Italy Section

The International Society of Automation (ISA)

Cyber Security for Industrial Control and Automation Systems

ISA ITALY SECTION 20th JUNE 2018

Venue: MIOGE - Moscow Crocus Expo Russia

www.aisisa.it

"While no one can prevent industrial cyber attacks from occurring, you can significantly reduce your risk by understanding your vulnerabilities and minimizing the consequences."

Our conference is focused on raising awareness of Industrial Cyber Security, and preventing or mitigating the damage that a cyber attack will have on your Control and Automation Systems used throughout manufacturing, utility and transportation sectors.

Without implementing the proper preventative measures, an industrial cyber attack could contribute to equipment failure or impairment, production loss or regulatory violations, with possible negative impacts on the environment or public welfare. Incidents of attacks on these critical network infrastructure and control systems highlight vulnerabilities in the essential infrastructure of our society such as the smart grid, which could become more of a focus for cybercriminals in the coming years.

Our conference is targeted at the Industrial Control Sector that affects all manufacturing industry to a high degree as well as the national utility and transportation providers. These are systems that cannot afford to be shut down immediately when they come under cyber attack.

The conference aims to:

- Reveal how to detect cyber threats, and mitigate the risks and exposure to your plant systems and networks
- Introduce proven industrial control systems security standards and practices and demonstrate how to apply them
- Showcase best practices utilized in various industries and highlight peer experiences and lessons learned

As well as threats from external sources you also need to take steps to protect your Control and Automation Systems from internal threats which can cripple a company for days, weeks or even months.

Please send your paper to event@baggi.com
no later than 31.05.2018

Corporate Sponsors

To be defined:

Some Important Information regarding Cyber Security & Control & Automation Systems

There are many publicly available reports on cybersecurity attacks, and there has been a common theme throughout these for the past few years, exemplified by statistics from Verizon's breach reports of 2012 - 2013:

Ninety seven percent were avoidable with basic or intermediate security controls (2012).

- Ninety two percent were discovered by a third party (2012).
- Twenty percent of network intrusions involved manufacturing, transportation, & utilities (2013).
- Seventy six percent of network intrusions exploited weak or stolen credentials (2013).

When we talk about cyber threats, the natural tendency for all of us has been to think of identity theft and other cyber attacks affecting traditional information technology (IT) systems -- and not cyber threats to operational technology (OT) systems affecting our nation's critical infrastructure (e.g. systems that control the operations of our manufacturing plants, chemical plants, water/ utilities, power, transportation etc.).

Cisco 2014 Annual Security Report: using their FireAMP software, 28 Million Network Connects are evaluated every day and 50,000 network intrusions are detected

In the US the threats are now taken very seriously and in February 2013 President Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" which aims to protect critical infrastructure from cybersecurity risk was issued. A draft framework was issued for public comment, with the final version released in February 2014 by NIST (National Institute of Standards and Technology).

The report indicates that in 75 percent of attacks it took just minutes to compromise an organization. The definition of "critical infrastructure" in the executive order is: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"

Combining technical countermeasures with policies, procedures and organizational changes, and following the ISA99 standard, gives companies the same robustness for their process control networks as they have for their office networks.

ISA Italy Section

Who should attend:

- **Control & Automation Engineers / Managers** in Manufacturing, Transportation and Utilities
- Control System **Integrators** and Application Support Personnel
- **Consultants, Vendors and Designers** working in the Industrial Control & Automation Industry
- **IT Security Management** professionals working with control and automation systems
- Operational Technology / **PCS / ICS / SCADA Professionals**
- **System Administrators** working with industrial control environments
- **Business Continuity** specialists
- **Risk Management / Compliance / Auditors** dealing with industrial control & automation systems
- **Corporate Security** personnel with applications in utilities, transportation or manufacturing industries
- **Facility management** professionals
- Government officials, academics, consultants, vendors and everyone with an interest in security and control practices
- Everyone required to learn about state of the art security & control practices, their practical implementations in securing their enterprise and its industrial requirements The Industries, Utilities and Transportation applications which would benefit from this conference include all manufacturing with special emphasis on:

Industrial Sectors
Pharmaceutical / Bio-Pharma, Medical Device
Chemical Oil & Gas Production and Storage
Food & Beverage, Electronics

Critical Utilities / Transportation
Gas / Electricity networks
Water Purification / Waste Water treatment
Airports / Railways / Harbours / Ports / Tunnels / Bridges

If your career is in Automation or Measurement and Control, then the Ireland Section of ISA, which caters for the technical, scientific and educational needs of its members, can help you. As automation professionals you can further your career goals by availing of training and networking opportunities, and benefit from improved technical and leadership skills.

Founded in 1945, the International Society of Automation (www.isa.org) is a leading, global, nonprofit organization that is setting the standard for automation by helping over 30,000 worldwide members and other professionals solve difficult technical problems, while enhancing their leadership and personal career capabilities. Based in Research Triangle Park, North Carolina, ISA develops standards, certifies industry professionals, provides education and training, publishes books and technical articles, and hosts conferences and exhibitions for automation professionals. ISA is the founding sponsor of the Automation Federation (www.automationfederation.org).

Our Mission is to Enable our members, including world-wide subject matter experts, automation suppliers, and end-users, to work together to develop and deliver the highest quality, unbiased automation information, including standards, training, publications, and certifications.

ISA sets the standard for automation by enabling automation professionals across the world to work together for the benefit of all

BOOKING FORM

Name(s)	
Contact No.	
Email	
ISA Membership No (if applicable)	
Company	
Company Address	

Golden sponsors € 5000

Basic sponsors € 1000

Please find enclosed my paper for approval

Please find enclosed a cheque for the above amount: _____

Please invoice me using the following PO No: _____

Signed: _____ Date: _____

Please send the returned form with cheque payable to:

ISA Italy Section
Viale Campania 31
20133 Milan ITALY

You may also email the completed form with your PO number to: event@baggi.com