Source and destination address authentication
- Source and destination address and data format whitelisting
- Security label checks against source and destination clearances
• Data format consistency and validity checking
• Scanning data for known malware
• Validation of digital signatures
• Inspection of encrypted content
• Checking text against a blacklist of phrases
• Removal of redundant data
• Generation of logs recording security relevant events
• Self-test mechanisms

Suppliers of bidirectional solutions include General Dynamics, Rockwell Collins, Raytheon, Lockheed Martin, Embvue, Advatech Pacific, MdeX, and DRS Defense Solutions.

CONCLUSION
Cybersecurity is one of many concerns today’s automation engineers must address. While no “one size fits all” magic solutions exist, employing a Defense in Depth strategy that includes technologies, procedures, training, diligence, awareness, and vigilance can provide systems that support and enhance business and production targets while offering reduced risk and increased protection to automation systems from cyberattacks. The use of CDSs is worth consideration in any cyberattack defense design.

REFERENCES
3. ICS-CERT website,
5. NIST 800-82, Industrial Control System Security.
61st ISA International Instrumentation Symposium Delivers 120 Technical Sessions, Attracts Dozens of Industry Experts
Research Triangle Park, NC (21 May 2015)—The 61st Annual ISA International Instrumentation Symposium (IIS), jointly developed with the Machinery Failure Prevention Technology (MFPT) Society, was held at the Westin Hotel in Huntsville, Alabama, USA.

The event is jointly sponsored by ISA’s Aerospace Industries, Test Measurement and Process Measurement and Controls Divisions, and is recognized globally as a forum for discussion of new and innovative instrumentation techniques, developments, and applications.

200 attendees, 90 industry experts and 18 exhibitor companies enjoyed more than 120 technical paper presentations, keynote addresses, panel discussions, networking receptions, a cutting-edge exhibit, technical tours, tutorials and an ISA training course on industrial wireless technology.

The theme of the conference was “Technology Evolution: Sensors to Systems for Failure Prevention.” The 61st IIS Symposium provided a remarkable opportunity for ISA Divisions and authors to expand their professional networks and learn about innovative instrumentation techniques.

Few forums offer this level of variety of topics and focus on current and pressing problems in industrial instrumentation. This was the instrumentation, prognostics, health management and automation event to attend in 2015 as leaders from ISA joined forces with MFPT to bring attendees seven tracks on health management and engineering,” said IIS General Chair Kash Behdinan, PhD., PMP.

Technical sessions, developed by ISA and MFPT, focused on key instrumentation challenges and developments across multiple industries. Topics covered included diagnostics, health management practices, control system instrumentation, communications and networks, process measurement and control applications, cybersecurity, signal analysis, condition based maintenance, process safety, test and measurement, failure analysis and prevention, fault detection and more. Tutorials covered key challenges and hot topics such as systems engineering, envelope analysis, generating business case analyses for implementing health management capabilities and, on the softer side, maintaining balance while managing a successful career.

Keynote addresses were delivered on Thursday, 12 May, after a welcome from ISA and MFPT leadership. The first keynote, titled “Bringing Back the ’70s: Simplifying IC Manufacturing Problem Resolutions with Machine Learning,” was given by Ben Eynon, Senior Director of Engineering Development at Samsung Austin Semiconductor.

Next, Joshua Kennedy, Associate Director of Sustainment Analysis for the U.S. Army Aviation and Missile Command, presented a dynamic address focused on “Managing and Implementing the Biggest CBM Program in the World,” covering trials, tribulations, and lessons learned.

The keynote sessions continued with Professor Dale Carl Teeters, Chair of the Department of Chemistry and Biochemistry at The University of Tulsa. Professor Teeters’ keynote, titled “Nanotechnology for Improvement and Control of Power Systems,” detailed the latest research and development work in this important area of study.

Finally, Dr. William Kyle Simmons, Principal Investigator at the Laureate Institute for Brain Research, delivered a fascinating theory-based discussion on “Using Human Brain Imaging to Map the Neurocircuity Underlying Food Motivation.”

In addition to the keynotes, tutorials and technical sessions, attendees enjoyed several receptions and networking events, including an awards presentation for each Society, throughout the conference.

“ISA is pleased to offer attendees and exhibiting companies an interesting, broad conference program that focused on their specific challenges and opportunities,” commented ISA Executive Director and CEO Patrick Gouhin

2015 PMCD Scholarship Recipients

We wish to congratulate the following recipients of the 2015 PMCD scholarships. These recipients represent a wide spectrum of students with affinity for industrial automation and engagement in the International Society of Automation.

Through its scholarship program, PMCD contributes over $10,000 toward student education and the fostering of the industrial automation profession.

*Mojdeh Jabari was awarded the Hugh Wilson Honor Scholarship*

*Gaurav Singh was awarded the Jere Haney Honor Scholarship.

Congratulations to all the award recipients!

1. Pranjal Bhadti
2. Lakshy Bhandari
3. Yogesh Gajjar
4. Mojdeh Jabari
5. Shin Jong
6. Elham Naghoosi
7. Dhrushant Patel
8. Khushaal Popli
9. Nandini Ramu
10. Adhish Raval
11. Shama Tajani
12. Nima Sammaknejad
13. Shaheeda Shahin
14. Gaurav Singh
15. Upendra Singh
16. Nirja Thakkar
17. Hasan Tinwala
18. Sandeep Vysyaraju

2014 Outstanding Member of the Year

BakerRisk Project Engineer & PMCD Scholarship Administrator Murtaza Gandhi is PMCD’s 2014 member of the year. Murtaza has been instrumental in the development and administration of the division’s scholarship program, a program he has led for over five years.

Since the program’s beginnings, he has helped raise awareness of the need to supply scholarships as a means to foster the society’s goals, inviting students to apply and speaking about the program at ISA Houston section and PMCD events.

In addition, Murtaza was an avid contributor at the division’s first Process Control and Division Symposium, where he served as chairman of the instrumentation and controls sessions, led a tutorial on practical types on the application of fault three analysis for SIL selection, and presented the paper “Performance Based Fire and Gas System Design.”

Murtaza’s dedication to the society and the division hasn’t waned over the years. Indeed, it seems Murtaza is intent on improving his contribution. Congratulations, Murtaza!
Pictures from the last year
Reach hundreds of experienced process control and automation end-users in the Houston area and across the gulf coast region when you exhibit at the ISA Process Control and Safety Symposium. With content brought to you by the ISA Process Measurement and Control Division and the ISA Safety and Security Division, this rich program also gleans content from several other ISA Technical Divisions and will be a truly world-class learning and networking event.

Conference tracks, featuring sessions led by the world’s leading experts, will cover critical topics in the areas of instrumentation, communications, control systems, process variables, SCADA, safety, integration, and cybersecurity. Engineers, technicians, and plant managers from the oil and gas, refining, chemical, petrochemical, and other process industries will gather for three days to network and to learn from these technical presentations. Social events, keynotes, panel discussions, training courses, standards committee meetings, and a focused exhibit featuring leading companies will round out the event.

A limited number of exhibit tables and sponsorships are now available. Reserve your exhibit space and sponsorship now to guarantee access to this prime group of prospects, customers, buyers, and influential leaders in oil and gas, chemical, petrochemical, and related markets.

Exhibitors and sponsors for this 2015 event will enjoy priority exhibit and sponsorship selection in 2016.

Build important alliances, increase your customer base, and increase profit.
Hurry!—Limited exhibit space and event champion packages are available.

ISA Staff Contact:
Carol Schafer
cschafer@isa.org
+1 919-990-9206

Houston Volunteer Contact:
Ardis Bartle
ardisbartle@apexmeasurement.com
+1 713-446-1902
Champion Packages

Platinum Evening Reception Champion

Exclusive Champion of the Evening Reception: $4,750.00
- You may display your company banner at the evening reception
- Exhibit space includes 6’ skirted table (a $1,400.00 value)
- Your logo will be featured on all promotional material and attendee manual handouts
- Your company will be featured on the ISA event website with a link to your company website
- Back cover ad on the conference handout
- Mention in three (3) email blasts

Platinum Lunch Champion

Exclusive Champion for a Conference Luncheon: $3,500.00
- You may display your company banner or sign at the luncheon
- Exhibit space includes 6’ skirted table (a $1,400.00 value)
- Your logo will be featured on all promotional material and attendee manual handouts
- Your company will be featured on the ISA event website with a link to your company website
- Full page ad in the conference handout
- Mention in two (2) email blasts

Platinum Registration Table Champion

$3,500.00
- You may display your logo and product brochures at registration throughout the event
- Exhibit space includes 6’ skirted table (a $1,400.00 value)
- Your logo will be featured on all promotional material and registration e-mail blasts
- Signage featured at the door of the conference session
- Your company will be featured on the ISA event website with a link to your company website
- Full page ad in the conference handout
- Mention in two (2) email blasts

Gold Champion

Conference Presentations Noteiset: $3,000.00
- Exhibit spaces includes 6’ skirted table (a $1,400.00 value)
- Your company logo and URL will be included in the conference handouts, which will contain the slide presentations of the featured speakers
- You may display company informational handouts at the conference
- Your company will be featured on the ISA event website with a link to your company website
- Your logo will be featured on all promotional material and attendee manual handouts
- Mention in one (1) email blast

Silver Champion

Coffee Breaks (three available), Lanyards, or Tentcards
One Break: $1,500.00  Two Breaks: $2,500.00
- You may display your company banner or sign at one of the coffee breaks and registration desk during the conference
- Your logo will be featured on all promotional material and attendee manual handouts
- Your logo and company information will be printed on the back of name place cards—displayed on every attendee table

Other High Profile Champion Support Opportunities May Be Available.

Contact: Carol Schafer
cschafer@isa.org
+1 919-990-9206

Ardis Bartle
ardisbartle@apexmeasurement.com
+1 713-446-1902

Exhibit Days: Monday – Thursday, 9–12 November 2015

Exhibit Opportunities

Showcase Exhibitor
$1,550.00
- Exhibit space includes:
  - 6’ skirted table
  - Two chairs
  - Duplex outlet
  - One full conference registration
  - One exhibit staff registration

Additional Exhibitor Conference Registrations:
- ISA Member: $545.00 each
- Affiliate Member: $620.00 each
- List: $695.00 each

Floor Plan
available upon request
2015 Process Control and Safety Symposium

9–12 November 2015 • Houston Marriott Westchase • 2900 Briarpark Drive • Houston, TX 77042

Please complete this form and mail it with your payment to:
ISA, P.O. Box 12277, Durham, NC 27702-3561
Phone: +1 919-549-8411 • Fax: +1 919-549-8288

Name for Badge: ____________________________
ISA Division Member? □ Yes □ No

Title: ____________________________
Name of Division ____________________________

Company or Organization: ____________________________

Address/PO Box: __________________________________________
City: __________________________________________
State/Province: ____________________________  Zip/Postal Code: ____________________________
Country: __________________________________________
Phone: ____________________________  Fax: ____________________________  Email: ____________________________

All attendees, including speakers and session chairs, must register and pay the application registration fee.

2015 Process Control and Safety Symposium Registration

9 November through 12 November 2015

Full registration includes one copy of Conference Handouts; lunch Monday and Tuesday, food function and exhibits. (ISA training course registration is separate)

PRICE: $515 ISA Member
$645 Community Member/List
$100 Student (banquet not included)
$250 Nonworking Retiree (banquet not included)
Confirmed Speaker Pricing
$100 - 1 Day Event
$300 - 3 Day Event

Total Symposium Registration Payment: $ __________

ISA Training Course Registration

Each course runs from 8:00 a.m. – 4:00 p.m. on 9 November;
CEUs/PDHs: .7/7

□ IC39C-Introduction to the Management of Alarm Systems
□ IC32C- Introduction to Industrial Automation Security and the ANSI/ISA99 (IEC 62443) Standards
□ EC50C- Introduction to Safety Instrumented Systems
□ IC85C- Industrial Wireless Systems

PRICE (per course): $575 ISA Member
$645 Affiliate Member
$720 Community Member/List
$575 Group Discount

Total Training Course Registration Payment: $ __________

Method of Payment

□ Check enclosed (payable to ISA)
□ MasterCard □ Visa □ American Express □ Discover

Card Number: ____________________________
Cardholder’s Name: ____________________________
Expiration Date: ____________________________
Signature of Cardholder: ____________________________

Total Payment: $ __________

Make Hotel Reservations at:

Houston Marriott Westchase
2900 Briarpark Drive
Houston, TX 77042
Phone: +1 713-978-7400
www.isa.org/PCS2015hotel

Rates: $185.00 per night (ask for the ISA PMCD/Safety-Security Symposium Rate)
Cut-off date is 18 October 2015