



Water / Wastewater Industry Division

Setting the Standard for Automation™

Calendar of WWID Events

Jan-Dec 2022	WWID Connect Live virtual events Dates TBD
Jan 31, 2022	WWID Scholarship Applications Due
Jun 12-15, 2022	AWWAACE 2022
Summer 2022	2022 Energy and Water Automation Conference (EWAC) – Dates TBD
Oct 8-12, 2022	WEF WEFTEC 2022 (includes WEF LIFT Challenge (2022))

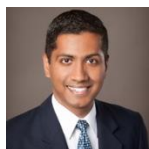
In this Issue:

- 1 Director's Welcome
- 1 Newsletter Editor's Welcome
- 3 Director-elect's Welcome
- 3 Please welcome our incoming 2022 WWID Board of Directors
- 4 Spotlight on the WWID LinkedIn group
- 4 Longtime WWID Volunteer wins ISA Standards Leader of the Year Award
- 5 ISA Announces Free Year of Membership for New Grads
- 5 ISA & WWID to continue to provide virtual programming in 2022
- 6 ISA WWID supports the 2022 LIFT Intelligent Water Systems Challenge
- 7 ISA WWID was at WEFTEC 2021 to present "Digital Solutions Session with ISA"
- 7 Looking Back on 2021 – by Manoj Yegnaraman & Hasan Ajami
- 8 Thank you to our 2021 WWID Volunteers
- 9 Tech. Article – A Practical approach to applying the IEC-62443 cybersecurity standards
- 13 Tech Article – New York Lawmakers reference ISA/IEC-62443 in New Proposed Bill
- 14 FM Approvals Accredited by Standards Council of Canada for ISASecure Program
- 15 IEC Designates ISA/IEC-62443 as a Horizontal Standard
- 17 ISA112 SCADA Systems Standards Update
- 18 The New Normal – Steve Mustard, 2021 ISA society president
- 19 Call for Articles
- 20 WWID Contacts

Newsletter December 2021

Director's Welcome

Manoj Yegnaraman, Carollo Engineers Inc.



Welcome to our December 2021 edition of our WWID Newsletter.

I'd like to start with a question this time - **Are there any critical automation challenges and solutions that you think we should be aware of/focus in these newsletters/discuss as a group, for our Water Wastewater (W/WW) Industry?** If yes, please send an email to me or anyone within our WWID Board (see last page of this newsletter for our contact information).

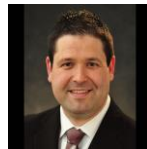
The goal of every W/WW automation professional is to provide services and solutions that has the highest level of quality, reliability, and efficiency on their jobs/projects. Our goal is for WWID to be the platform to enable our members to provide such high level of care on their tasks.

It takes a significant amount of effort from multiple entities and individuals in order to ensure that our residents receive the best water and wastewater service. These include our end users/owners, vendors, contractors, integrators, programmers, consulting engineers, SCADA/OT experts, and other automation service providers in W/WW industry. All of you reading this article have, or are currently contributing towards such efforts, and we thank you for your service and support.

This substantial planning and efforts, combined with the awareness of critical issues and ... **(continued on page 2)**

Newsletter Editor's Welcome

Graham Nasby, City of Guelph Water Services



Welcome to our December 2021 newsletter. In this issue, we will bring you up to date on what the WWID has been up to during the past year, and provide you with updates about ISA's overall cybersecurity strategy when it comes to the ISA/IEC-62443 family of cybersecurity standards.

The year 2021 was a challenging one due to our seemingly never-ending global pandemic, but the WWID was still able to provide programming for both our members and the wider municipal automation community. This included both webinars, online discussion boards, virtual meetings, our newly deployed ISA Connect online community, our website at www.isawaterwastewater.com, and this very newsletter. We also managed to grow our volunteer board of directors this year, with two more new volunteers joining the team.

I would like to thank our division director Manoj Yegnaraman and our director-elect Hassan Ajami for their ongoing drive to provide virtual programming during the past year. Using these tools, we have been able to stay connected with our membership and renew some of our long-standing collaborations with other industry groups. The WWID has just recently signed a memorandum of understanding (MOU) with the Water Environment Federation (WEF) to support the 2022 LIFT Intelligent Water Challenge. It is a pleasure to be involved in this annual event once again. Read more about it in the news article by Don Dickinson. **(continued on page 2)**

WWID Director's Message (continued from Page 1)

... associated solutions would allow us to provide an enhanced level of service to our residents/users now and in the future.

I look forward to hearing from many of you on this topic.

Regarding other division activities, we have submitted our 2021 Annual WWID Report and our 2022 WWID Business plan. These can be found in our WWID Division library under ISA Connect. One of the key highlights in our 2022 Business plan is to execute Memorandums of Understanding (MOUs) with the two leading Water/Wastewater based non-profit technical and education organizations – **Water Environment Federation (WEF)** and the **American Water Works Association (AWWA)**. The WWID will work with WEF and AWWA to participate in each other's annual conferences this year (**2022 WEFTEC, 2022 ACE and 2022 EWAC**).

Finally, I take this opportunity to thank you all for your support and service towards the W/WW Industry and our Division here at ISA. My best wishes for a Happy New Year 2022!

Manoj Yegnaraman, PE

Director, ISA WWID

Associate Vice President, Carollo Engineers Inc.

myegnaraman@carollo.com



WATER
OUR FOCUS
OUR BUSINESS
OUR PASSION

carollo
Engineers...Working Wonders With Water®

Dallas office: 972.239.9949 | carollo.com

Newsletter Editor's Welcome (continued from Page 1)

...This issue also provides a report on what ISA is doing to make it easier to apply the ISA/IEC-62443 series of cybersecurity standards for industrial control systems. In his article "A Practical Approach to Adopting the IEC 62443 Series of Cybersecurity Standards", Felipe Sabino Costa of the ISA Global Cybersecurity Alliance provides a top-down overview of how the standards can be applied to a typical industrial control system, such as a water/wastewater utility's SCADA system. The article has been deliberately written at a high level so that it can be easily read by a member of senior management, without getting lost in the many technical details are typically associated with keeping a system secure. The article also provides an overview of how concepts like risk analysis, defense in depth, security levels, and separating the system into multiple zones are essential ingredients for keeping a control system secure. The article concludes by discussing factor such as active monitoring, situational awareness, and keeping the supply chain secure.

This is then followed by three update articles about how the series of ISA/IEC-62443 standards are being applied and used. In the state of New York (USA), a newly proposed cybersecurity bill is directly referencing the risk management framework in ISA/IEC-62443. The ISA's "ISASecure" program is starting to gain traction, with the Standards Council of Canada (in Canada) recently accrediting FM Approvals to issue certificates of conformance for products meeting requirements outlined in the ISA/IEC-62443-2 and ISA/IEC_62443-3 standards. Lastly the IEC (International Electrotechnical Commission) has recently designated the ISA/IEC-62443 series of standards as a "Horizontal Standard", meaning that is now considered a base standard that applies to a multitude of industries. Indeed, the ISA/IEC-62443 series of cybersecurity standards continue to gain traction in all industries, including our very own municipal water/wastewater sector.

Our newsletter concludes with a swan song from our going 2021 ISA Society President, Steve Mustard. Steve reflects on the past year of propelling ISA forward in the face of a global pandemic, the hiring of a new ISA Executive Director, and the continued evolution of cybersecurity threats in the marketplace.

I am very much looking forward to 2022 and opportunities that it will bring for all of us.

Regards,

Graham Nasby, P.Eng.

WWID Newsletter Editor

graham.nasby@guelph.ca

WELCOME

Director Elect's Welcome

Hassan Ajami, PCI-Vetrix



Wintertime is upon us here in the Midwest of the United States. Usually, this time of year brings family gatherings for the holidays, vacations off to warmer climates, or having fun in the snow. Unfortunately, Covid had other ideas with the resurgence of infections and a new strain. All we can do is keep ourselves and our loved ones safe.

On a professional note, the talk of the industry has been cybersecurity and how to protect critical systems from hackers. Water systems are one of the most critical assets that we have, directly effecting the health of all peoples. There are threats and nefarious actors out there that we, as an industry, must protect against.

The Water/Wastewater sector in the USA is expected to receive federal guidelines and requirements for securing systems against attack. WWID is working within ISA and with other industry groups to understand the new federal requirements and their impacts on our industry. We will keep our membership updated throughout the year through ISA Connect, LinkedIn and ConnectLive technical discussions. Cybersecurity will also be a main focus of our EWAC webinars later this year.

We are working on some changes within WWID this year. Our plan is to expand our board by creating subcommittees who can focus on topic areas as they relate to the W/WW industry.

We call upon our members to volunteer and participate in these committees, as well as the general industry discussions on ISA Connect. It is through open dialog and discussions that we share information and learn. Keep an eye on your email for announcements of upcoming virtual events and volunteer opportunities.

As we start the new year and embark on our new year resolutions, I ask you all to protect yourselves and your loved ones.

Warmest Regards,

Hassan Ajami, PE, CAP

2021-2022 Director-Elect, ISA WWID

2021-2022 General Chair, ISA EWAC

Vice President / Lead Technical Officer

hajami@pci-vetrix.com

WWID NEWS

Please welcome our incoming 2022 WWID Board of Directors

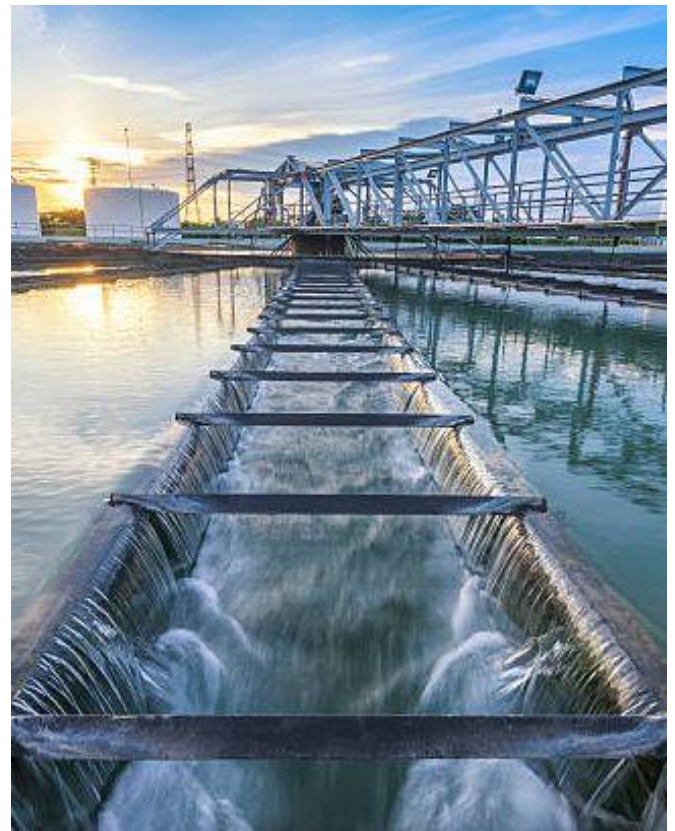
From the WWID committee

We are pleased to announce the member of our incoming 2022 Board for the ISA Water/Wastewater Division.

2022 WWID Board

- Manoj Yegnaraman – Director
- Hassan Ajami – Conference Chair, Director-Elect
- Mike Briscoe – Secretary
- Don Dickinson – Past Director, ISA Connect, LinkedIn
- Joe Provenzano – Program Chair
- Colleen Goldborough – Membership Chair
- Graham Nasby – Newsletter Editor & Website Editor
- Kevin Patel – Scholarship Chair, Asst. Newsletter Editor
- Pavol Segedy – Honors/Awards, Section-Division Liaison
- David Hobart – Committee Member
- Steve Valdez – Committee Member
- Jason Hamlin – Committee Member

Please welcome our new incoming 2022 WWID Board!



WWID NEWS

WWID LinkedIn Group – Spotlight

From Don Dickinson, WWID LinkedIn Coordinator

Since 2010, the ISA Water/Wastewater division has had a presence on the LinkedIn Platform. If you have yet visited the WWID LinkedIn group, take a look at this address:

<https://www.linkedin.com/groups/2031271>

OR

Log into www.linkedin.com and search for “ISA Water & Wastewater Industries Division”

On our LinkedIn group you will find a wide variety of technical posts, discussion items, and announcements for the municipal water/wastewater sector. Currently the group has over 2053 members and membership is open to all interested individuals. Our WWID LinkedIn group is moderated Don Dickinson (me!)

Here are the WWID LinkedIn group guidelines, which are automatically sent to all new members of the group:

Welcome to the ISA WWID LinkedIn Group!

Your interest and participation are welcomed.

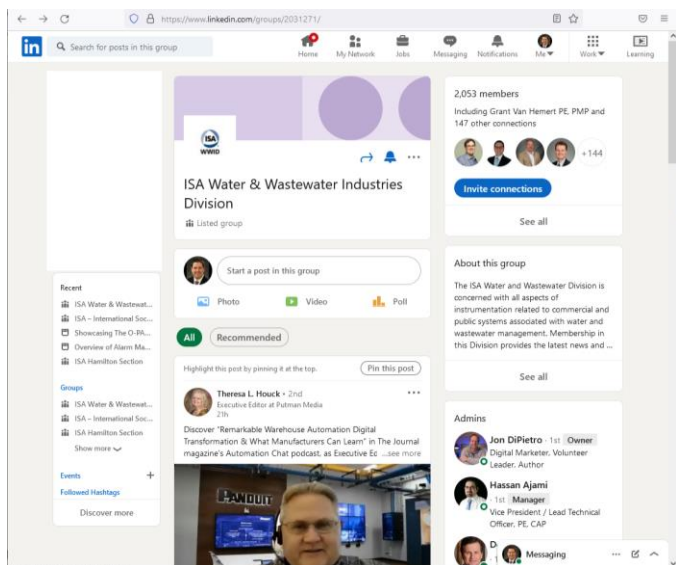
Please note this group is a professional platform intended for sharing content of value relating to the application of automation and advanced technologies in the water sector. It is not intended for the promotion of commercial products or services.

By joining this group, you agree to the following simple rules:

- Be supportive of your fellow members
- Bring value to the discussions
- Do not post commercial content unless it brings significant or meaningful value to fellow members

Questions? E-mail Don Dickinson, ddickinson@phoenixcontact.com

Again, welcome to our group of water professionals from around the world.



WWID NEWS

Graham Nasby receives 2021 ISA society-level Standards Excellence Award

By Pavol Segedy, WWID Honors and Awards Chair

The ISA Water/Wastewater Division is pleased to report that long-time WWID volunteer Graham Nasby has received the 2021 society-level “Standards Excellence” award from the ISA. Graham has been on several standards committees, including ISA18 (alarm management), ISA101 (HMI), ISA99 (cybersecurity), and ISA112 (SCADA systems). Since its inception in 2016, Graham has been the co-chair of the ISA112 SCADA systems committee.



The award, for Standards Leader of the Year, is given out annually “recognizes an ISA standards committee member for exceptional efforts in organization, development and/or administration to further the development of ISA standards and for services to advance the mission of the Society.” The award recognizes “Exceptional leadership and/or technical knowledge essential to the organization, development and/or administration of ISA standards to advance the mission of the Society.”

Graham has been active with the ISA Water/Wastewater division since 2009, including leading our ISA Water/Wastewater Symposium in 2012-2013, Director 2013-2015 to 2015. Graham is currently editor of the WWID newsletter.



WWID NEWS

ISA Student members to receive 1-year Free Professional Membership on Graduation

From ISA News release

As part of its ongoing efforts to support the next generation of automation professionals, the ISA's membership committee has set up a new program where ISA student members will receive a free year of membership when they graduate from school.

Here is some of the marketing materials being provided by ISA to support his new membership drive at <https://programs.isa.org/student-to-professional>

CONGRATULATIONS! Graduation is a very important milestone. Your career began with your ISA Student membership. Take the next step.

An ISA professional membership can unlock even more opportunity to start or learn about an automation career. To help you transition, ISA is offering a free year of professional membership for the first year after your graduation. It is a significant upgrade from your student status. You already made a good start, keep that momentum going.

Join us as we build a better world through automation!




Recent or soon-to-be graduates,
Take the next step in your career with a FREE professional ISA membership!

Keep the momentum going with your automation career. All you have to do is sign up!

There are significant feature upgrades for a professional membership beyond your student member status. With a professional membership, you can:

- Participate in technical conversations on **ISA Connect**
- Access **standards** and other technical resources
- Make your mark as a **YP** (ISA Young Professionals)
- Network in your local area through a **Geographic Section**
- Share knowledge with **Technical Divisions**
- Hone leadership skills by **volunteering**
- Get **Discounts** on training, books and certifications

You are only one step away from a professional membership with ISA. Visit: <https://programs.isa.org/student-to-professional>.

programs.isa.org/student-to-professional

WWID WEBINARS

ISA & WWID Continue to Provide Virtual Events and Plan for 2022 and Beyond

From the WWID program committee

With the unprecedented cancellations of in-person events due to the COVID-19 pandemic, our industry has had to pivot to providing online events. Both the WWID and ISA as a whole, has been actively working to adapt to this new format.

For the WWID, this has meant providing a series of technical webinars for our members. We organized 4 webinars in 2020, 3 days of multiple webinars in 2021, and have already started planning our 2022 events. The Webinars are free, so we encourage you to register and attend future events. Keep an eye on the ISA website for more announcements.

In addition to WWID-associated events, the ISA has also embarked on providing a wide range online programming:

These include:

- Virtual Conferences
- Cybersecurity Series Webinars
- IIOT & Smart Manufacturing Webinars
- Digital Transformation Webinars
- Process Control and Instrumentation Webinars
- Division-Specific Webinars
- ISA Connect Live Events

Please visit www.isa.org/virtualevents for more information.

Setting the Standard for Automation™

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.**

61284

WWID NEWS**ISA WWID supports the 2022 LIFT
Intelligent Water Systems Challenge...
You can too!**

by Don Dickinson

Now is the time to consider your participation in the 2022 LIFT Intelligent Water Systems Challenge. The Leaders Innovation Forum for Technology (LIFT), a joint effort of the Water Research Foundation (WRF) and the Water Environment Federation (WEF) is holding its fourth annual, Intelligent Water Systems Challenge. The goal of the Challenge is to foster the adoption of smart water technologies by showcasing the use of intelligent water systems to effectively leverage data for better decision-making in operating increasingly complex water treatment, collection, and distribution systems.

The Challenge gives students, professionals, and technology enthusiasts the opportunity to showcase their talents and innovation in a team environment by demonstrating the value of using advanced sensing and/or data technology to address real-world challenges faced by utilities. If you have a specific challenge and a potential solution, you and your team are encouraged to participate.

As with each year of the challenge, the ISA Water and Wastewater Industries Division is an active supporter and encourages its members to participate. After all, ISA is committed to helping professionals in the water and wastewater – and now, stormwater community improve efficiency and operational performance through the application of automation, instrumentation, and advanced technologies. The LIFT Intelligent Water Systems Challenge is the perfect opportunity to share ISA's vision of creating a better world through automation. Please consider participating in the 2022 LIFT Intelligent Water Systems Challenge. Important dates and links to more information are provided below.

2022 LIFT Intelligent Water Systems Challenge

<https://www.waterrf.org/news/2022-intelligent-water-systems-challenge>

Important Dates to RememberTeam Registration Submission

Deadline: April 11, 2022

[> Submit your Team Registration](#)Challenge Plan Submission**Deadline: May 16, 2022**Challenge Solution Submission**Deadline: August 15, 2022**Finalist Presentations at WEFTEC 2022**October 10, 2022****About the Water Research Foundation (WRF)**

The Water Research Foundation is a US-based 501(c)3 non-profit organization that was officially formed in January 2018 after the merger of the Water Environment & Reuse Foundation and Water Research Foundation. The merged Foundation is the leading water research organization, funding research, pilot projects, and technology demonstrations that maximize the value of all water, including wastewater, stormwater, drinking water, and recycled water. Learn more at www.werf.org or www.waterrf.org.

About the Water Environment Federation (WEF)

The Water Environment Federation (WEF) is a not-for-profit technical and educational organization of 35,000 individual members and 75 affiliated Member Associations representing water quality professionals around the world. Since 1928, WEF and its members have protected public health and the environment. As a global water sector leader, our mission is to connect water professionals; enrich the expertise of water professionals; increase the awareness of the impact and value of water; and provide a platform for water sector innovation. To learn more, visit www.wef.org.

About the ISA Water/Wastewater Division

The ISA Water / Wastewater Industry Division (WWID) is concerned with all aspects of instrumentation and automated-control related to commercial and public systems associated with water and wastewater management. Membership in the WWID provides the latest news and information relating to instrumentation and control systems in water and wastewater management, including water processing and distribution, as well as wastewater collection and treatment. The division actively supports ISA conferences and events that provide presentations and published proceedings of interest to the municipal water/wastewater sector. The division also publishes a quarterly newsletter and has a scholarship program to encourage young people to pursue careers in the water/wastewater automation, instrumentation, and SCADA field. For more information see www.isa.org/wwid/ or www.isawaterwastewater.com



WEF & ISA COLLABORATION

ISA WWID holds “Digital Solutions Session with ISA” at WEFTEC 2021

By WWID Committee

The WWID was at the WEFTEC 2021 conference in Chicago and online as part of a technical session called “Digital Solutions with ISA”. Held as part of the WEFTEC Innovation Pavilion, the event took place on Oct 20, 2021 as part the mornings activities. Since the Innovation Pavilion was on the Exhibition Floor, attendees were able to attend with both a full WEFTEC pass and the special Expo-Only pass. The Expo-Only pass was free to WEF members and only \$75 for non-members.

The “Digital Solutions Session with ISA” was held on Wednesday, October 20, 2021 at 9:00 AM – 9:30 AM CT at Booth 4817 in South Hall A, of Chicago’s McCormick Conference Centre.

EVENT INFORMATION

Title: All Electric Society (AES) and the Water Sector

Description: The greatest challenges facing humanity – climate change and sustainable development – can be met from a technical perspective by the All Electric Society. AES is a world in which affordable electrical energy generated from renewable sources is available on a virtually unlimited basis as the main form of energy. However, AES is more than just decarbonization and the reduction of greenhouse gases. It also involves energy conservation through increased efficiency, and energy recovery/production to reduce operating costs and enhance asset management. The key to realizing this world is the comprehensive electrification, networking, and automation of all sectors of the economy and infrastructure to provide a cleaner, healthier, and more prosperous future for all. This presentation will introduce the goals and tenants of AES that provide a roadmap for building the resilience and sustainable water infrastructure of the future.

SPEAKERS

Ajami, Hassan and Don Dickinson
ISA Water and Wastewater Industry Division



WWID NEWS

Looking Back to 2021 with WWID

By Manoj Yegnaraman & Hassan Ajami

Though in the midst of a global pandemic, the WWID was able to have a productive year in 2021 with a wide range of online events and programming. We have been fortunate to have a dedicated group of volunteers to continued the WWID’s mission of outreach and promoting technical excellence for automation in the municipal water/wastewater sector.

Some of the highlights of this past year’s 2021 WWID activities have included:

1. We had an active Division leadership, consisting of about 14 members. We added several new Division leaders in 2021.
2. Hassan Ajami (our Director-Elect) served as the General Chair for the 2021 ISA EWAC webinar series. We successfully conducted 2-hr sessions of multiple webinars on three different days this year..
3. We published 4 ISA WWID newsletters in 2021, similar to past years.
4. We signed an MOU (memorandum of understanding) with Water Environment Federation (WEF) to support the activities of each organization.
5. We had our own ISA WWID scholarship program similar to previous years. We provided two scholarships.
6. We gave two awards to our longtime volunteers (ISA Member of the Year Award to Graham Nasby and ISA Service Award to Joe Provenzano)
7. We conducted three online ConnectLive events with our WWID membership and participated in several technical forums.
8. We had representation in several ISA-conducted leader training.
9. Our Division participated in the Spring Leaders zoom call and several calls with Executive Board
10. We have been in touch with our Members via emails from our Membership chair.
11. We have been active outside the ISA connect page as well with efforts towards our external website, and in social media.
12. Several of our Division members are active on the ISA112 SCADA Systems standards committee, with longtime WWID volunteer Graham Nasby being the Co-chair of ISA112

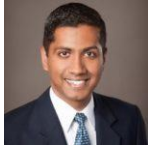
Plus, we have a strong volunteer board going into 2022. We are very much looking forward to the year ahead!

WWID NEWS

Thank you to our 2021 Board Volunteers

By WWID Committee

The WWID would like to thank our volunteer board members from last year for their service. Many will be continuing in the coming year as part of our 2022 volunteer board.



2021-2022 Director, WWID

Manoj Yegnaraman, PE
Carollo Engineers Inc.
Dallas, Texas, USA



2021-2022 Conference Chair

2021-2022 Director-Elect

Hassan Ajami, PE, CAP
PCI-Vertex
Detroit, Michigan, USA



Secretary

Mike Briscoe
Signature Automation
Dallas, Texas, USA



Past Director

& ISA Connect Chair

Don Dickinson
Phoenix Contact USA
Cary, North Carolina, USA



Program Chair

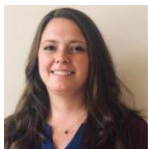
Joe Provenzano
KPRO Engineering Services
Naugatuck, Connecticut, USA



2021-2022 Asst. Conference Chair

2021-2022 Director-elect-elect

Jon Grant, PE, CISSP, CISM
DirectDefense
Boston, Massachusetts, USA



Membership Chair

Colleen Goldsborough
United Electric Supply
Lancaster, Pennsylvania, USA



Asst. Membership Chair

Juliana Wafer, PE
Signature Automation
San Antonio, Texas, USA



Newsletter Editor

& Co-Chair, ISA112 SCADA Systems Standards Committee

Graham Nasby, P.Eng, PMP, CAP
City of Guelph Water Services
Guelph, Ontario, Canada



Scholarship Committee Chair

& Asst. Newsletter Editor

Kevin Patel, PE, MBA
Signature Automation
Dallas, Texas, USA



Honors and Awards Chair

& Section-Division Liaison

Pavol Segedy, PE
HDR Inc.
Raleigh, North Carolina, USA



Committee Member

David Hobart, P.Eng, CAP
Hobart Automation Engineering
Portland, Maine, USA



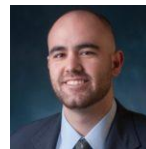
Committee Member

Steve Valdez
General Electric
Paramus, New Jersey, USA



Committee Member

Jason Hamlin
Instrulogic



Committee Member

Chris Hidalgo
Signature Automation
Dallas, Texas, USA

TECHNICAL ARTICLE

A Practical Approach to Adopting the IEC 62443 Series of Cybersecurity Standards

By Felipe Sabino Costa, ISA Global Cybersecurity Alliance

From cybersecurity strategy to technical projects, many companies struggle with how to put theory into practice for industrial control systems (ICS). Although it is difficult to completely cover the full range of the IEC 62443 standards and the related literature, this blog summarizes the key points for the IEC 62443 standards and provides some practical recommendations for Cybersecurity Management System (CSMS) development. This blog will also consider the importance of product and company certifications to support asset owners in their journey towards IEC 62443 compliance.

I. Executive Summary

This blog considers different aspects of how the IEC 62443 standard provides a holistic and wide-ranging approach to securing industrial control systems. The first step before creating a CSMS is to have the management team's support to ensure the CSMS will have sufficient financial and organizational support to implement necessary actions. Afterwards, a risk assessment should be performed to understand the company risks, respective security levels (SL), and critical assets.

Once the risk and security factors are defined, it is necessary to develop countermeasures to bring the SuC to a level of risk that the company is willing to accept. This comprises of different steps and techniques, such as defense in depth and the creation of zones and conduits to provide different levels of protection.

A further step is the security monitoring for enhancing network visibility and planning how to respond to incidents. Finally, the human factor and supply chain management aspects should also be considered throughout the CSMS development process.

II. Introduction

In general, many companies struggle with how to transform theory into practical actions. These challenges range from how to gain the executives' buy-in for cybersecurity strategy, to which technology will better fit their needs, and what the most relevant risks are for technical projects. This blog provides some guidance on how to perform key actions recommended by the IEC 62443 standards. Although we are just scratching the surface of this extensive work, this blog may help technicians and executives to improve their understanding of the standard recommendations.[5][6]

The series of IEC 62443 standards provide a holistic and wide-ranging approach to securing industrial control systems (ICS). These standards are holistic because they embrace the different structural aspects of security strategy, defined by the International Electrotechnical Commission (IEC) as **People, Process, and Technology**. In addition, these standards are

wide-ranging because they cover a lot of ground providing internal and external recommendations to asset owners, supply chain management, and product development. For asset owners, the IEC 62443 standard recommends the creation of a Cybersecurity Management System (CSMS) that includes analyzing, addressing, monitoring, and improving the system against risks, according to the company's risk appetite. For supply chain management, the specifications recommend security development throughout the product lifecycle. It starts from aspects of secure by design and extends to product manufacturing. The goal is to develop and maintain a reasonable level of security in the products and systems the solution provider offers during the product life cycle.[1][2][3][4]

The cybersecurity management system (CSMS) proposed by the IEC 62443 standard has six main elements:

1. *Initiating the CSMS program* (to provide the information that is required to get support from management).
2. *High-level risk assessment* (identifying and assessing the priority of risks).
3. *Detailed risk assessment* (detailed technical assessment of vulnerabilities).
4. *Establish security, organization, and awareness policies*.
5. *Selecting and implementing countermeasures* (to lower risk to the organization).
6. *Maintaining the CSMS* (to ensure the CSMS remains effective and supports the organization's goals).[4]

III. Management Support

Before starting to consider technical aspects, the first important recommendation from the IEC 62443 standard is to consider the business rationale and obtain support from management. To obtain support, the company needs to have a clear understanding of the systems, subsystems, and respective components that are essential or critical to operation and safety. Once this has been established, it will be easier to communicate to management the possible consequences if any component is impacted.[4]

A. Critical Assets

Critical assets include any device that, once compromised, may generate a high financial, health, safety, or environmental impact to an organization. The list of the company's critical assets forms the basis of the risk management analysis and will be used to guide further decisions.[18]

B. Business Rationale

Once the company has identified the critical assets, it is necessary to obtain the management engagement and commitment to invest in the cybersecurity plan that will be developed. Without this support, the plan has a very low chance of success. High-level management should approve and participate in defining the business rationale to ensure the

CSMS will have enough resources and support to deploy the necessary changes to the system and throughout the entire organization. In some cases, it is necessary to create a business case or business rationale, as suggested by the IEC 62443 standard to present to the management team. The business case or business rationale contains a list of the potential threats and the possible consequences to the business with an estimation of the costs annually, as well as the cost of any countermeasures. This will provide a clear overview of the risks and costs for mitigation to acceptable levels, increasing the chances of obtaining support from management.[4][7][8]

IV. Risk Assessment

Once the management team is engaged and committed to supporting the CSMS, it is important to perform a risk assessment. Risk assessment is part of the overall risk management strategy of every company, and it is a mandatory step to create a solid and efficient cybersecurity strategy. It requires correlation and collaboration between many different groups of people within the company. These levels have been defined by the National Institute of Standards and Technology (NIST) at the organization, mission/business processes, and information system (IT and ICS) levels.[11][13]

Risk management aims to assess and understand the different types of risks the company is susceptible to in different areas such as investment, budgeting, legal liability, safety, inventory, and supply chain risks. The focus of this blog will be on the ICS risks, which is generally agreed to pose one of the greatest potential areas of risk.[9][10][12]

To perform a risk assessment of the ICS, it is necessary to define the scope and boundaries of the system that will be assessed, also known as the System under Consideration (SuC). Once the SuC is defined, it is necessary to systematically identify, analyze the threats and vulnerabilities, and prioritize the risks based on their potential consequences. At the same time, it is also important to define asset criticality and dependencies to the operation.[9]

The risk formula is as follows:[1][2][4]

$$Likelihood_{EventOccurring} = Likelihood_{ThreatRealized} \times Likelihood_{VulnerabilityExploited} [1]$$

$$Risk = Likelihood_{EventOccurring} \times Consequence [2]$$

There are two different types of risk assessments applicable to ICS: *high level* and *detailed risk assessments*. As their names suggest, one approach deals primarily with high-level concepts and the other involves a detailed look at the different types of risk. It is common to perform a high-level risk assessment to support the business rationale and business case, with the latter performing a detailed risk assessment to ensure the system has specific countermeasures included in the design.[4][9][10][13][14]

An expected outcome from this step is to be able to form a comprehensive list of critical assets and determine where connectivity is taking place. The assessment should also be able to identify dependencies, determine what the critical risks

are to the operation/safety of these processes, and the appropriate responses to these risks, which include the partition of the system into zones and conduits to mitigate risks to levels the company can accept.[15]

V. Defense in Depth

One of the most common security weaknesses in an ICS is the use of flat networks where there are no internal layers of protection and segregation, allowing all the devices to communicate with each other, even if it is not necessary. This is an undesirable scenario due to different internal and external factors: the facilitation of threats propagation (external factor) and the communication degradation (internal factor), which both result from a lack of control of the information on the network.[30]

To address this type of problem, upon completing the high-level cybersecurity risk assessment, it is necessary to begin the initial partitioning of the SuC. Each partition is called a zone. The concept of zones is detailed in the next section, but it also forms an important part of the broader concept of the defense-in-depth approach.[18]

Defense in depth is a military concept that provides different levels or layers of protection against a potential attacker or intruder trying to hack the SuC. In the context of a network, the result is a different tailored cybersecurity countermeasure deployed throughout the system. Although it is closely linked to technology, defense in depth should also consider other aspects, such as people and processes, as part of its deployment. Some important aspects of defense in depth include, but are not limited to, physical security, ICS network architecture (zones and conduits), ICS network perimeter security (firewalls and jump servers), host or device security, security monitoring, the human element, and vendor management.[10][19]

A. Establishment of Zones and Conduits

A zone, as part of the defense-in-depth strategy, is a subset of the network communication system where all the communication devices share the same security requirement and consequently are equally critical. It is possible to have a zone inside another zone with different security requirements.

Conduits provide inspection and protection of the communications shared by different zones. Zones and conduits can be established in the physical or logical sense. Lastly, conduits include the concept of a *channel*, which is a specific link within the conduit that respects the security level of the conduits where it is inserted. All these concepts are intended to achieve uniformity in protection. It should be noted that each zone is only as secure as its weakest link, therefore, it is highly recommended to isolate the high-risk assets into specific zones.[17]

B. Security Levels

An important part of the defense-in-depth strategy is to consider countermeasures for zones and internal products. Accordingly, the IEC 62443 standard introduces the concept of security levels (SL) that can be applied to zones, conduits, channels, and products. The security level is defined by researching a particular device, and then determining what level of security it should have, depending on its place in the system. The security levels may be classified into four distinct levels 1 to 4, (although the standard also mentions an “open” level 0 that is rarely used):

- Level 1 is a casual exposure
- Level 2 is an intentional attack with low resources
- Level 3 is an intentional attack with moderate resources
- Level 4 is an intentional attack with extensive resources

Once the security level target of a zone is defined, it is necessary to analyze if the devices inside the zone can meet the corresponding security level. If they do not, it is necessary to plan which countermeasures can help reach the SL target. These countermeasures can be technical (e.g., firewall), administrative (e.g., policies and procedures), or physical (e.g., locked doors).[17]

C. Protection of Critical Assets

As discussed in Section II, critical assets are essential to the correct operation of the ICS. Any impact on those assets may have a high financial, health, safety, or environmental impact on an organization. Those assets should always have a high priority in the risk assessment and in the company security strategy.

The criticality assessment is one input for the definition of scope and zone protection. This assessment identifies the level of impact that assets have on the organization. Other assessments, such as CARVER (Criticality, Accessibility, Recuperability), from the U.S. Department of Defense (DoD), aim to identify, from an attacker’s perspective, which targets could cause the largest impact to businesses. Regardless, it is expected that critical assets have higher security levels with proportional countermeasures that adhere to levels the company can accept. This is one of the reasons why the IEC 62443 standard foresees the use of zones inside zones with different security levels.[9][24][35]

D. Device Security

The same concept of security levels (SL) is also applied to products. The IEC 62443-4-2 defines the security requirements for four types of components: software application requirements (SAR), embedded device requirements (EDR), host device requirements (HDR), and network device requirements (NDR). There are also seven different perspectives, defined as foundational requirements (FR) for each type of component, including identification and authentication control (IAC), use control (UC), system integrity (SI), data confidentiality (DC), restricted data flow

(RDF), timely response to events (TRE), and resource availability (RA). These definitions help asset owners simplify technical specifications and the product selection process, ensuring the expected security level is applied to their application, as each security level (SL) has distinct foundational requirements and details that can be tangibly measured and compared.[20]

In order to support an organization’s audit as to whether all of the above foundational requirements were really deployed on the devices, there are different laboratories, such as ISA Secure, that can certify products that satisfy the requirements of IEC 62443-4-2. These laboratories simplify the selection process for the asset owner, as all they need to do is determine the level of security required and select a certified product that meets that requirement. Consequently, all security features that the organization needs to satisfy the security requirements for the defined SL will be available.[21]

This component level security assurance adds another layer of protection to the system as part of a defense-in-depth strategy. This is known as hardening, and facilitates security level zone protection.[22][23]

VI. Security Monitoring for Enhancing Visibility

According to the U.S. Department of Homeland Security, in 2016, the most common threat was “unknown.” As it was only possible to manage what is visible, most incidents could not be investigated due to a lack of visibility, making it difficult to identify threats, understand how threats pass through defenses, and determine the steps taken to identify the origin of the attack. This is known as *forensic analysis* and provides important information to asset owners so they can understand how the incident happened and help avoid similar incidents in the future.[36][37][38]

Enhancing visibility requires a proper cybersecurity strategy to continuously monitor the system in order to identify potential threats that passed any defenses that were implemented.[4][24][25][26][27]

The most common solution for monitoring a network is a network intrusion detection system (NIDS), or simply, Intrusion Detection System (IDS). It enhances network visibility through the monitoring of anomalies in network traffic or malicious signatures. Adoption of an IDS facilitates forensic analysis and a response to the incident. To enhance efficiency, any forensic data collected from the IDS and other devices should be synchronized, as this will facilitate proper correlation analysis among the different types of data collected.[10]

It is also necessary to have a proper understanding of how to calculate the number of sensors needed, define where to install them, and determine whether a passive or active topology is most suited to each application. Each one of these aspects has advantages and disadvantages that should be evaluated when selecting a monitoring solution.[39][40]

VII. Response to Incidents

Although network visibility is important, it is more important to respond to the incidents detected, which requires a cybersecurity incident response plan. In short, cybersecurity incident response planning is the preparation for any negative events that may affect the ICS and how to get back to normal as quickly as possible after the incident occurs. Its main elements include planning, incident prevention, detection, containment, remediation, recovery and restoration, and post incident analysis/forensics. It also requires proper communication paths and to assign respective owners who will conduct forensic analysis for each response.[4][24][25][26][27][41]

One current discussion is the use of an intrusion prevention system (IPS) inside the ICS to respond to certain types of incidents. An IPS may use different types of technologies, such as a signature-based detection (which monitors specific events and threats) or anomaly-based detection (which monitors changes in trends) to identify a threat and execute pre-approved responses. Although it may vary case by case, a general recommendation for increasing its effectiveness and minimizing false positives is that if the IPS uses anomaly-based detection, it is to train the IPS and its algorithm offline first (passively). In this manner, the IPS will learn the network patterns and provide some potential answers that can be validated by the security analyst first, increasing its effectiveness. For example, one of the most common types of attack is the denial of service (DoS) that affects the network traffic flow pattern. Due to the deterministic nature of an ICS, these attacks are easily detected and are a good starting point to calibrate the effectiveness of an IPS.[10][31][32]

VIII. Human Factors, Training, and Security Awareness

When it comes to cybersecurity, the human factor should also be considered. This is a wide and complex topic because humans can insert different vulnerabilities into a system. Social engineering and misconfiguration are common examples, independent of the motivation (intentional and unintentional) and their causes (e.g., fatigue or lack of expertise). It is necessary to implement countermeasures to minimize these risks.[28][29]

For this reason, the IEC 62443 standard specifically calls for regular staff training and security awareness to all employees, providing them the information needed to perform their responsibilities in a more secure way, in order to minimize the risks caused by human error.[4]

IX. Supply Chain Management and Support

Another important element that spreads across all previously discussed items is the security of the supply chain and solution providers. Suppliers should provide security throughout the product lifecycle, including support, quality control, validation of performance, and vulnerability responses, among other

aspects. To support conformity with those aspects, the IEC 62443 standard has a specific subsection, IEC 62443-4-1, to specify the requirements for ensuring secure by design throughout the product lifecycle (i.e., building, maintaining, and discontinuing devices). These requirements are generally associated with the support needed for patch management, policies, procedures, and security communications about known vulnerabilities. Similar to the IEC 62443-4-2 standard for product certification, it is possible to certify that a solution provider is following good security management practices and adheres to tangible criteria in the IEC 62443-4-1 standard, simplifying the asset owner's decision-making process.[10][33][34]

X. Conclusion

Although now it is possible to become certified for devices and supply chain according to the IEC 62443 recommendations, asset owners should still consider holistically implementing the IEC 62443 standard. The IEC 62443 standard brings together several important aspects widely discussed by a global community of subject matter experts (SME). Even though this blog considers some important aspects that were presented in a progressive and actionable manner, it is difficult to simplify such an extensive body of information such as the IEC 62443. As a result, it is highly recommended that companies looking to adopt the recommendations of the IEC 62443 standard into their own applications consult certified partners and experts as they embark on their IEC 62443 journey.

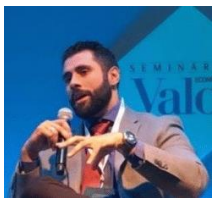
References

1. IEC: "IEC Cyber security Brochure overview," 2018.
2. SH Piggins: "Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security," 2013.
3. M Portella, M Hoeve, F Hwa, et al: "Implementing An Isa/Iec-62443 And ISO/IEC-27001 OT Cyber Security Management System At Dutch DSO Enexis," 2019.
4. ANSI/ISA-62443-2-1: "Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program," 2009.
5. Doan: "Companies Need to Rethink What Cybersecurity Leadership Is," <https://hbr.org/2019/11/companies-need-to-rethink-what-cybersecurity-leadership-is>. Accessed May 17, 2019.
6. J Parenty, JJ Dome: "Sizing Up Your Cyber risks," <https://hbr.org/2019/11/sizing-up-your-cyber-risks>. Accessed May 17, 2019.
7. Elkhannoubi, M Belaisaoui: "Fundamental pillars for an effective cybersecurity strategy," 2015.
8. Winkler I: "7 elements of a successful security awareness program," CSO; <https://www.csoonline.com/article/2133408/network-security-the-7-elements-of-a-successful-security-awareness-program.html>. Accessed July 26, 2021.
9. ISA/IEC-62443-3-2: "Security for Industrial Automation and Control Systems: Security Risk Assessment and System Design," 2015.
10. Homeland Security: "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," 2016.
11. NIST SP 800-82 Rev. 2: "Guide to Industrial Control Systems (ICS) Security."
12. FIPS PUB 200: "Minimum Security Requirements for Federal Information and Information Systems."
13. NIST SP 800-39: "Managing Information Security Risk Organization, Mission, and Information System View," 2011.
14. Ganin P, Quach M, Panwar Z, et al: "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management," 2017.
15. Office of the Secretary of Defense: "Handbook for Self-Assessing Security Vulnerabilities and Risk of Industrial Control Systems on DOD Installations," 2014.
16. NISTIR 8179: "Criticality Analysis Process Model," 2018.
17. "IEC TS 62443-1-1:2009 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models," 2009.
18. Papakonstantinou J, Linnosmaa A, Z Bashir, et al: "Early Combined Safety - Security Defense in Depth Assessment of Complex Systems," 2020.
19. Idaho National Laboratory: "Control Systems Cyber Security: Defense in Depth Strategies," 2006.

20. ISA/ANSI-62443-4-2: "Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components," 2018.
21. ISASecure: "IEC 62443 - CSA Certification;" <https://www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification>.
22. Kwan: "Ironshield Best Practices Hardening Foundry Routers & Switches," 2003.
23. Laszka, W Abbas, Y Vorobeychik, et al: "Synergistic Security for the Industrial Internet of Things: Integrating Redundancy, Diversity, and Hardening," 2018.
24. ANSI/ISA-62443-3-3: "Security for industrial automation and control systems Part 3-3: System security requirements and security levels," 2013.
25. ISO/IEC 27001: "Information technology — Security techniques — Information security management systems — Requirements," 2013.
26. NIST SP 800-53 Rev 4; "Security and Privacy Controls for Federal Information Systems and Organizations."
27. CIS Controls, 2019.
28. Dekker: "The Field Guide to Understanding 'Human Error,'" 2011.
29. Adams, M Makramalla: "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach," 2015.
30. Homeland Security: "Common Cybersecurity Vulnerabilities in Industrial Control Systems," 2011.
31. Nurcan Y, S Gönen: "Attack detection/prevention system against cyber attack in industrial control systems," 2018.
32. Das, V Menon, TH Morris: "On the Edge Realtime Intrusion Prevention System for DoS Attack," 2018.
33. ISASecure: "IEC 62443 - SDC Certification;" [https://www.isasecure.org/en-US/Certification/IEC-62443-SDC-Certification-\(1\)](https://www.isasecure.org/en-US/Certification/IEC-62443-SDC-Certification-(1)).
34. IEC 62443-4-1: "Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements," 2018.
35. Cook, R Smith, L Maglaras, et al: "Measuring the Risk of Cyber Attack in Industrial Control Systems," 2016.
36. CISA: "Incident Response Pie Charts (YIR 2016 Addendum)," 2016.
37. Spyridopoulos, T Tryfonas, J May: "Incident Analysis & Digital Forensics in SCADA and Industrial Control Systems," 2013.
38. AP Rodrigues, RO Albuquerque, FEG Deus, et al: "Cybersecurity and Network Forensics: Analysis of Malicious Traffic towards a Honeynet with Deep Packet Inspection," 2017.
39. S Ashoor, S Gore: "Importance of Intrusion Detection System (IDS)," 2011.
40. Homeland Security: "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," 2008.
41. Homeland Security: "Developing an Industrial Control Systems Cybersecurity Incident Response Capability," 2009.

Article reprinted with permission. This article originally appeared at: <https://gca.isa.org/blog/a-practical-approach-to-adopting-the-iec-62443-standards> in 2021.

About the Author



Felipe Sabino Costa is an electrical and electronics engineer and an official ISA/IEC 62443 industrial cybersecurity instructor for the International Society of Automation (ISA), trained at ISA Headquarters in the U.S. He is also a LATAM Industrial Cybersecurity (IACS) Expert, an international speaker, and an author of books and white papers. With more 15 years inside the industrial sector dealing with a wide array of technologies and products, Felipe is dedicated to developing mission-critical solutions that include cybersecurity by design. Felipe holds cybersecurity certifications from the U.S. Department of Homeland Security, MIT, IBM, and Stanford. He recently obtained his MSc. in industrial cybersecurity from the Industrial Cybersecurity Center in Spain. He also has a specialization from Harvard University in Innovation and an MBA in Marketing.

STANDARDS NEWS

New York Lawmakers Reference ISA/IEC 62443 in New Proposed Bill

From Sept 7, 2021 ISA news release

New York state legislature is hoping to add additional protections to the state's critical infrastructure via a [newly proposed cybersecurity bill](#). The bill leverages the industry-adopted ISA/IEC 62443 series of standards to shape metrics and benchmarks for operational technology cybersecurity. If passed, the bill's measures would be applied to the state's critical infrastructure facilities, including: public transportation; water and wastewater treatment facilities; public utilities and buildings; hospitals, public health facilities, financial service organizations; and automation and control system components.

"There have been an increased amount of cyberattacks where hackers are just holding people hostage," [Senator Kevin Thomas, the bill's sponsor, said](#). "The bill looks to address this by updating systems to match international standards so that the state's critical infrastructure is protected as much as possible. There needs to be more vigilance. We need to know whether these critical infrastructure systems can be compromised and how to upgrade them to prevent them from being compromised."

The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). The committee draws on the input and knowledge of IACS security experts from across the globe to develop consensus standards that are applicable to all industry sectors and critical infrastructure.

"The technologies that control and automate the world's most critical operations, including the facilities where we work and live, are under constant threat and attack," said ISA Global Cybersecurity Alliance Managing Director Andre Ristaino. "Consistent, global adoption of the ISA/IEC 62443 series of standards will help vendors, third parties, and end users—indeed, the entire digital supply chain—effectively and proactively manage risks to their people, assets, and operations."

Many critical infrastructure and industrial manufacturing companies already have or are working diligently to integrate cybersecurity into their risk-management and business continuity plans and strategies. Using the ISA/IEC 62443 series of standards as their foundation, they focus on adopting security as part of the operations lifecycle, ensuring compliance with various aspects of the standards across their supply chains, and including cybersecurity in operational risk-management profiles.

STANDARDS NEWS

FM Approvals Accredited by Standards Council of Canada: ISASecure Program*From Sept 30, 2021 ISA news release*

The Standards Council of Canada recently accredited FM Approvals to be an ISASecure® certification body (CB). FM Approvals is now authorized to issue certificates of conformance for the ISA/IEC 62443-based ISASecure automation and control systems cybersecurity certification scheme upon successful completion of the required testing.

FM Approvals joins the growing list of highly specialized and internationally recognized ISASecure CBs that assess and certify automation and control system products to the ISA/IEC 62443 family of standards.

“We thank our collaborators at the Standards Council of Canada and the energetic team at FM Approvals, LLC,” stated Andre Ristaino, ISCI Managing Director. “These two organizations were well prepared, a pleasure to work with, and completed the accreditation in record time. The addition of these two organizations elevates the credibility of the ISASecure ISA/IEC 62443 cybersecurity certification program.”

FM Approvals has developed a new cyber security laboratory, located in Norwood, Massachusetts and is staffed with a dedicated team of cyber security and industrial control experts, is a fully virtualized security test environment, hosting its own servers and specially designed cyber security test stations.

Jim Marquedant, VP of Electrical Systems at FM Approvals, states, “The lab is configured to efficiently evaluate multiple ICS products in parallel for compliance with the applicable cyber security standards. ICS products that successfully complete FM Approvals’ ISASecure evaluation program will bear the FM Diamond along with a specific security level which signifies that the ICS product is robust against cyber-attacks and free from known vulnerabilities.”

The ISASecure scheme is a standards-based certification scheme that assesses the cybersecurity of automation and control systems to the ISA/IEC 62443-4-2 and ISA/IEC 62443-3-3 standards and certifies that the supplier/manufacturer’s development processes are conformant to the eight practice areas in ISA/IEC 62443-4-1 international standard.

ISASecure CB’s are independently assessed by ISO/IEC 17011 (EN 45011) accreditation bodies (ABs) such as the Standards Council of Canada for conformance to ISO/IEC 17025, ISO/IEC 17065 and, ISASecure technical readiness specifications. ISASecure CB’s are audited annually by the AB to ensure they maintain current and updated ISASecure accreditation requirements for participation in the ISASecure scheme.

About FM Approvals

FM Approvals is an international leader in third-party testing and certification services. FM Approvals tests property loss prevention products and services—for use in commercial and industrial facilities—to verify they meet rigorous loss prevention standards of quality, technical integrity, and performance. FM Approvals employs a worldwide certification process that’s backed by scientific research and testing, and over a century of experience.

About the ISA Security Compliance Institute (ISCI)

Founded in 2007, the ISA Security Compliance Institute’s mission is to provide the highest level of assurance possible for the cybersecurity of automation control systems.

The Institute was established by thought leaders from major organizations in the automation and controls community seeking to improve the cybersecurity posture of critical Infrastructure for generations to come.

Founders and key supporters of ISASecure include BP, Chevron, ExxonMobil, Saudi Aramco, Shell, Honeywell, Johnson Controls, Schneider Electric, Yokogawa, Siemens, exida, TUV Rheinland, CSSC, FM Approvals, Synopsys, DNV, Applied Risk, Trust CB, Security Compass, SGS Espanola de Control, BYHON, TUV SUD, WisePlant HQ, and Bureau Veritas.

The Institute’s goals are realized through industry standards compliance programs, education, technical support, and improvements in suppliers’ development processes and users’ life cycle management practices. The ISASecure designation ensures that automation and control system products conform to industry consensus cybersecurity standards such as ISA/IEC 62443, providing confidence to users of ISASecure products and systems and creating product differentiation for suppliers conforming to the ISASecure specification.

www.isasecure.org

ISASecure® is a registered trademark of the ISA Security Compliance Institute.



STANDARDS NEWS

IEC Designates ISA/IEC-62443 as a Horizontal Standard*From Nov 17, 2021 ISA news release*

The International Society of Automation (ISA) and the ISA Global Cybersecurity Alliance (ISAGCA) are proud to announce that the International Electrotechnical Commission (IEC) has officially designated the IEC/ISA 62443 series of standards as “horizontal,” meaning that they are proven to be applicable to a wide range of different industries.

According to the IEC decision, “The IEC Technical Committee 65 (TC 65) publishes IEC 62443 for operational technology found in industrial and critical infrastructure, including but not restricted to power utilities, water management systems, healthcare, and transport systems. These horizontal standards, also known as base standards, are technology independent. They can be applied across many technical areas.”

“The ISA99 committee of the International Society of Automation (ISA) and IEC Technical Committee 65 Working Group 10 have been collaborating on the development of the ISA/IEC 62443 cybersecurity standards for industrial automation and control systems (IACS) cybersecurity for many years. While broad applicability has always been the intent, there has been a common perception that they were most appropriate for process industries such as chemicals and refining,” explained ISA99 Co-Chair Eric Cosman. “Despite that perception, there have been several examples of successful applications in other sectors, such as transportation, building automation, metals and mining, and discrete manufacturing. It’s ultimately best for users if they can rely on one set of sector-agnostic standards, and we are very happy to receive the IEC decision to designate the ISA/IEC 62443 series as horizontal standards.”

The ISA/IEC 62443 series of standards is the world’s only consensus-based cybersecurity standard for automation and control system applications. These standards codify hundreds of years of operational technology and IoT cybersecurity subject matter expertise. Using the ISA/IEC 62443 series of standards as a foundation, companies can focus on adopting security as part of the operations lifecycle, ensuring compliance with various aspects of the standards across their supply chains, and including cybersecurity in operational risk-management profiles.

“While this news might seem like a procedural detail, it will have significant implications,” said Cosman. “Various other IEC technical committees that represent the needs and interests of specific sectors will presumably base their cybersecurity-related efforts on what is in the 62443 standards, focusing on defining how they should be interpreted and applied in a given set of circumstances. This will almost certainly lead to the creation of a set of sector-specific profiles for this purpose. To help in this effort, TC65 WG10 is developing guidance on how to develop such profiles, rather

than pursue sector-specific and perhaps inconsistent standards. Guidelines, frameworks, training materials, and other resources can also take on a more general focus, incorporating the needs of many sectors.”

The designation of the ISA/IEC 62443 series as a horizontal standard will have many benefits to stakeholders:

- Asset owners who have a presence in or exposure to more than one sector will be able to align their cybersecurity programs, leveraging ISA/IEC 62443 as the one single source for the fundamental principles and requirements of automation cybersecurity
- Automation system suppliers will be able to certify their products for a broader range of applications, using a common set of conformance specifications based on 62443
- IEC TC 65 WG 10 and the ISA99 committee will be able to focus their efforts on collaboration and advancement of the series of standards, especially around current demands in areas such as IIoT, sensor-level security, and supply chain risks
- The ISA Global Cybersecurity Alliance (ISAGCA) and its 50+ member companies will partner with asset owners and suppliers to build relevant, applications-focused materials to enable companies in different sectors around the world to adopt and implement the series of standards at scale

“The member companies of the ISA Global Cybersecurity Alliance have long believed in the broad applicability of the ISA/IEC 62443 series of standards,” said ISAGCA Chair Megan Samford. “We could not be more excited to see this news from IEC, because it echoes and confirms the work we’ve done. This series of standards is the only complete set of practices and security capabilities that can be applied to consistently assess and improve cybersecurity for operational technology systems, and our members stand ready to help companies all over the globe implement it successfully.”

About ISA

The International Society of Automation (ISA) is a non-profit professional association founded in 1945 to create a better world through automation. ISA advances technical competence by connecting the automation community to achieve operational excellence. The organization develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its members and customers around the world.

ISA created the ISA Global Cybersecurity Alliance (isa.org/ISAGCA) to advance cybersecurity readiness and awareness in manufacturing and critical infrastructure facilities and processes. The Alliance brings end-user

companies, automation and control systems providers, IT infrastructure providers, services providers, system integrators, and other cybersecurity stakeholder organizations together to proactively address growing threats.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (automationfederation.org), an association of non-profit organizations serving as “The Voice of Automation.” Through a wholly-owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (isasecure.org) and the ISA Wireless Compliance Institute (isa100wci.org).

About ISAGCA

The ISA Global Cybersecurity Alliance (ISAGCA) is a collaborative forum of member companies that aim to advance cybersecurity awareness, education, readiness, and knowledge sharing industry-wide, on a global scale. The alliance’s objectives include expanding the development and use of the ISA/IEC 62443 series of standards, knowledge-sharing in an open environment, providing best practice tools to help companies secure their infrastructure, creating education and certification programs, and advocating for cybersecurity awareness and sensible approaches with world governments and regulatory bodies.

About ISAGCA Members

The ISA Global Cybersecurity Alliance is made up of 50+ member companies, representing more than \$1.5 trillion in aggregate revenue across more than 2,400 combined worldwide locations. Automation and cybersecurity provider members serve 31 different industries, underscoring the broad applicability of the ISA/IEC 62443 series of standards. Current members of ISAGCA include 1898 & Co. (Burns McDonnell), ACET Solutions, aeSolutions, Baserock IT Solutions, Bayshore, Carrier Global, Claroty, ConsoleWorks, Coontec, CyberOwl, CyPhy Defense, Deloitte, Digital Immunity, Dragos, Eaton, exida, Ford Motor Company, Fortinet, Honeywell, Idaho National Laboratory, Idaho State University, ISASecure, Johns Manville, Johnson Controls, KPMG, LOGIIC, Mission Secure, MT4 senhasegura, Munio Security, Nova Systems, Nozomi Networks, PAS, PETRONAS, Pfizer, Radiflow, Redacted, Red Trident, Rockwell Automation, Schneider Electric, Surge Engineering, TDI Technologies, Tenable, TI Safe, Tripwire, TXOne Networks, UL, Wallix, WisePlant, Xage Security, and Xylem. For more information about ISAGCA, visit isa.org/isagca.

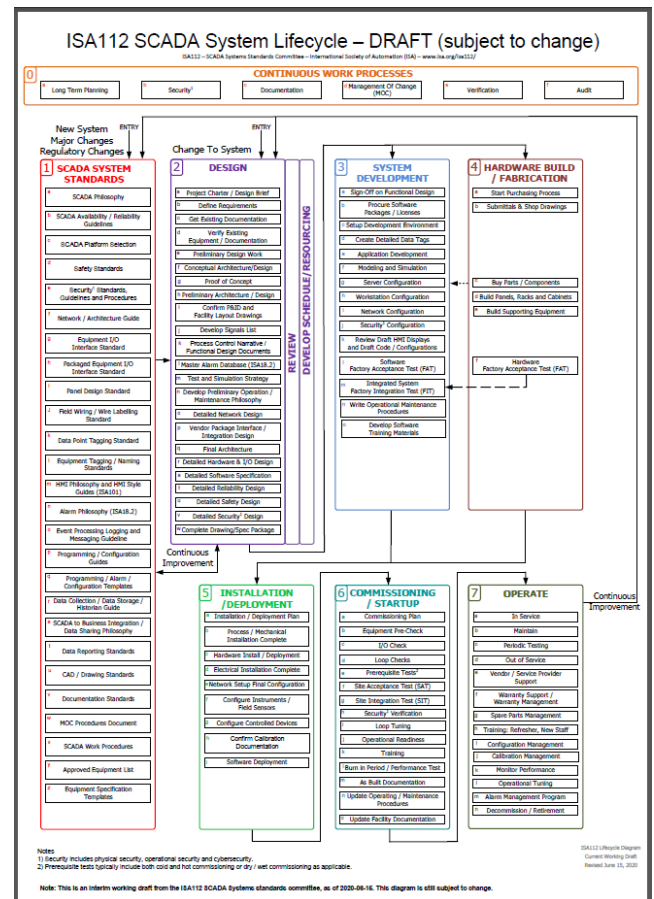
STANDARDS NEWS

ISA112 SCADA Systems Standards Update

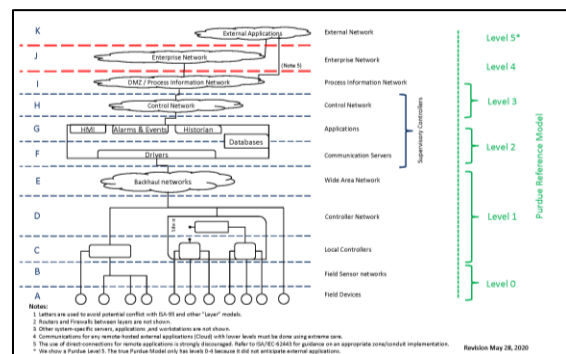
by Graham Nasby, ISA112 committee co-chair

The ISA112 SCADA Systems committee has been hard at work during the past 2 years assembling content to go into the upcoming publication of the ISA112 standard. The master working drafts now comprise of over 600 pages of technical text, with 70% of the sections written. A small army of authors is now working to finish up the remaining 30% of sections.

The main work products from the ISA112 committee are the ISA112 SCADA system management lifecycle and the ISA112 model architecture diagram. Both are now available as free PDF downloads at www.isa.org/isa112/



ISA112 SCADA Systems Management Lifecycle



ISA112 SCADA model reference architecture diagram

AUTO-QUIZ: BACK TO BASICS

Slip in AC Induction Motors

From the ISA Certification Program

This automation industry quiz question comes from the ISA Certified Automation Professional (CAP) certification program. ISA CAP certification provides a non-biased, third-party, objective assessment and confirmation of an automation professional's skills. The CAP exam is focused on direction, definition, design, development/application, deployment, documentation, and support of systems, software, and equipment used in control systems, manufacturing information systems, systems integration, and operational consulting.

Question:

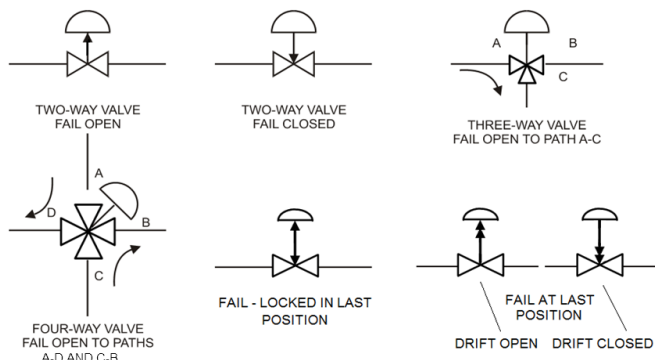
Failsafe positions for a valve can be:

- A) Fail Closed
- B) Fail Open
- C) Fail Last or Locked
- D) All of the above

Answer:

The correct answer is **D - All Of The Above**.

The actuator action and mounting position determine the fail state of the valve package. The arrow on the stem of a two-way actuator shows if the valve/actuator package is a fail open or fail closed. On three- and four-way actuators the arrows show the failed paths. The letters "FO" (fail open) and "FC" (fail closed) are sometimes used in place of the arrows on two way valves. The letters "FIP" also are used to refer to a valve that Fails In Place.



Want to learn more about control valves? Sign up for ISA's training course, [Control Valve Mechanics and Operations from Analog to Digital](#).

Reference: Nicholas Sands, P.E., CAP and Ian Verhappen, P.Eng., CAP., [A Guide to the Automation Body of Knowledge](#). To read a brief Q&A with the authors, plus download a free 116-page excerpt from the book, [click this link](#).

ISA CAP and CCST certification programs provide a non-biased, third-party, objective assessment and confirmation of an automation professional's skills.

The CAP exam is focused on direction, definition, design, development/application, deployment, documentation, and support of systems, software, and equipment used in control systems, manufacturing information systems, systems integration, and operational consulting.

Certified Control System Technicians (CCSTs) calibrate, document, troubleshoot, and repair/replace instrumentation for systems that measure and control level, temperature, pressure, flow, and other process variables.

Question originally appeared in the ISA Certified Automation Professional; (CAP) program column of <https://blog.isa.org>.

Reprinted with permission.

(<https://blog.isa.org/autoquiz-slip-ac-induction-motor>)



Setting the Standard for Automation™

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.**

612864

SOCIETY NEWS

The New Normal*By Steve Mustard, 2021 ISA Society President*

It feels like it was only yesterday when Eric Cosman passed the gavel to me, and yet here we are at the end of my term as ISA President. Time really does fly!

*“But after a while
You realize time flies
And the best thing that you can do
Is take whatever comes to you
'Cause time flies”*

- Steven Wilson (“Time Flies,” Porcupine Tree)

Being ISA President is a unique experience. ISA has a diverse portfolio of activities, from membership to events, standards, training, and certification. Being responsible for the strategic direction of such an organization is quite a challenge. There are almost as many viewpoints on strategic direction as there are members and staff. Even if we had a perfect strategy, there are so many external factors that can derail it.

The COVID-19 pandemic could have been a disaster for a society that relies on in-person activities such as training and events for revenue. Thankfully, the team of staff and volunteers responded to this challenge. And, despite everything, I believe ISA is in a much better place now. Online training and events have created new opportunities for engagement in our global profession. I believe these opportunities are going to continue to grow as we create more training and develop more events.

It was disappointing that I was unable to meet many of you in person this year, but our virtual Executive Board meetings, District Leadership Conferences, and Connect Live meetings ensured we were able to keep in touch.

I enjoyed the opportunity to meet ISA members around the world—to hear about successful initiatives to grow membership from Pakistan to Portugal. I was able to participate in excellent technical discussions with Divisions on subjects such as project management and cybersecurity. I particularly enjoyed informal virtual meetings with former ISA Presidents. Being in the presence of such a distinguished group of leaders really brings home the significance of this role you all entrusted me to do.

Being President also allowed me to work closely with the staff. ISA has a very dedicated staff who work hard to create a vibrant society for our members and the wider profession. [Back in May](#), I wrote about *mutually beneficial volunteerism*, where volunteers and staff work together, building on each other's strengths. I really believe we are better when we work together. With this in mind, we took the opportunity to introduce our volunteer leaders to the team during monthly all-staff meetings. These meetings were a

great way of encouraging collaboration between staff and volunteers.

And this new year brings a lot of “new” to ISA—a new [Executive Director](#) and a new office. But we do not lose our steadfast focus on our [strategic objectives](#). In my column [last month](#), I asked for everyone's patience. We all want ISA to be the *home of automation*, the place where everyone in our profession goes for guidance, instruction, and support. I know we can be that place, but it will take time, and we need *your* support to make it happen.

As always, feel free to [contact me](#) if you have any thoughts or comments. How was your 2021? What would you like to see ISA achieve in 2022 and beyond?

I close out my last official column with my heartfelt gratitude for this opportunity. It has been my honor and privilege to serve as ISA President. While my term comes to an end, I am very pleased to pass the gavel to my friend, Carlos Mandolesi. I know that he will continue to lead ISA toward bigger and better things. Please help him, as you have me, create a better world through automation.

Steve Mustard
2021 ISA President

About the Author

Steve Mustard is an industrial automation consultant with extensive technical and management experience across multiple sectors. He is a licensed Professional Engineer (PE), ISA Certified Automation Professional® (CAP®), UK registered Chartered Engineer (CEng), European registered Engineer (Eur Ing), GIAC Global Industrial Cyber Security Professional (GICSP), and Certified Mission Critical Professional (CMCP). Backed by 30 years of engineering experience, Mustard specializes in the development and management of real-time embedded equipment and automation systems and cybersecurity risk management related to those systems. He serves as president of National Automation, Inc. Mustard writes and presents on a wide array of technical topics and is the author of ‘Mission Critical Operations Primer,’ published by ISA.



Call for Newsletter Articles

The WWID newsletter is published four times a year (winter, spring, summer, and fall) and reaches the WWID's 2,000+ members. Each issue is approximately 16-32 pages long, and is electronically printed in color PDF format. A notification email goes out to all WWID members and it is available for public download at www.isawaterwastewater.com.

We are always on the lookout for good articles, and we welcome both solicited and unsolicited submissions.

Article submissions should be 500-2000 words in length and be written for a general audience. While it is understood that the articles are technical in nature, the use of technical jargon and/or unexplained acronyms should be avoided. We actively encourage authors to include several photos and/or figures to go along with their article.

We actively welcome articles from all of our members. However, we do ask that articles be non-commercial in nature wherever possible. One or two mentions of company and/or product names for the purposes of identification are acceptable, but the focus of the article should be technical content and not just sales literature. If you are unsure of whether your article idea is workable, please contact our newsletter editor for more information – we are here to help.

Some examples of the types of articles we are looking for include:

- Explanatory/teaching articles that are meant to introduce or explain a technical aspect of automation and/or instrumentation in the water/wastewater sector.
- Biographical stories about personalities and/or leaders in the water/wastewater sector.
- Case Studies about plant upgrades and/or the application of new technologies and techniques. This type of article must include at least two photos along with the article text.
- Pictorial Case Studies about a plant upgrade consisting of 4-6 photos plus a brief 200-500 word description of the project undertaken. The article should ideally include one to two paragraphs about lessons learned and/or advice for other automation professionals.
- Historical reflections on changes in technology pertaining to specific aspects of instrumentation or automation, and how these changes point to the future.
- Discussions about changes in the water/wastewater sector and how these affect automation professionals.

Once we receive a submission, we will work with you to edit it so it is suitable for publication in the newsletter.

Article submissions can be sent to the WWID newsletter editor Graham Nasby at graham.nasby@grahamnashby.com.

WWID Newsletter Advertising

The WWID newsletter is an excellent way to announce new products and services to the water/wastewater automation community. With a distribution of 2,000+ professionals in the automation, instrumentation and SCADA fields, the WWID newsletter is an effective targeted advertising tool.

The WWID newsletter is published quarterly, on the following approximate publication schedule:

- Winter Issue – published in January/February
- Spring Issue – published in April/May
- Summer Issue – published in July/August
- Fall Issue – published in October/November

Advertising in the newsletter is offered in full page, half-page and quarter page formats. Advertisements can be purchased on a per issue basis or for four issues at a time. The newsletter itself is distributed as a full-color PDF, so both color and black/white artwork is acceptable.

The current advertising rates are as follows:

Per Issue:

- Full page, full color (7" x 9"): \$500
- Full page, full color, (8.5x11"), with bleed \$600
- Half page horizontal, full color (7"x4.5"): \$350
- Half page vertical, full color (3.5"x9"): \$350
- Quarter page, full color (3.5" W x 4.5" H): \$250

Per Year: Apply 20% discount if purchasing 4 ads at a time

Other sizes of advertisements are available, but are priced on an individual basis. Contact us for more information.

Please book advertising space as early as possible before the intended publication date. Artwork for advertisements should be submitted a minimum of two weeks prior to the publication date; earlier is always better than later. Artwork for advertisements can be submitted in EPS, PDF, PNG, JPG or GIF formats. EPS, PDF and PNG formats are preferred. Images should be at least 300dpi resolution if possible. A complete list of ad specs can be found at www.isawaterwastewater.com.

The ISA Water/Wastewater Industry Division is run on a non-profit basis for the benefit of its members. Monies raised from the sale of advertising in the newsletter are used to help offset the cost of division programming and events. Like its parent organization, the ISA, the WWID is a non-profit member-driven organization.

For more information, or to discuss other advertisement sizes not outlined above, please contact the WWID newsletter editor Graham Nasby at graham.nasby@grahamnashby.com.



WWID Board Member Contacts

Director (2021-2022)

Manoj Yegnaraman, PE
Carollo Engineers Inc.
Dallas, Texas, USA
Tel: (972) 239-9949
myegnaraman@carollo.com

2021-2022 Conference Chair

2021-2022 Director-Elect

Hassan Ajami, PE, CAP
PCI Vertix
Detroit, Michigan, USA
Tel: 313-874-5877
hajami@pci-vertix.com

Past Director

Don Dickinson
Phoenix Contact USA
Cary, North Carolina, USA
Tel: (919) 633-0147
ddickinson@phoenixcontact.com

Program Chair

Joe Provenzano
KPRO Engineering Services
Naugatuck, Connecticut, USA
Tel: (203) 560-1816
provenzano2@comcast.net

Honors and Awards Chair and Sections-Divisions Liaison

Pavol Segedy, PE
HDR Inc.
Raleigh, North Carolina, USA
Tel: (919) 427-5313
pavol.segedy@segedyfam.com

Membership Chair

Colleen Goldsborough
United Electric Supply
Lancaster, Pennsylvania, USA
Tel: (717) 392-8500
cgoldsborough@unitedelectric.com

Newsletter Editor

& Co-Chair, ISA112 SCADA Systems Standards Committee

Graham Nasby, P.Eng, PMP, CAP
City of Guelph Water Services
Guelph, Ontario, Canada
Tel: (519) 822-1260 ext. 2192
graham.nasby@grahamnashby.com

Scholarship Committee Chair & Asst. Newsletter Editor

Kevin Patel, PE, MBA
Signature Automation
Dallas, Texas, USA
Tel: (469) 619-1241
knpatel@sig-auto.com

Secretary

Mike Briscoe
Signature Automation
Dallas, Texas, USA
Tel: +1 (469) 619-1241
mbriscoe@sig-auto.com

David Hobart, P.Eng, CAP
Hobart Automation Engineering
Tel: (802) 253-4634 – Portland, Maine, USA
dghobart@gmail.com

Steve Valdez
Generic Electric
Paramus, New Jersey, USA
Svaldez1210@gmail.com

Jason Hamlin
Instrullogic
Lynchburg, Virginia, USA
jhamlin@instrullogic.com

Student Scholarship Committee Members

Kevin Patel, Signature Automation (chair), knpatel@sig-auto.com
Sean McMillan, Jones & Carter, sean.mcmillan@jonescarter.com
Steve Valdez, General Electric, svaldez1210@gmail.com
Thomas C. McAviney, I&C Engineering, tcmcav@gmail.com
Wally Ingham, Consultant, wally1234ingham@gmail.com

ISA Staff Contacts – Division Services

Andrea Holovach, Rachael McGuffin,
Karen Modrow, MaChelle Beason
ISA Headquarters, 67 T.W. Alexander Drive, PO Box 12277, Research
Triangle Park, North Carolina, 27709, USA
Tel: (919) 990-9404
Fax: (919) 549-8288
divisions@isa.org

ISA Water/Wastewater Division Links:

Website: www.isawaterwastewater.com
Blog: www.isawaterwastewater.com/blog/

ISA Microsite: www.isa.org/wwid/
ISA Connect: connect.isa.org
LinkedIn: <https://www.linkedin.com/groups/2031271/>
Facebook: <https://www.facebook.com/ISAWaterWastewater/>

ISA Customer Service

ISA Headquarters - Raleigh, North Carolina, USA
Tel: 1 (919) 990-9404
Fax: (919) 549-8288
Customer Service Hours: Mon-Fri 9am-4pm (Eastern, UTC-05:00)
Email: info@isa.org

About the ISA Water/Wastewater Industries Division

The ISA Water / Wastewater Industry Division (WWID) is concerned with all aspects of instrumentation and automated-control related to commercial and public systems associated with water and wastewater management. Membership in the WWID provides the latest news and information relating to instrumentation and control systems in water and wastewater management, including water processing and distribution, as well as wastewater collection and treatment. The division actively supports ISA conferences and events that provide presentations and published proceedings of interest to the municipal water/wastewater sector. The division also publishes a quarterly newsletter, and has a scholarship program to encourage young people to pursue careers in the water/wastewater automation, instrumentation and SCADA field. For more information see www.isa.org/wwid/ and www.isawaterwastewater.com



**Water/Wastewater
Industry Division**