CHEMPID is growing... Come join us

Director’s Message

By Prabhu Soundarrajan

Greetings to all Chemical and Petroleum Industries Division Members:

It is my pleasure to address the membership of CHEMPID and inform you of all the great activities that are going on with the division.

In my last letter, I shared my goal with you to create a world-class division board for CHEMPID to provide a high level of visibility to 6000+ members at our division and to accomplish all of our goals and satisfy our member’s needs. I am very happy to inform you that we have completely staffed our board in a few months with leaders who will make a difference to the CHEMPID membership. I would like you to join me in welcoming them to the CHEMPID board.

News Letter Editor: Rhonda Pelton
rwpelton@dow.com
Director Elect: Matthew Conklin
matthew.conklin@remasonco.com
Director Elect-Elect: Alan Bryant
Alan_Bryant@oxy.com
Webmaster: George Robertson
George.Robertson@chevron.com

Our social outreach activity is quickly gaining momentum. My special thanks to members who joined. We have members from all over the world in our Linked in group and several interesting discussions are ongoing for the membership benefit. I highly encourage you to start a discussion that is of interest to your company, plant, job or day to day function. Do not hesitate to ask a question. Do you have a job opening you need to fill? Post it online on our LinkedIn group. I created this open group for CHEMPID members and strongly encourage you to get involved. It is your group, it is open, help us grow CHEMPID on LinkedIn.

CHEMPID is collaborating with other ISA divisions to provide you a forum to discuss important topics for the petroleum and chemical industry. We are working with the Analysis Division (AD) on the 2012 Analysis Division Symposium which will be held 22-26 April 2012 in Garden Grove (Anaheim), California, USA. We are also working with the 58th International Instrumentation Symposium (IIS) which will be held at the Hyatt Regency La Jolla, San Diego, California, 4-7 June 2012. It is jointly sponsored by the Aerospace Industries, Test Measurement, and Process Measurement and Controls Divisions of ISA. Please contact Alan Bryant with topics of interest and your technical papers.

Student outreach is an important growth objective for CHEMPID. In these tough economic times, we would love to mentor students and help them find a job. Our Director Elect, Matthew Conklin will be leading this activity. If you are a recent graduate and looking for a position within the automation industry, feel free to contact us.

Leadership is the key to our success. In the next few months, you will see several interesting developments with CHEMPID. I welcome you read this version of the newsletter and provide any feedback you may have to our newsletter editor, Rhonda Pelton. I would also encourage you to contribute an article, talk about what ISA and CHEMPID has done for you and more importantly how we can help you!

CHEMPID was actively represented at ISA Automation Week in Mobile, Alabama, USA, with a division meeting. The CHEMPID board discussed a new vision and mission for the division. I will tell you more in the next newsletter.

CHEMPID is growing…come join us to enjoy the experience and to create a world of difference. On behalf of CHEMPID, I also wish all our members and leaders a happy holiday season.

Until next time,
Prabhu Soundarrajan
p.soundarrajan@lumasenseinc.com
The Chemical and Petroleum Industries Division was featured on ISA Insights
Reprinted from ISA Insights article by Emily Kovac

1. **Describe your division as if you were speaking to someone hearing about it for the first time.**

   The International Society of Automation (ISA) has two departments each with multiple technical divisions. The Chemical and Petroleum Division (CHEMPID) is part of the Industries and Sciences Department of ISA.

   CHEMPID is a re-energized and refocused to serve the ISA membership and professionals involved in the processing of chemicals, petrochemicals, petroleum, and natural gas. From raw materials to products, CHEMPID strives to advance best practices in: Safety, Environmental, Production Efficiency, Operations, Process Control, and Process Automation. CHEMPID produces two technical letters each year to promote innovation within the Chemical and Petroleum Industry.

2. **Tell Insights readers about something your division educated you on or will allow them to explore within the automation industry.**

   With Global competition, no operation can run the same year after year. Plants are either improving or declining. The key to success is to capitalize on problems that have already been solved and focus your engineering talent on problems that require innovation. CHEMPID is here to give its members the tools they need to be in the “improving” category.

   One of CHEMPID’s key objectives is to provide a discussion forum, in which engineering professionals can get real-time answers to technical questions. To meet this objective, CHEMPID maintains an active LinkedIn group where automation professionals can interact and discuss important industry and automation issues.

   In addition to the benefits of the increased knowledge and skills, the division plans for the future include rewarding contributors, through a feature of the Top-10 Contributors on the CHEMPID Website. Of course, there is always the benefit of professional recommendations from engineers that have received help.

3. **What items/events are coming up that your division is preparing for?**

   CHEMPID will co-sponsor conference tracks at ISA Analysis division and IIS symposia in 2012. The CHEMPID board regularly attends local chapter and regional meetings, as well as the leader’s meeting. Professionals are encouraged to get engaged and get an inside view of this exciting, enlightening division. Your career and professional development will take a whole new path—upward!

   If someone is interested in joining your division or learning more, who is a good contact for them? (We will also include the link to your division on the web.)

   - Join the ISA CHEMPID division: Link
   - Get involved. Serve on the CHEMPID Board, now or in the future.
   - Join our growing LinkedIn group and start a conversation: Link
   - Contact one of the board members directly (p.soundarrajan@lumasenseinc.com; matthew.conklin@remonsonco.com, rwpelton@dow.com; Alan_Bryant@oxy.com)

Cybersecurity certification program launches

Sypris Electronics, LLC, a subsidiary of Sypris Solutions, Inc. partnered with Career Technical Education Foundation, Inc. (CTEF) and The MITRE Corporation to develop, establish, and host a cybersecurity curriculum for local and national high school students. The curriculum was co-developed by Sypris, MITRE, and CTEF, and it is under evaluation by (ISC)². The training takes place in Sypris’ Cyber Collaboration Center located in Tampa, Fla.

The two-week pilot program had 20 students enrolled from high schools representing three counties in Florida, as well as others outside the state. Students were selected based on their strong computer science backgrounds and interests. The course curriculum, based on cyber attack defense and offense methodologies and techniques, provides students with a broad base of cybersecurity foundations that can be used immediately and aid in the path of becoming a cyber security professional.

The course is being taught by a team of MITRE and Sypris computer scientists and is being audited by (ISC)² to validate the course maps to the (ISC)² SSCP common body of knowledge, a compendium of global information security topics. Students who successfully pass the program, along with a Systems Security Certified Practitioner (SSCP) certification exam, will become an Associate of (ISC)² toward the SSCP certification, an opportunity not currently available to any other high school students in the nation.

“There is no other cybersecurity curriculum available for secondary education anywhere in the country, and we are the first to make it available,” said Paul Wahnish, president of CTEF. “Students are excited to learn from cyber experts in this new, real-world cyber lab. I would like to personally thank our partners for taking the initiative in helping to educate our future workforce.”

“We are proud to have the opportunity to serve our community and stakeholders by providing this unique educational opportunity to future Cyber Warriors, both locally and across the nation,” said John Walsh, president of Sypris Electronics.
Cybersecurity meets plant politics

Don’t neglect your control system.

By Joseph M. Weiss

Control systems are the backbone and mission critical components of global industrial infrastructures, such as electric power, oil and gas, chemical, pharmaceutical, water, paper, metal refining, auto manufacturing, transportation, and food processing. However, these open systems have come with a cost: cyber vulnerability. Proprietary systems are included in those cyber vulnerabilities. We have either ignored them or assumed they fall into the category of security by obscurity.

Nearly every country in the world sells a limited number of operational control systems. The wide geographical distribution of a relatively small global market, compounded with the growing threat of intentional and unintentional cyber incidents, could result in wide-spread impact to the reliable operations of control systems.

In theory and practice

Security studies from the U.S. Department of Energy (DOE) and commercial security consultants, including KEMA, have demonstrated the cyber vulnerabilities of control systems. More than 60 identified (though not publicly documented) real-world cases have occurred where electronic means have impacted the control systems’ reliable operations. The expectation was a cyber event involving a control system would be obvious and publicly known. That assumption has turned out to be wrong.

Companies whose control systems are impacted by cyber are not willing to publicly acknowledge the intrusions or impacts. Cyber events have occurred in control systems within electric power transmission, distribution, and generation (including fossil, gas turbine, and nuclear) and also within control systems for water, oil and gas, chemical, paper, and agri-businesses.

Control systems could offer some of the most attractive targets to malicious actors since they contain critical data and often are the least electronically protected assets.

We can hope as industry and governments become more aware of and active in the issues surrounding control system security, Internet monitoring organizations will recognize and analyze related incidents in collaboration with vendors. They would promulgate the results to the infrastructure owners and operators. As the risk environment continues to evolve, the security community can no longer afford to focus solely on enterprise business applications, and incident analysis must now include control systems and the associated impact on critical infrastructures.

Risk environment

Control systems could offer some of the most attractive targets to malicious actors since they contain critical data and often are the least electronically protected assets. Control systems have been designed with specific reliability and availability requirements but not specific cybersecurity requirements. Adapting cybersecurity to these requirements is another challenge, and one we must meet.

If malicious actors could access these systems, they would have access to operational data critical to the operation of the system.

Also, a knowledgeable attacker could modify the data used for operational decisions, the programs that control critical industry equipment, or the data reported to control centers. The impact could be destructive.

Such attacks could exceed equipment design and safety limits and potentially result in damage, premature system shutdown, and interference with safety system operations. Or they could immobilize control equipment. Consequences could include endangerment of public health and safety, environmental damage, or significant financial impacts due to loss of power production, transmission, or distribution.

Control system researchers at the DOE’s national laboratories have gone so far as to demonstrate the feasibility of cyber attacks on control systems similar to those installed at electric power generation facilities. Using tools readily available on the Internet, researchers have bypassed the protection features of firewalls to take over direct control of substation LANs as a means to change settings and create new output that could incapacitate or even damage power plant equipment.

Control systems are susceptible to attack because they weren’t designed to meet cyber threats. As control systems move from traditional closed networks into highly interconnected heterogeneous networks, containing both standardized and legacy technology, the threat environment has changed. In light of these heterogeneous networks, we cannot directly apply security technologies designed for common business IT systems to control systems and still provide adequate protection. Designers of control systems did not design them with operational requirements for reliability and availability. Hence, the integration of security into those systems must account for these requirements, which can differ drastically from those of business IT systems.

Most control systems in use perform specific tasks and contain only limited processing power and memory. Consequently, they don’t have the computing resources needed to leverage the authorization, authentication, encryption, intrusion detection, and filtering capabilities of modern security technology. To date, these constraints preclude the use of technologies like National Institute of Standards and Technology (NIST)-approved block encryption and public key infrastructure (PKI) without seriously degrading control system performance. This is mainly because these technologies are too resource-intensive for many legacy control systems and may actually cause the systems to fail as they attempt to keep up with the demands on their limited resources. Although modern control systems are based on standard operating systems, they are typically customized to support control system applications. Consequently, vendor-provided software patches may either be incompatible with the customized version of the operating system or be difficult to implement without compromising service.

Industry activities

Several governments and private organizations, as well as industry associations, have developed cybersecurity courses, guidelines, and standards aimed at promoting awareness of control system vulnerabilities and mitigation measures.
Traditional control system vendors are usually not supplying secure control systems, and customers (utilities) are not requesting them. This could be due in part to vendors not seeing a market demand for security since customers are not demanding it. Another aspect could be the extensive system lifecycle for control systems and the perception of “if it isn’t broken, don’t fix it.” This perceived gap between vendors and customers could further link to the lack of existing specifications, potentially due to the absence of a government mandate for control systems security. ISA’s SP99 Committee and the NIST-established Process Controls Security Requirements Forum (PCSRF) are working to define a common set of information security requirements for control systems that users and vendors alike can reference, and several groups are developing standards that increase the security of control systems.

**Economic hurdles**

Justifying security investments is not unique to industrial operations. They constantly question implementing security for return on investment. Cyber incident statistics for enterprise business applications is readily available, such as CERT/CC and tracked, as is the associated economic impact.

However, economic justification for industrial security, including electric power, is difficult. Operational managers are required to perform economic trade-offs between O&M expenditures and control system cybersecurity mitigation. A quantitative business case documenting cyber incident impacts could help others develop an economic justification for industrial security. Consequently, a study is in progress to develop representative case histories of companies in which cyber intrusions have impacted control systems. Some of these are power plant cases.

Some results to date include that companies are reticent to report control system cybersecurity incidents and expenses result even if power is not interrupted. Penetration testing and scanning control systems is another issue. Most of the cases could have been prevented or at least substantially mitigated with adequate security policies and procedures.

Although there are quite a few hurdles impeding control system security, continued collaborative efforts between industry, standards organizations, vendors, and governments will advance and promulgate security for these systems to customers. Education, standards, and guidelines for control systems will lead to enhanced security and maintained reliability for the industry as a whole and to enhanced economic viability and public safety.

---


ISA Member Price: $99.00  
List Price: $459.00  
Product ISBN/ID: 978193600-7370
Introduction

The proliferation of industrial Ethernet today is putting manufacturing at risk for inadvertent and deliberate intrusions. Security measures tailored specifically for production environments are imperative for keeping operations protected and profitable.

Security today is a necessary part of every manufacturing operation that expects to run smoothly, efficiently, safely, and profitably. But protecting the industrial environment is far from an easy job. As production equipment and the systems that connect and control it grow increasingly more complex and sophisticated, the measures needed to protect them become more critical as well.

Fueling these developments in large part is the recent evolution of Ethernet technology from the office enterprise to the industrial environment. Once thought to be insufficiently robust and lacking in functionality, industrial Ethernet (standardized Ethernet communications over a hardened networking infrastructure) has advanced remarkably, becoming, in a few short years, the communications staple of manufacturing and production, of automation and control.

Although it offers many benefits, industrial Ethernet is not without issues, especially in terms of security. It typically must carry signals between devices on a precise, exacting schedule. While standard Ethernet in the office environment may be unharmed by a signal transmission fault, it is a different story in the industrial world. Networks here must be able to withstand harsh and hazardous environments with little margin for error. Downtime caused by a security breach on the manufacturing side—whether it is from an inadvertent or unintentional error or from a deliberate cyber attack—is always expensive and can put assets at risk.

In particular, two developments accelerated the growth of industrial Ethernet:

• Operating system vendors used Ethernet to create networks that united once-isolated clusters of information (standalone personal computers and servers); and
• Software vendors developed applications that allowed this information to be shared over a common network resource.

Once industrial automation developers saw how flexible and reliable Ethernet networks had become in the enterprise world, they started looking at how they might capitalize on Ethernet technologies as well. The result was an industrial automation revolution that used Ethernet networks as the core technology to drive increased productivity, reduce costs, and integrate real-time data from manufacturing to the front office.

Using common protocols over standardized networking equipment brought many advantages to industrial and enterprise networks. Thanks to interconnected enterprise and industrial networks, seamless interoperability from the shop floor to the front office made multi-network connectivity, anytime, anywhere, a reality.
Corporations with multiple geographical locations could be united as if in a single building. Multi-faceted organizational and commercial entities could more easily collaborate, simplifying intersystem relationships. Yet these advantages are the very cause of the vulnerabilities and weaknesses that expose industrial networks to many of the same security woes of the enterprise network. In some cases, even more.

**A Different Animal: The Need for a Special Kind of Protection**

The security mechanisms and controls used to protect enterprise networks are, quite simply, insufficient or ineffective for industrial networks. Although they use the same types of networking equipment and protocols, industrial and enterprise networks have different characteristics, adhere to different performance criteria, and can be affected in dramatically different ways by the same types of events.

Enterprise networks usually can withstand periodic network outages anywhere from a few minutes to a couple of hours, depending on the type of failure. Firewalls and proxy servers protect them from external threats. Operating system patches, intrusion detection mechanisms, and anti-virus software keep them safe from internal threats. In addition, they are continuously scanned by designated security systems, operate in a relatively controlled environment, and are cared for by a dedicated, trained technical staff. Communications on enterprise networks are rarely time sensitive and the traffic often comes in bursts, as, for example, when data files or documents are transferred from one server to another. Many mechanisms used by today’s popular operating systems rely heavily on broadcasts and multicasts to resolve network resources and establish communications with peer systems.

Industrial networks are a different animal. They have a more specialized nature, with environments ranging from climate controlled clean rooms to hazardous manufacturing environments. Rarely is a dedicated staff on hand to monitor and maintain an industrial network. Its care becomes one more duty for plant, production, or control engineers who are already maintaining high production rates on lean budgets within stringent timelines.

Deterministic control networks usually operate within strict timing constraints and sustained rather than intermittent traffic. Outages are intolerable. Any disruption is too long, and can lead to waste or contamination of raw or in-process materials or goods. It might also mean an entire process needs to be restarted. Unplanned disruptions can pose risks of all kinds to manufacturing assets. The capability must be there to restore a system to operation as quickly as possible. Further, production machines rarely can be secured with a software patch, anti-virus system, or intrusion detection mechanism. Most

---

**Ethernet Topology**

*BUILDING A*

- **CORPORATE NETWORK/RACK/BONE**
  - **ENTERPRISE/OFFICE NETWORK**
  - **PLANT/FACILITY FLOOR**
- **PLANT ENGINEERING OFFICES**
- **REDUNDANT Link**
- **HI PEr Ring**
- **RS-485**
- **RSTP (Rapid Spanning Tree)**

*BUILDING B*

- **CORPORATE NETWORK/RACK/BONE**
  - **ENTERPRISE/OFFICE NETWORK**
  - **PLANT/FACILITY FLOOR**
- **PLANT ENGINEERING OFFICES**
- **REDUNDANT Link**
- **HI PEr Ring**
- **RS-485**
- **RSTP (Rapid Spanning Tree)**

Ethernet topology showing integration of the corporate network with the manufacturing plant. Security is achieved through use of Hirschmann® Eagle Firewall/VPN devices in three areas: at Plant Engineering (highlighted in light blue) and two areas of the plant floor in Building B (highlighted in light orange). Eagle VPN devices are ideal for remote, secure access – isolating a network by controlling what data is allowed to pass in either direction and to perform NAT (Network Address Translation).
of the time, they must be updated by the vendor, at significant cost in time and money.

Industrial networks vary widely in how they are linked to corporate networks today. Some are directly connected on the same enterprise domain. Others consist of segmented networks connected by routers or VLANs (virtual local area networks). Still others remain completely isolated while sharing common resources over the Internet. In too many instances, security measures for these networks mirror the controls and mechanisms used in the enterprise network…and subsequently fail to address the requirements of the industrial side. What is needed is a more robust method of securing the industrial network by adapting, modifying, and configuring tried-and-true security techniques developed by the enterprise for use in the industrial world. These adaptations must consider the differing security focus, performance requirements, production architectures, and risk management goals of the manufacturing processes, facilities, and networks.

Ways and Means: Building Protection into the Network

Let’s look in more detail at these characteristics, at how they impact the development of a secure communications network, and at some of the measures, procedures, and devices that can be applied to provide protection. Just what are the needs of an industrial security network compared to the capabilities of an IT-system security network? The overall goal of any industrial network protection strategy should be to protect all sensitive areas of the production process while supporting the long-term integration of the office and industrial networks in the company-wide environment. Building such a system can be a delicate balancing act. On the one hand, the industrial network cannot merely copy the security measures used in the office environment. To do so will leave security gaps. On the other hand, care must be taken not to over-engineer network security. To do so might be too restrictive or make certain necessary actions prohibitive.

The challenge to the manufacturer is to become familiar enough with the points of vulnerability of his operation, acquire an understanding of the security tools available, and then build a system that will provide adequate protection. A variety of security techniques and technologies exist today, and virtually thousands of products are available to help do the job. These include, but are not limited to, industrial networking firewalls and routers; security appliances; and VPN, authentication, and encryption devices discussed here. Properly applied and installed, these mechanisms and techniques can give your industrial network the security it requires for directly connecting either the network or individual production devices to the Internet, corporate or remote offices, remote production facilities, duplicate production cells, or other areas that need secure industrial Ethernet communications.

Firewalls...and Firewall/Routers. Firewalls come in many types; common among them are transparent products that operate out of the box.

Such plug-and-play devices can be installed anywhere on the network without the need to configure or re-configure end devices. No changes to the network settings (IP addresses, subnet masks, and default gateways) are required; networks do not have to be divided into separate IP subnets.

Firewall/routers usually are combination devices. They consist either of routers with some built-in firewall functionalities, or firewalls with routing functionalities built in. They excel at protecting the industrial network edge: the points of vulnerability where the industrial network meets the corporate network or Internet.

These devices can segment networks, be used as a gateway, and enable safe access to the Internet. Firewall functions include isolating critical devices from threat sources, separating the network into security zones, restricting communications between zones, and protecting controllers from known vulnerabilities.
In a typical firewall/routing operation, all IP (Internet Protocol) traffic sent from a secure network to an unsecured network or beyond is permitted to traverse the firewall/router. Traffic sent to the secured network from an unsecured network is blocked automatically. Replies from any secured traffic that establishes and maintains a TCP (Transmission Control Protocol) connection with an external host should be inspected against a stateful inspection firewall to ensure that the traffic is authorized and that it is not being spoofed or forged from an unknown or unauthorized external host.

The stateful inspection firewall feature is an important technology for industrial-grade firewalls/routers today as it analyzes the type of traffic going through the network. It tracks where it is coming from, where it is going, and, most importantly, examines packet characteristics. Rather than simply filtering data based on source and destination, it looks deeper into the packet. It not only tries to establish that the data are coming from an authorized source, but also that established connection rules were followed. Such capabilities help avoid “man in the middle” attacks, in which a hacker eavesdropping on the Internet hijacks a communication session between two parties and impersonates one of the parties.

**Security Appliances.** Security appliances are another type of in-line hardware intended to give a single device or a small group of devices real-time protection from unwanted and undesirable traffic. Among the newest types are those that offer zone level security, including deep packet inspection for groups of programmable logic controllers (PLCs), distributed control systems (DCSs), remote terminal units (RTUs), and human-machine interfaces (HMIs) and their industry specific communication protocols. These devices are usually simpler to install than many other security products, and can be installed and implemented on a live network with no special training, pre-configuration, or system downtime.

These types of products usually are offered as a distributed security solution. The central management software that accompanies the devices enables modular configuration, management, and monitoring of multiple appliances from a single management workstation. The management software allows a virtual model of an entire control network to be quickly developed; many offer drag-and-drop tools to simplify creating, editing, and testing the configuration of the appliances and devices deployed in your network. The status of an entire system is visible at a glance on a single monitor, providing real-time information about non-conforming events in your network.

**VPNs, Authentication and Encryption Techniques.** Secure communications can be extended beyond the network’s edge, local security cell, or device level using remote user authentication or VPN (virtual private network) connections. Most firewalls can support the establishment of VPN connections using secured socket layer (SSL), pre-shared key (PSK) or X.509 certificates to provide encrypted access across intermediate or untrustworthy networks such as the Internet. Additional secured communications can be established using user authentication and user specific firewall rule bases. The firewall may be used on a network’s edge between the office and the plant floor or duplicate production cells, or act as a gateway to the Internet.

For example, a VPN solution should create secure tunnels of communication over untrustworthy networks, including the Internet or corporate business network. It should be easy to deploy, test, and manage and should provide ways to build pre-configured installation files to help ensure that security is not compromised by configuration errors. In addition, it should support industrial automation devices and protocols, be industrially hardened, and be able to be combined with other equipment to create a comprehensive security solution.

**Beyond the Basics: Putting It All Together**

Choosing devices to secure the industrial communications network is only part of the challenge. Installing the right equipment properly also plays a significant role, with the volume of components and number of variables involved making for an often enormous task. And unfortunately, one size, system, or approach does not fit all, or even most. However, some general concepts and guidelines do apply.

Different products are intended for different purposes. For example, a security appliance protects at the device level and has no routing or network segmentation capability. For a small plant with no on-site IT staff that needs to link to the Internet to connect to its main corporate office, a firewall would be a better choice. The security appliance usually cannot act as a traditional firewall or router. It cannot construct separate network segments by creating an IP network segment on one interface and an IP network segment on the other. Although it will not modify or route traffic to a different network segment, it will, however, protect end-devices through comprehensive traffic monitoring and customizable granular firewall rule bases.

Because systems vary so widely, specifics are impossible to enumerate in this paper. In general, however, when putting together such a system, take time to answer such questions as:

- Does the device or system provide scalable security functionality?
- Is it easy to integrate into the existing architecture?
- Is it easy to install, operate, and maintain?
- Does it include comprehensive diagnostics, such as Web-based management and status LEDs?
- Does it support redundancy mechanisms?
When choosing protection, take time to determine whether the devices being considered were developed with your personnel in mind. Is the system designed so that your staff can use it effectively without needing to be an IT expert, or to call one at every turn? In addition, any industrial security device must be designed, approved, and hardened for harsh environments. It should include ruggedized housings, redundant internal power supplies, and a wide operating temperature range to enable installation wherever security is needed.

Most security systems accommodate a variety of network connectivity media, the most common being copper or fiber optic cabling, and wireless—or, in some cases, a combination. Although all provide optimum signal transmission performance, high-risk installations might lean toward fiber optics, which offers high bandwidth, is not susceptible to interference (EMI or RFI), and offers a more robust medium that is less prone to hackers. When fiber optic cable is chosen, however, some special installation concerns must be addressed—among them bend radius restrictions, maximum load, and certain environmental hazards, in particular moisture.

Overall, industrial Ethernet security devices should be capable of being managed individually using either your Internet browser of choice or with additional software from the device manufacturer. Multiple firewall configurations should be maintainable on the device or off-line, as required. Security equipment may be applied at the edge of the industrial network, the subsystem level, and/or the production cell or machine itself. Such umbrella protection offers simplicity and reliability, providing local security for a full range of control applications, remote operations and maintenance, and links to adjacent processes.

**Go the Extra Mile:**
**Developing Defense-in-Depth Security**

Today's burgeoning technology, coupled with exploding industrial automation, is advancing the need for security. Industrial Ethernet unquestionably has brought innumerable benefits to control systems and to the plant floor. It has also opened the door to many problems. Protecting the industrial operation is not discretionary. Failure to safeguard it puts a company at risk for expensive and time-consuming downtime and damages.

No system should be installed and forgotten. Security is a dynamic process that involves, beyond the initial effort, regular maintenance and improvement; periodic evaluation and updates; and continuing education. Every facility should work with its security solution vendor to perform, at regular intervals, a security risk assessment and review the measures that have been put in place, especially in terms of process or production changes that may have been implemented. Be aware of modifications that may create new vulnerabilities, and know that products continue to evolve, offering improved performance and greater efficiency.

Further, no single source should ever be expected to provide all the answers. Take time to learn about security measures and advancements. Help is available: Ask your vendor, attend workshops and seminars, consult outside experts, and make use of online resources. Helpful U.S. government sites include the Department of Homeland Security's US-CERT [computer emergency readiness team], which makes available a variety of information online and through security publications (www.us-cert.gov). The Computer Security Division Computer Security Resource Center (csrc.nist.gov) of the U.S. National Institute of Standards and Technology (NIST) is another good source. Helpful international organizations include the International Electrotechnical Commission, or IEC (www.iec.ch) and the International Organization for Standards, or ISO (www.iso.org). Independent organizations such as the Industrial Society of Automation, or ISA (www.isa.org), also offer materials and advice. Finally, check with your own industry associations to see what they offer. In all cases, search "security" on the home page of any of these websites to see what information might be available.

A system of well-placed security products and procedures—only a few of which have been touched upon here—is time and money well spent. Giving your manufacturing operation the defense-in-depth security it needs, tailored to its specific demands, precision levels, and rugged environments, requires careful planning, diligent installation, and continuing vigilance. A system design must take into account the industrial security focus, performance requirements, and risk management goals of the manufacturing process that standard IT solutions fail to provide. To do otherwise, is just risky business.
The 57th Analysis Division Symposium will be held 22–26 April 2012 in Garden Grove (Anaheim), CA, USA

This symposium is recognized as the outstanding forum for discussion of new and innovative analytical techniques, developments, and applications for process and laboratory. Speakers and attendees to the symposium are from all over the world and share the opportunity to speak to an international audience, participate in informal discussions and social gatherings, and acquire the latest information about analytical sciences.

Papers are accepted which address topics in process and laboratory analysis including methods, analytical applications, analytical hardware and software, analytical systems and analyzer system operation and maintenance. Subject content may concern technology in development or technology as applied in industry practice.

General subject areas of interest
- Chemical Analyzers
- Systems Integration
- Physical Properties Maintenance
- Spectroscopy
- Chromatography Gas Detectors
- Sampling Systems Emerging Technology
- Validation
- Environmental

Submission guidelines
All papers are reviewed by the official Analysis Division Paper Review Committee and must conform, or be modified to conform, to Analysis Division and ISA format and content guidelines. Papers must address the technology and may not be commercial in nature.

All papers must be submitted in electronic format (Microsoft Word) suitable for publication in the proceedings by the deadlines indicated below. All overhead slides or presentation materials used at the symposium must be provided in electronic format (Microsoft PowerPoint) prior to the symposium for review and approval. A publication release form is required by ISA for all papers.

How to submit
An "Intent to Present" is due immediately to Mike Chaney, the Technical Program Chairperson, at michael.chaney@lyondellbasell.com, with abstracts to be submitted by 30 November 2011 to the Paper Review Committee Chairperson, Paul Barnard at paul.barnard@lyondellbasell.com.

Draft Paper to Review Chairman: 20 January 2012
Reviewers' Comments to Authors: 24 February 2012
Final Paper for Publication: 2 March 2012
Papers Sent to Publisher: 16 March 2012
Oral Presentation Electronic Materials: 10 April 2012
Symposium Presentation: 23–25 April 2012

General Chairperson
Sandra Krauthamer  krth@chevron.com

CHEMPID Scholarships
Spread the word!

CHEMPID is pleased to fund scholarships for outstanding students who are pursuing automation careers in the chemical and petroleum industries. The CHEMPID-funded scholarships are among the many ISA Educational Foundation Scholarships awarded to college or university students who demonstrate outstanding potential for long-range contribution to the fields of automation and control. The scholarships support tuition, related expenses, and research activities and initiatives.

Application for these scholarships will beginning in September for the 2011–2012 academic year. At that time, application forms and rules will be posted on ISA’s website at www.isa.org/scholarships.

To be eligible, applicants must be currently enrolled in a graduate or undergraduate program in an instrumentation, systems, or automation discipline (two-year program or four-year baccalaureate program or its equivalent) at an educational institution in their country of residence.

- Two-year program applicants must have completed at least one academic semester or 12 semester hours or its equivalent.
- Four-year degree program applicants must be in their sophomore year, or higher, of their study, or its equivalent at the time of application.
Upcoming ISA Events

ISA’s unbiased symposia and technical conferences provide automation professionals across the world with the latest technologies, trends, real-world examples, tutorials, and updates needed to remain competitive in today’s and tomorrow’s markets.

Mark your calendars and make plans to attend an ISA symposium or technical conference in 2012!

**Wireless Factory Automation Workshop**
17–18 April 2012
Detroit, Michigan

**57th Analysis Division Symposium**
22–26 April 2012
Crowne Plaza Anaheim Resort
Anaheim, California

**2012 Safety and Security Division Symposium**
25–26 April 2012
Crowne Plaza Anaheim Resort
Anaheim, California

**12th ISA Fugitive Emissions-LDAR Symposium**
14–16 May 2012
Astor Crowne Plaza
New Orleans, Louisiana

**55th ISA Power Industry Division Symposium**
3–8 June 2012
Renaissance Austin
Austin, Texas

**58th International Instrumentation Symposium**
4–8 June 2012
Hyatt Regency La Jolla
San Diego, California

**ISA Communications Division Symposium**
5–7 June 2012
Hyatt Regency La Jolla
San Diego, California

**ISA Automation Week**
24–27 September 2012
Orange County Convention Center
Orlando, Florida

**Water and Wastewater and Automatic Controls Division Symposium**
7–9 August 2012
Holiday Inn Resort Orlando
Orlando, Florida

**7th Annual ISA Marketing & Sales Summit**
15–17 August 2012
Austin, Texas

Find out more at [www.isa.org/events](http://www.isa.org/events)
58th International Instrumentation Symposium

Hyatt Regency La Jolla, San Diego, California, June 4 - 7, 2012
Sponsored by ISA’s Aerospace Industries (ASD), Test Measurements (TMD), and Process Measurement and Control (PMCD) Divisions, in conjunction with the participation of the Propulsion Instrumentation Working Group (PIWG)

Call for Papers

58 YEARS IN THE MAKING...

The 58th International Instrumentation Symposium (IIS) is sponsored jointly by the Aerospace Industries, Test Measurement, and Process Measurement and Controls Divisions of ISA. It is recognized internationally as the outstanding forum for discussion of new and innovative instrumentation techniques, development and applications. The symposium will include paper sessions, short courses, workshops and tutorials. Program information will be available on www.isa.org/iis. For the latest list of short courses, workshops and tutorials refer to the ISA website. Papers will be considered for publication in ISA’s technical journal ISA Transactions.

Guidelines for submission:

• All Authors/Speakers in attendance must pay registration fee
• 500-word (max) abstract in English shall be submitted electronically
• Final presentations must be on the official ISA Symposium template
• Papers accepted for publication and presentation will require completion of the ISA’s Rights and Responsibilities form

The lead author is the main contact. Submit your abstract via email to Bryan.Hayes@arnold.af.mil and techconf@isa.org

Deadlines:

Abstracts 20 January 2012
Draft Papers 23 March 2012
Final Papers 18 May 2012

For additional information, contact:
Edward Naranjo
General Chair
+1 (949) 581-4464
edwardn@generalmonitors.com

Bryan Hayes
Program Chair
+1 (931) 454-5810
Bryan.Hayes@arnold.af.mil

Rodney Jones
ISA Staff
+1 (919) 990-9418
rjones@isa.org

Topics include but are not limited to:

Instrumentation
➤ Sensors
➤ Transducers
➤ Wireless, Electromagnetic, and RF Instrumentation
➤ Remote Sensing
➤ Environmental Monitoring
➤ Laser and Electro-Optics Instrumentation
➤ Power Systems, Radiation, and Nuclear
➤ Intelligent Instrumentation and Measurement

Data systems
➤ Measurement Standards
➤ Automated Measurement Techniques

Communications
➤ Telemetry
➤ DCS, SCADA,
➤ Industrial Instrumentation

Turbine Engine Testing
➤ Tip Timing Technologies
➤ Hot Section Gas Temperature, Dynamic Pressure,
➤ Tip Clearance Technologies

Platform Testing
➤ Ground
➤ Autonomous Vehicles
➤ Manned Flight
➤ Unmanned Flight
➤ Process

Test Facilities
Metrology
➤ Field
➤ Bench
➤ Uncertainty

Cyber and Homeland Security
Safety Instrumented Systems
Process Measurement and Control
Control System Instrumentation
Student paper Sessions
➤ Undergraduate
➤ Graduate

Setting the Standard for Automation™
So...what do you know?

Do you have insights and ideas that might interest your automation colleagues? Have you ever thought about sharing them with ISA's InTech magazine?

You don't have to be an accomplished writer. If your ideas are a good fit with InTech's editorial calendar, our editorial staff will collaborate with you on your story. If you're already an author, that's great! If your article is published, InTech will award you with our ultra-cool "Brain Swap Contributor" T-shirt.

Contact our editors at intechmagazine@isa.org to discuss how you can contribute.
Show your success
With ISA Senior membership

Pssst, been in the business ten years? Or, have a degree and six years of work experience? Sounds like you may qualify for ISA Senior Member grade. Why apply? ISA Senior Member grade is a statement of your knowledge and experience. It’s also a requirement for becoming a candidate for ISA Fellow grade or to hold a Society-level office.

Find all the details and an application form at www.isa.org/seniormember or call (919) 549-8411.

Brag a little. Apply today for ISA Senior Member grade.

Setting the Standard for Automation™
As an ISA Member, you can stay up-to-date on the latest technical issues by downloading your choices from more than 2,500 technical papers published at ISA conferences and symposia. New papers are added every year as new conferences are conducted. Get the latest today!

Free, unlimited access to these resources is just one of the many valuable benefits available to you as a Member.

Take advantage of this vast resource, visit www.isa.org/technicalpapers.
Mr. Alex Neubaver
Mr. Peter A. Nick
Senior Consultant

Joseph N. Nista, Sr.
Consultant

Rogerio de Souza Nogueira
Tecnico Automacao

Mr. Fernando Noriega
DCS Engineer
YPFB Chaco SA

Mr. John Mark Norrell
Discipline Lead Control Systems
CH2M Hill Engineers

Mr. John Mark Norrell
DCS Engineer
YPFB Chaco SA

Mr. Richard Forga Nwantoly

Alejandro Ochoa

Rodrigo Okamura

Mr. Gustavo Vinicius Lopes
De Oliveira

Leonardo Henrique S. de Oliveira

Rodrigo Oliveira

Mr. Enrique Oliveira de Assis
UFES

Jose Miguel Olza Martin
Loeches
Ingieniero Proyecto
Westinghouse Electric Spain

Mateus Orth

Mr. Hoag Ostling, ISA84 SFS
Consulting Engineer
Hoaglund Engineering

Mr. Francis J. Otto, Jr.
Sr Instrument & Controls Engineer

Ms. Lucimara Andrade
Paggiossi
Gerente De Projetos

Ivan Ferreyro Paladín
Tecnico De Instrumentacao

Kenneth M. Palesh

Mr. Jeffery A. Parsons
Senior Engineer

Ms. Monica Pascua
Tecnico De Inspeccion
Repsol YPF

Mr. Fred Patrick
E&I Project Engineer

Mr. Hugo Pellissari Pavan

Mr. Elian Santana Peruci

Tate Petronski

Mr. Gary R. Pfrehm
Vice President

Mr. Phil Philpott
Lead Instrument Engineer
Plexal Group

Silvio Pinto

Mr. Caio Yohames Pax Pio

Ricardo Andreotte Francini

Piolli Costardi

Matthew Prater
Demar Services LLC

Mr. Bryant Price
Process Control Engineer
Marathon Oil Company

Michael John Proppe

Manuel Guillermo Quijano Ortega
Engineer Control & Instrumentation

Ralph Rabie
Area Sales Manager
PR Electronics

Ms. Ivana Rezende

R. L. Rhodes

Ms. Tania M. Rhodes
Project Manager Cyber Security Manager
Emerson Process Management

Mr. Fabio Silva Ribeiro

Edvaldo Ribeiro
Engenheiro De Automacao Sr

Mr. Felipe Tiago Ribeiro
Reinan Ribeiro

Mr. Pedro Miguel Ribeiro
Ferreira
Inside Sales Engineer

H. F. Richter, Jr.

Mr. Marshall G. Rife

Mr. Henry Rivera, Jr.
Coordinator Network Services
Chevron

Wilmar Ferney Rivera Perez

Mr. Russell T. Rivers
William R. Rockholt
Inside Sales & Technical Support
Controlco

Mr. Joaquim A. Rodeia
MSC Engineer
Comartec Lda

Mr. Gilmar Dias Rodrigues

Mr. J. B. Roede
Control & Instrumentation Consultant

Gustavo Enrique Rojas
Perilla
General Manager

Rodrigo Alonso Rueda Blanco
Engineer Instrumentation
Ecopetrol

Mr. Scott Ruppert
ConocoPhilips

Mr. Edward Sablatura
Analyzer Technician

Mr. Alireza Sahraei
Senior Control Systems Engineer

Fidel Salazar
Automation/Instrumentation Engineer

Mr. Fernando Boiko Salles

Luis Alejandro Sanchez Rozo
Line Director

Mr. Alexandre Careli Dos Santos

Paul Oliver Santos Marin
Ingeniero De Proyecto
Centro De Ingenieria Y Desarrollo

Larry Joe Scarcella
Technical Sales

Rodrigo Alexander Schinemann

Ms. Michelle R. Scott
Territory Manager
Techstar

Mr. Subhro Sengupta
Senior Deputy General Manager

Mr. R. L. Sharp
Sales Marketing Manager

Paul B. Shaver
Sr. Automation Technician
Cannon

Mr. Neal Anthony Sholl
Senior Instrument and Control Engineer

Andre Luiz R Da Silva
Engenheiro De C&A

Muller Antonio Basso Silva

Mr. Elision Carvalho Silva
Gerente Tecnico

Mr. Wagner Silva Sterquino
IFES

Mr. M. Robert Skrokov

Stephen W. Soetemans

Mr. Andre Ribeiro De Souza

Mr. Gabriel Tourinho
De Souza

Adalberto Souza
De Andrade
Engeneiro Especialista
Leonardo Spricigo

Mr. Wayne Staggs
Senior Design Specialist
CH2MHill

Mr. Chad D. Standley
Joel R. Steinmetz
I & C Engineer

Mr. Michael Stinson
Citizen Gas

Dr. Thomas M. Stout
Conslnt

Mr. Syed Sultan
VP-Engineering
ISE-Magtech

Mr. Dexiang Sun
Senior Process Control Engineer
Is it time to join a committee?

Serving on a committee is a great way to help our division or to help your local section—and to sharpen your leadership skills. Divisions and sections have lots of committees and positions that need smart, energetic volunteers like you. Surely, you’ll find a good fit!

Just let any of our leaders know the area in which you are interested. They’ll give you the information you need to make your decision. Volunteering is a great way to learn valuable skills while you network with other motivated automation professionals. Our division benefits, your section benefits, and you do too!

Insurance benefits for ISA members

Did you know that your ISA member benefits also include personal benefits? Discounted insurance programs are one way ISA adds value to your membership. If you’re looking at insurance programs, be sure to check out these opportunities.

Automobile Insurance – Special discounts for ISA members on automobile insurance from GEICO. Call for free, no-obligation rate quotes, 1-800-368-2734. Available in the US only.

Group Insurance Programs – Competitive rates on the following insurance plans, available in the US only.

- Term Life
- Accidental Death and Dismemberment
- Catastrophic or Excess Major Medical
- Medicare Supplement
- Disability Income
- Member Assistance
- Cancer Expense

Contact Selman & Company, the plan administrator, at 1-800-556-7614 or click here to access their website.

The next time you need insurance, check out the competitive rates you can get as an ISA member!

Do you qualify for ISA Life Member Grade?

You might! If you are a Regular Member, Senior Member, or Fellow Member who has been a member of ISA in good standing for a total of at least 25 years, and whose combined age and years of ISA membership equal or exceed the sum of 90—then, submit your application today!

The Life Member Grade is ISA’s way of recognizing the many years a member has devoted to the Society. Life Members are exempt from paying dues, yet still get to enjoy all the benefits of membership.

To apply, visit www.isa.org/lifememeber and complete and submit the online form or contact Member and Customer Services at +1 919-549-8411 or info@isa.org and request a “Life Member Grade Application.”
Recruit new ISA members and get rewarded!

The ISA Rewards for Recruiting Program

YOU are ISA’s best source for recruiting new members. Introduce your colleagues to ISA! They’ll appreciate your contribution to their career development when they learn the benefits of ISA membership.

What better gift could you give them than the latest in technical information and opportunities to network with other motivated automation and control professionals? Use your local connections to expand your section’s network of professionals today—and claim your reward!

How the Rewards for Recruiting Program Works

ISA’s Rewards for Recruiting Program recognizes your contribution in recruiting new ISA members.

• Recruit one new ISA member and ISA will send you a $25 gift certificate good toward any ISA product or training course registration

• Recruit five or more new ISA members over the course of one program year (July through June) and receive a $100 gift certificate good toward any ISA product or training course registration

Each of these rewards can be claimed just once per program year.

To get credit for recruiting, make sure your name and member number appear in the Rewards for Recruiting box in the upper right corner of the new member’s enrollment form.

Note: This program does not apply to student memberships

For details go to: www.isa.org/rewards.

Restrictions apply.

Don’t miss your chance to earn your reward. Introduce someone to the benefits of ISA membership today!

Setting the Standard for Automation™