GLOBAL CYBERSECURITY ALLIANCE

ISA Global Cybersecurity Alliance Position on Automation Cybersecurity Requirements in Public Policy

Recent discussions have surfaced in the United States and in other world governments about how to best secure automation and control systems that affect our everyday lives, especially in critical infrastructure. US President Biden issued Executive Order 14028 on May 12, 2021, addressing securing automation in critical infrastructure; and the ISA Global Cybersecurity Alliance submitted a formal response.

We hope this executive order and other measures will encourage those who support the nation's critical infrastructure to develop and implement automation cybersecurity capabilities that will ensure the security of our way of life. This position paper describes the public policies and associated reference standards supported by the ISA Global Cybersecurity Alliance (ISAGCA.)

About the ISA Global Cybersecurity Alliance

The ISAGCA is a collaborative forum hosted by the International Society of Automation (ISA), a global professional automation engineering society. ISAGCA's mission is to advance cybersecurity readiness through awareness, education, standards, and knowledge sharing. Membership is open to any organization concerned about cybersecurity—end users, automation providers, system integrators, consultants, government agencies, and more.

ISAGCA member companies, industry organizations, and their constituents represent over $1.5 trillion in annual revenues, coming from industries such as critical infrastructure, oil & gas, pharmaceuticals, automotive, automation suppliers, IT suppliers, and providers of cybersecurity products and services.

ISAGCA member companies and thought leaders have a long history of adopting a standards-based approach for securing automation products and operating sites based on the ISA/IEC 62443 series of international cybersecurity standards.

More

Together, we advocate for broad adoption and implementation of this series of standards that are proven to protect critical infrastructure and other important technology that affects our everyday lives.

About the ISA/IEC 62443 Series of Standards

Post 9/11, ISA members recognized the need to secure automation that controls equipment and operations comprising US critical infrastructure. In 2002, ISA's ANSI-accredited standards department stood-up the ISA99 committee to develop cybersecurity standards for automation and control systems and, has since, published a comprehensive family of 15 standards and technical reports purpose-built to address securing automation and control systems.

Over 1,000 engineering professionals and cybersecurity experts contributed to the ISA/IEC 62443 standards, codifying thousands of years of engineering and cybersecurity subject matter expertise into a coherent series of standards.

The ISA 62443 standards are submitted to the International Electrotechnical Commission for global adoption as international standards IEC 62443. The IEC 62443 standards are endorsed by the United Nations. By leveraging use cases from more than 20 different industry verticals, the ISA/IEC 62443 standards have demonstrated their usefulness in all industry sectors that use operational technology. ISA/IEC 62443 approaches the cybersecurity challenge in a holistic way and addresses the connections between operations technology and information technology.

A founding principle of the ISA/IEC 62443 standards is the concept of shared responsibility as a necessary part of securing automation. The standards define requirements for key stakeholder groups who are involved in control system cybersecurity. Stakeholder groups include asset owners (end users), automation product suppliers, integrators who build and maintain control system solutions and their components, and service suppliers who support the operation of control systems.

The ISA/IEC 62443 series addresses the security of industrial automation and control systems (IACS) throughout their lifecycle (which includes all automation and control systems; not just industrial.) IACS includes more than the technology that comprises a control system; it also includes the people and work processes needed to ensure the safety, integrity, reliability, and security of the control system. Without people who are sufficiently trained; risk-appropriate technologies and countermeasures; and work processes throughout the security lifecycle, an IACS could be more vulnerable to cyberattack.

More >

The ISA/IEC 62443 standards and technical reports have been successfully applied to a variety of industry sectors, including process industries such as chemicals and oil & gas, building automation, electric power generation and distribution, medical devices, and transportation.

Because IACS are physical-cyber systems, the impact of a cyberattack could be severe. The consequences of a cyberattack on an IACS include, but are not limited to:

- Endangerment of public or employee safety or health
- Damage to the environment
- Damage to the equipment under control
- Loss of product integrity
- Loss of public confidence or company reputation
- Violation of legal or regulatory requirements
- Loss of proprietary or confidential information
- Financial loss
- Impact on entity, local, state, or national security

The ISA/IEC 62443 series of standards provides guidance for securing IACS by:

- Defining common terms, concepts, and models that can be used by all stakeholders responsible for control systems cybersecurity; these concepts are used consistently throughout the ISA/IEC 62443 standards.
- Providing a list of security technologies and processes that assets owners can implement to ensure the level of security required to meet their unique business and risk needs.
- For asset owners and integrators, the series defines the steps needed to design and build a control system with the appropriate level of security controls.
- For product developers, the series establishes a common set of requirements and a cybersecurity lifecycle methodology for the development of products and services. This includes a mechanism to certify the products and vendor development processes.
- Defining the risk assessment processes that are critical to protecting control systems, including:

    - For asset owners, assessing business risks to define the priorities of the cybersecurity program and help identify the counter measures that are needed to protect the business
    - For asset owners and integrators, assessing risks when designing control systems
    - For product developers, assessing potential risks to product designs during the product lifecycle

More >

ISA/IEC 62443 addresses the importance of functional safety requirements

ISA/IEC 62443 standards align with the requirements in IEC 61511 for Safety Instrumented Systems (SIS). These requirements include performing a security risk assessment to identify the security vulnerabilities of the SIS. The requirements also address the design of the SIS to ensure it provides the necessary resilience against the identified security risks. These standards further define the Functional Safety Lifecycle to ensure cybersecurity requirements are addressed through the lifecycle phases of the SIS.

Legislation and Public Policy Considerations

ISAGCA is working with state and federal legislators, regulators, and other standards bodies to ensure that the ISA/IEC 62443 standards are included as the reference standards for establishing IACS cybersecurity metrics in automation that affects our everyday lives.

Principles guiding our IACS cybersecurity advocacy are:

1. **It is critically important for legislators and regulators to recognize the urgent need for response to this threat.** The operational technologies that automate the critical infrastructure and commercial facilities of daily life are experiencing a rapid increase in cybersecurity incidents. The impact is serious, affecting life, safety, the environment, and economic viability across sectors.

2. **A standard definition of the security capabilities for system components is necessary; it will provide a common language for product suppliers and all other control system stakeholders.** A standard definition of security capabilities simplifies the procurement and integration processes for the computers, applications, network equipment, and devices that make up a control system. The United States National Institute of Standards and Technology (NIST) published the NIST Cybersecurity Framework (CSF), which references several relevant cybersecurity standards including ISA/IEC 62443. The NIST CSF is becoming the de facto framework for public policy on cybersecurity in the US. The NIST CSF contains over 112 references to the internationally recognized ISA/IEC 62443 family of standards, which defines a set of measures and benchmarks purpose-built to guide organizations and measure compliance. ISA/IEC 62443 helps organizations through the process of assessing the risk of a particular automation and control system and provides guidance in identifying and applying security countermeasures to reduce that risk.

More >

3. **A fully developed ISA/IEC 62443 ecosystem enables facilities/operations across many different industries to achieve IACS cybersecurity. ISA/IEC 62443 provides guidance for all stakeholders in the entire automation lifecycle. Example usage of standards:**

   - Procurement, construction, reconstruction, alteration, design and commissioning of critical infrastructure or automation control systems or automation control system components. When procuring Automation and Control System components, services or solutions or when contracting for facility upgrades or the construction of critical infrastructure facilities, shall require those components, services, and solutions to conform to the ISA/IEC 62443 Series of standards as referenced by the NIST Cybersecurity Framework (NIST CSF) for defining measures to assure conformance. All contracts awarded for construction, reconstruction, alteration, design, and commissioning of facilities identified as critical infrastructure shall provide that installed automation and control components meet the minimum standards for cybersecurity as defined by ISA/IEC 62443 series of standards as referenced by the NIST Cybersecurity Framework (NIST CSF).
   - Operations and Maintenance of Critical Infrastructure. The asset owner shall be responsible for ensuring that the operation and maintenance of operational technology, including critical infrastructure, automation control systems, and automation control system components to be compliant with the standards and practices defined in the ISA/IEC 62443 series of standards as referenced by the NIST Cybersecurity Framework (NIST CSF), including periodic risk assessments and maintenance of plans for prevention, detection, responding, and rebuilding. Resilience plans and consequence mitigation are important dimensions of the plans.
   - The NIST CSF also references the ISO 27001/2 international standards for IT security. ISO 27001/2 are complementary to ISA/IEC 62443 and industry groups have published guidance for implementing the two standards as companion specifications for securing the entire spectrum of IT and OT technology in complex organizations.

4. **The standards are equally applicable to all technologies, so requiring compliance wouldn't give any stakeholder a marketplace advantage.** Legislation should include a transition time frame and a phased-in approach to requirements over several years to allow for economic and orderly implementation of the security policies.

ISAGCA will continue to work to ensure control system security is addressed in the creation and implementation of international standards, laws, and regulations. **We believe that control system cybersecurity is best achieved by referencing ISA/IEC 62443 as the common foundation for securing automation that affects our everyday lives.**