POSITION PAPER

Advancing Industrial Cybersecurity

Cybersecurity threats and vulnerabilities pose a clear and present danger to our facilities, our processes and the safety of our communities. But when most people think about cybersecurity, they focus on what are commonly considered information technology (IT) challenges impacting individual equipment or networks. While these are valid concerns, the impact on the facility or its operation from equipment or network compromise is much more concerning.

This position paper aims to address how policy makers and private-sector leaders can be best equipped to address the urgent need for improved critical infrastructure cybersecurity through globally relevant standards and conformance programs, as well as strong support for the community of engineers and automation professionals working every day to keep our facilities, processes and communities safe.

CYBERSECURITY INCIDENTS IN INDUSTRIAL CYBERSECURITY CAN SIGNIFICANTLY HARM CRITICAL INFRASTRUCTURE

The impacts of cyber intrusions on banking, business and government networks, and databases have been widely publicized and are well known to the general public. Much less publicized and understood are the devastating impacts to public safety and welfare that could result from cyber-attacks on the networks and technology that underlie the vast critical infrastructure and manufacturing sectors on which all modern economies depend.

While certain high-profile incidents have made international news (e.g., TRISIS,[1] NotPetya,[2] STUXNET[3]), in fact, control system cyber incidents have been more numerous and more impactful than most people have been aware.[4]

At the core of this challenge is identifying control system events and reportable cyber incidents.[5] Understanding the unique nature of control system equipment —and the impact of a compromise of that equipment on physical processes— requires specialist training for the engineering and automation community. Such training is available[6] from the International Society of Automation (ISA); however, a major concern is that not enough engineers are equipped for the unique and growing challenges of the industrial cybersecurity environment.

Training is just one need among many – in reality, what a lot of organizations require is a cultural shift that prioritizes cybersecurity alongside functionality, efficiency, and safety as one of the fundamental workplace tenets.

Until organizations prioritize cybersecurity at this level, even the best equipped and most trained engineers will be challenged to fully protect their industrial or infrastructure environment.

GOVERNMENTS AROUND THE WORLD ARE ISSUING DIRECTIVES TO ADDRESS THIS CHALLENGE

The US National Cybersecurity Strategy[7] and its Implementation Plan[8] address these dangers by explicitly calling for:

- Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance; and
- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services

Consequences

Compromise, whether malicious or unintentional, could result in any, or all, of the following:

- Harm to public and/or employees
- Loss of critical infrastructure services including power grids and water processing
- Damage to critical operational machinery
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Major economic losses
- Harm to the natural environment

However, the National Cybersecurity Strategy does not address the need for the engineering community to be involved, nor is the focus on control systems and processes. Further, the strategy does not specifically mention the leading consensus standards and conformance programs for industrial cybersecurity.

The European Union (EU)'s second iteration of the Network and Information Systems (NIS) Directive, NIS2,[9] contains stricter rules and applies to a broader set of industries. Together with the EU's Critical Entities Resilience directive, this will see member states incorporating key provisions on cybersecurity into their national law.

These are just two examples of countries and regions around the world that are taking such a stance and recognizing the threat to their critical infrastructure.

WHY ISA TAKES POSITIONS ON INDUSTRIAL CYBERSECURITY

The International Society of Automation (ISA), a member association of automation professionals from across the globe, believes that protecting critical infrastructure against cyber-attacks is essential to national security, public and employee safety and the economy. To help address the challenge of protecting critical infrastructure, ISA produces a series of international consensus standards addressing the security of industrial automation and control systems. The ISA/IEC 62443 series of standards[10] provides other guidance that provides a flexible and comprehensive framework to address and mitigate current and future security vulnerabilities in those systems.

This series of standards meets the World Trade Organization's criteria for international standards. The International Electrotechnical Commission (IEC), one of three United Nations sanctioned standards developers, has adopted the series, and designated as having "horizontal" status, establishing primacy across the entirety of the vast range of IEC technical

committees and subcommittees on matters pertaining to cybersecurity in industrial, critical infrastructure, and related applications. The United Nations Economic Commission for Europe has integrated the series into its Common Regulatory Framework on Cybersecurity, which serves as an official UN policy position statement for Europe.

ISA created the ISA Global Cybersecurity Alliance (ISAGCA)[11] 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 also offers the leading conformity assessment program for industrial cybersecurity products and systems—ISASecure[12]—which certifies against the ISA/IEC 62443 series of standards.

ISA's positions, standards, training, conformance programs, and guidance[13] can help reduce the likelihood and consequence of a cybersecurity incident in an industrial automation and control system environment.

ISA TAKES THE POSITIONS THAT:

- Mandating cybersecurity measures with prescriptive regulations is undesirable. Instead, regulations should support the use of risk-based approaches based on published consensus-based technical standards and conformance measures.
- Specific standards that take account of the unique characteristics of industrial automation and control systems should be used in preference to more general information technology standards.

ISA RECOMMENDS THAT:

Governments looking to secure their critical infrastructure should:

- Adopt by reference the ISA/IEC 62443 series of consensus standards addressing the security of industrial automation and control systems
- Direct their regulations towards ensuring that critical infrastructure owner-operators apply a formal risk-based approach to cybersecurity management

Organizations looking to secure their critical infrastructure should:

- Support their front-line engineers by fostering a cybersecurity culture within their organization, which prioritizes cybersecurity alongside other fundamental workplace tenets like efficiency and safety
- Provide ample opportunities for engineers to be trained and certified on the specific requirements of cybersecurity of industrial automation and control systems

ISA COMMITS TO:

- Developing and maintaining consensus-based standards, conformance programs and guidance that secure industrial automation and control systems using a flexible risk-based approach that ensures any size organization in any sector can use appropriately and efficiently

- Providing training resources to advance the understanding and application of the standards
- Promoting the adoption of standards and providing vendor- and sector-agnostic guidance on how to apply these standards
- Working with governments around the world[14] to adopt standards and guidance to secure critical infrastructure

CONCLUSION

An industrial automation and control system (IACS) is so much more than its hardware. It also includes the people and work processes needed to ensure the safety, integrity, reliability and security of the control system. Policy makers and private-sector organizations alike must strongly consider the need for compliance to global consensus standards for IACS cybersecurity, and must also create a culture of support and continuous training for the engineers who keep control systems operating at their best.

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 empowers the global automation community through standards and knowledge sharing, driving the advancement of individual careers and the overall profession. ISA develops widely used global standards; certifies 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.

RESOURCES

isa.org/standards	138+ standards for automation, cybersecurity, and more
isa.org/training	Unbiased, real-world training courses, personnel certifications, and certificates that help engineers and technicians take the next step in their automation career
isa.org/join	Membership in ISA offers unparalleled access to technical discussions and resources
isa.org/events	Network, hear best practices, and be part of the automation community dialogue at ISA events – both in person and virtual

WORKS-CITED

[1] Lee, R. M. (2017, December 14). TRISIS: Analyzing Safety System Targeting Malware. Dragos. Retrieved July 14, 2023, from https://www.dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/

[2] Lewis, J. A. (n.d.). How the NotPetya Attack Is Reshaping Cyber Insurance. Brookings Institution. Retrieved July 14, 2023, from https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/

[3] Zetter, K. (2014, November 11). Countdown to Zero Day: Stuxnet. *Wired.* Retrieved July 14, 2023, from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[4] ISA. (2023, February 28). More Than 17 Million Control System Cyber Incidents Are Hidden in Plain Sight. ISA Global Cybersecurity Alliance Blog. Retrieved from https://gca.isa.org/blog/more-than-17-million-control-system-cyber-incidents-are-hidden-in-plain-sight

[5] ISA. (2022, April 1). *I*ndustrial Cybersecurity for the CISO – Part 2 [Video]. Retrieved July 14, 2023, from https://www.youtube.com/watch?v=LUjjDyFE_AY&list=PLC3fVVaSjwYFnmFFvKlnJqD93i5muE_Xh&index=3

[6] ISA. (n.d.). Connectivity and Cybersecurity Courses. Retrieved July 14, 2023, from https://www.isa.org/training/training-courses-by-topic/connectivity- and-cybersecurity-courses

[7] White House. (2023). *National Cybersecurity Strategy 2023* [PDF]. Retrieved July 14, 2023, from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[8] White House. (2023). *National Cybersecurity Strategy Implementation Plan* [PDF]. Retrieved July 14, 2023, from https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[9] European Parliamentary Research Service (EPRS). (2021). *The NIS2 Directive:* A high common level of cybersecurity in the EU. Retrieved July 14, 2023, from https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

[10] ISA. (n.d.). I*SA/IEC 62443 Series of Standards*. Retrieved July 14, 2023, from https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards/

[11] ISA. (n.d.). ISA Global Cybersecurity Alliance. Retrieved July 14, 2023, from https://www.isagca.org/

[12] ISA Security Compliance Institute. (n.d.). Home. Retrieved July 14, 2023, from https://www.isasecure.org/

[13] ISA. (2020, June). *Quick Start Guide to ISA/IEC 62443. ISA Global Cybersecurity Alliance.* Retrieved from https://21577316.fs1.hubspotusercontent-na1.net/hubfs/21577316/2023%20ISA%20Website%20Redesigns/ISAGCA/PDFs/ISAGCA%20Quick%20Start%20Guide.pdf.

[14] ISA Global Cybersecurity Alliance. (n.d.). Advocacy & Adoption. Retrieved July 14, 2023, from https://isagca.org/advocacy-adoption