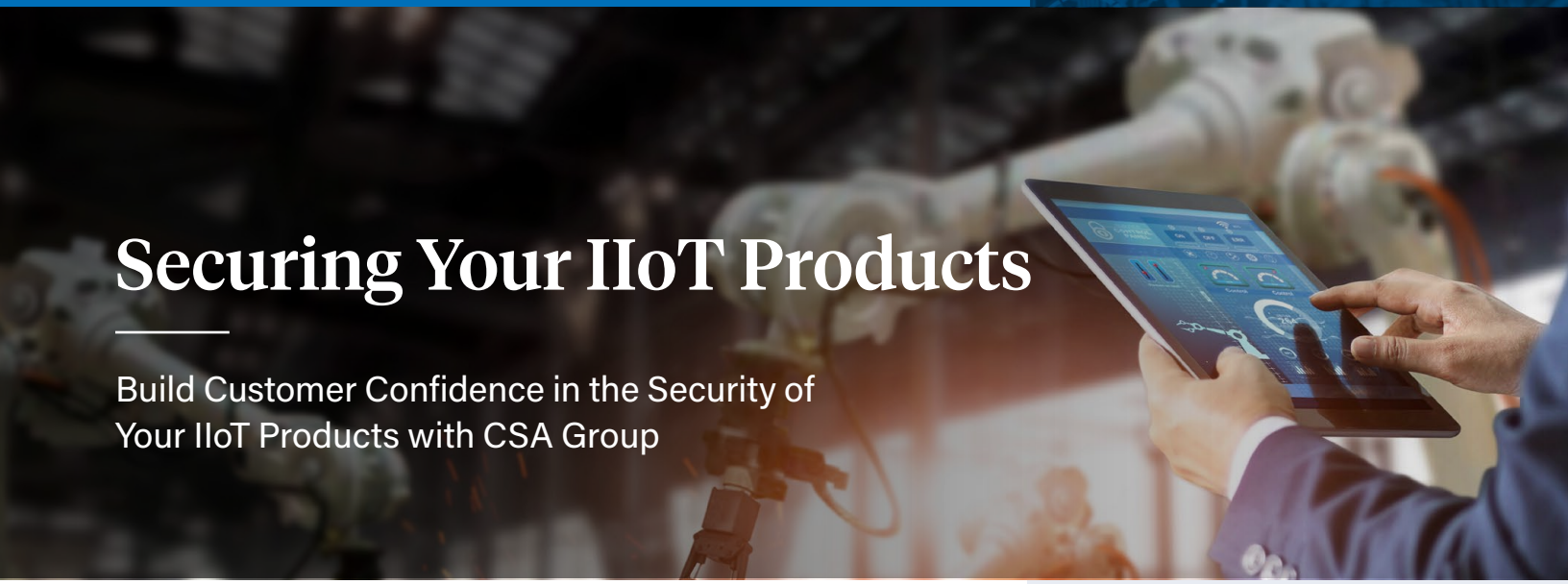

Securing Your IIoT Products

Build Customer Confidence in the Security of Your IIoT Products with CSA Group

Ransomware, botnets, and current event-themed attacks. These are some of the ominous threats that continue to plague Industrial Internet of Things (IIoT) and other systems and devices capable of connecting to a network. Cybersecurity incidents often result in increased expense and scrutiny coupled with loss of revenue and productivity. These adverse impacts can affect manufacturers and the customers and end-users of the compromised products.

Cybersecurity risks apply to manufacturers of IIoT products and systems used in many aspects of industrial, commercial, and consumer environments. The cyber-physical IIoT device and systems could be an easy target of an attack, although the device or system itself is not the intended target of harm.

One vulnerable connected device could be the weakest link that allows malicious activity to enter a network and wreak havoc on other connected systems, data, and the important functions they serve.

Are your IIoT products or systems the weakest link?

It took years to build your good reputation. Don't let product or system security ruin it.

To better understand, respond to, and control cybersecurity risks, a prudent first step is to better assess and monitor the threat landscape. For manufacturers, this implies incorporating security risk management into organizational operations and processes, ensuring products are secure by design, and implementing safeguards to maintain product security throughout the product's lifecycle.

Fast Facts

Cybersecurity incidents often result in increased expense and scrutiny coupled with loss of revenue and productivity. These adverse impacts can affect manufacturers and the customers and end-users of the compromised products.

One vulnerable connected device could be the weakest link that allows malicious activity to enter a network and wreak havoc on other connected systems, data, and the important functions they serve.

To better understand, respond to, and control cybersecurity risks, a prudent first step is to better assess and monitor the threat landscape.

Leveraging Standards and Guidance to Design and Deliver Secure Products, Systems and Services

The IEC 62443 standards series is an internationally-recognized set of published standards that establish baseline security expectations and guidance for organizational programs, processes, products, systems, and services. Manufacturers are able to leverage these standards to implement their security risk management programs and to design and provide secure, trustworthy products, systems, and services. Although initially developed with applicability focused on industrial automation and control systems (IACS) products and environments, these standards are beneficial and widely recognized in a variety of commercial, consumer, and non-IACS products and industries.

Here are examples of some of the IEC 62443 series standards CSA Group can help you with:

- **IEC 62443-4-1:** ***Secure product development lifecycle requirements*** – Establishes expectations and guidance for secure development lifecycle processes to incorporate throughout the lifecycle of a product
- **IEC 62443-4-2:** ***Technical security requirements for IACS components*** – Establishes technical control and security expectations and guidance for products and components aligned with seven distinct foundational requirements to define and measure security capability levels
- **IEC 62443-2-4:** ***Security program requirements for IACS service providers*** – Establishes security capability expectations and guidance for organizations providing services involved in the integration and maintenance activities of an automation solution or service
- **IEC 62443-2-1:** ***Establishing an industrial automation and control system security program*** – Establishes expectations and guidance on establishing cyber security management system (CSMS) with focus on the policy, procedure, practice, and personnel included in an organization's CSMS.
- **IEC 62443-3-3:** ***System security requirements and security levels*** – Establishes security and capability expectations and guidance for defining requirements for communication networks and systems security based on established security levels and aligned with foundational requirements

With over 100 years of experience and expertise in testing and certifying industrial and hazardous location products, CSA Group is ready to help you with navigating many of your cybersecurity objectives, including:

- **Technical Information Service (TIS):** We work with you to determine the cybersecurity-related standards, guidance, and requirements available and most applicable to your current and impending products, operations, and marketplaces.
- **Cybersecurity Training:** We deliver cybersecurity training to you and your team members on the published cybersecurity standards and guidance that are meaningful and important to your organization.
- **Assessments:** We work with you to perform assessments of your processes, products, systems, and/or services against one or more published standards, including any custom requirements. Upon successful completion of the assessment, you are presented with a report and letter of attestation or certification (if applicable).
- **System Security and Penetration Testing:** We work with you to determine targeted testing objectives and scope, then we perform independent testing of your product systems security, issuing a report with key findings and detailed results.

Contact Us

To learn more about our global testing & certifications services, contact us today.

866 797 4272
client.services@csagroup.org
csagroup.org