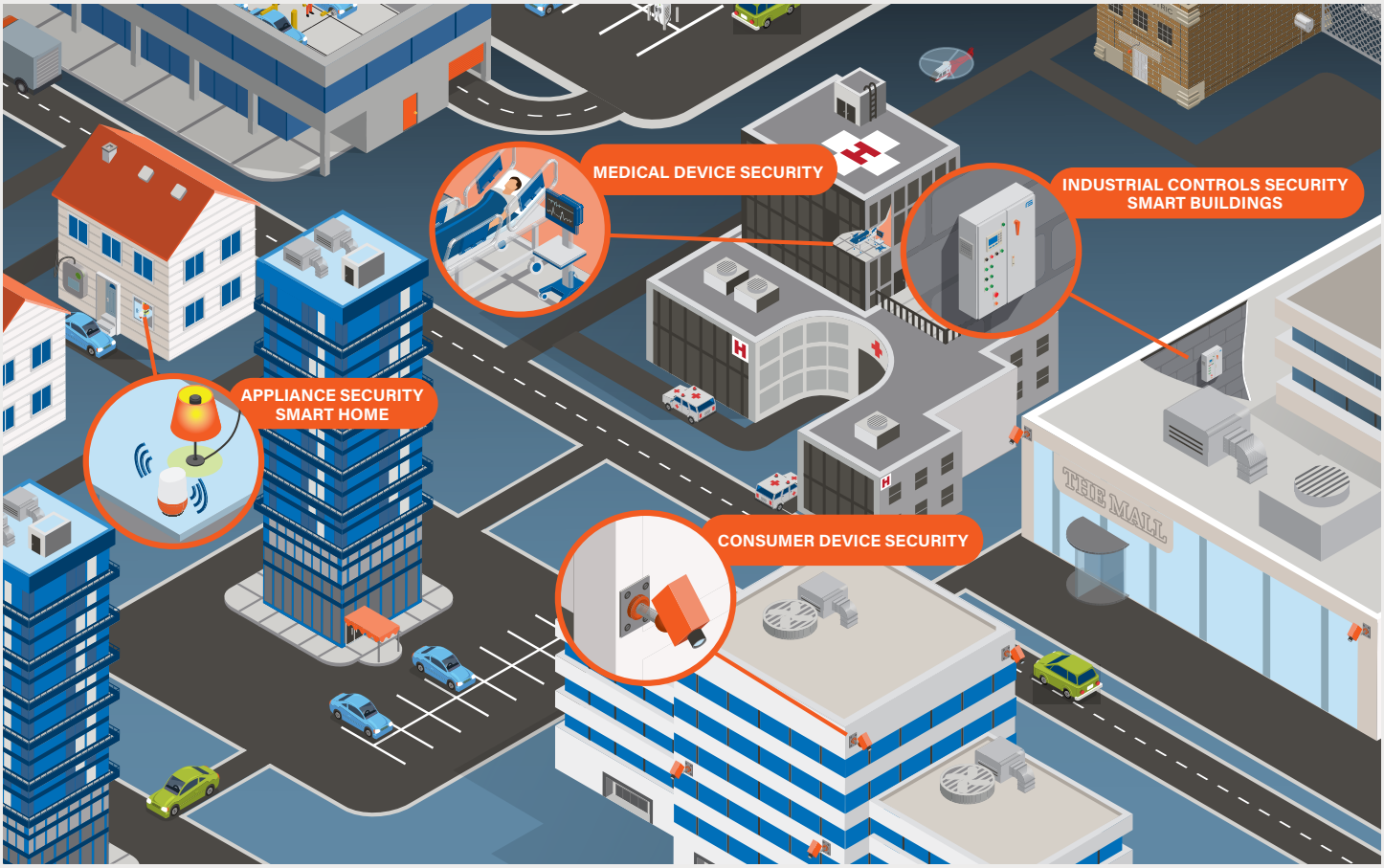
CSA GROUP

Cybersecurity Testing & Certification that Evolves with your Industry

We test to the standards, regulations, or directives developed by the following organizations:

IEC, ISO, CSA, UL, NIST,
Global Regulatory Guidance, EU Directives



Identify Potential Cybersecurity Issues Early in the Design Process

As the world becomes increasingly connected – from smart thermostats to industrial sensors – the risks associated with connectivity rise as well, putting privacy and safety at risk. CSA Group can help you verify your compliance with current and emerging codes and standards for cybersecurity.

Our services, which include gap analyses, bench testing, and standards compliance, help you identify potential cybersecurity issues early in the design process, and then verify that adopted security practices reduce the chance of malicious intrusions and attacks throughout the product lifecycle.

BENCH TESTING

Bench testing is independent product testing conducted in our cybersecurity laboratory. It can help you identify how robust and resilient your connected product or software is and will help you uncover mechanical or design flaws that could have safety and security implications. Our bench testing services include a variety of valuable evaluation techniques, such as:

- Black box / White box penetration testing
- Static source code analysis using the software weakness enumeration (CWE) database
- Binary code analysis using the CWE database
- Vulnerability identification using the common vulnerability enumeration (CVE) database
- Identification of known malware
- Structured penetration testing
- Communication robustness testing and fuzz testing
- Security controls evaluation

CUSTOM TRAINING PROGRAMS

Gain practical solutions for introducing or expanding security assurance know-how with our customizable interactive training workshops. We cover a variety of comprehensive topics, from introductory overviews to specific implementation considerations. Workshop topics include:

- Introduction to Cybersecurity: Suitable for all audiences, this workshop provides details to baseline the environment and needs of your specific industry's cybersecurity requirements.
- Security Risk Analysis (Threat Modeling): Provides examples of threat modeling practices with sufficient detail for adoption by your organization.
- Quality Management & Supply Chain Considerations: Presents an overview of QMS and supply chain practices needed to support security across the entire product lifecycle.
- Security Assurance: Explains specific activities and deliverables that will support your organization's need to demonstrate product security capabilities and security testing methods.
- Applicable Standards, Frameworks, and Regulations: Trains your organization on specific cybersecurity standards and other requirements, which help you meet regulatory requirements for cybersecurity assurance in your industry.

GAP ANALYSIS

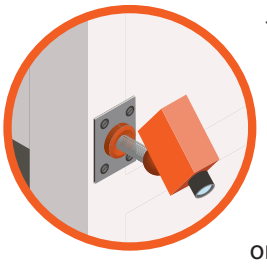
A gap analysis will provide a thorough evaluation of how well developed the cybersecurity controls implemented in your product, service, or company are. This service will help you determine the overall areas of cybersecurity weakness and understand where you need improvements.

CSA Group can provide gap analyses for key product and process standards and frameworks that address cybersecurity for your products, including:

- ANSI/CAN/UL 2900 series of Standards
- IEC 62443 series of Standards
- ISO 27001
- ISO 27034-1
- NIST Cybersecurity Framework

SECURITY DEVELOPMENT LIFECYCLE ASSURANCE (SDLA)

When cybersecurity protocols are established early with SDLA – before committing to production – you can help mitigate cybersecurity threats throughout your product's lifecycle. You'll have processes in place to verify that appropriate protocols are identified and implemented on an ongoing basis, reassuring stakeholders that your industrial automation and control systems products comply with requirements defined in IEC 62443-4-1.



CSA Group can help you verify your compliance with current and emerging codes and standards for cybersecurity.

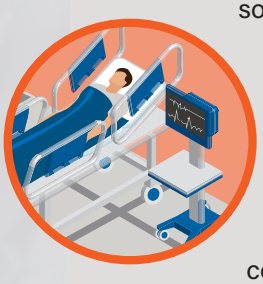
The CSA Group Difference

Rely on an internationally recognized company with over 100 years of expertise and knowledge. From our early beginnings developing standards for railway bridges to today's latest sustainable technologies, we're always looking forward and developing innovative standards and testing programs for the most advanced and emerging technologies. Drawing on our industry accreditations, our customer-focused experts can create custom solutions that meet your unique testing, inspection, and certification needs. That's how we're holding the future to a higher standard.

CYBERSECURITY VERIFICATION PROGRAM (CVP)

It is increasingly common for purchasing organizations such as hospitals or retail developers to have procurement language requesting information about the security of connected devices they are acquiring. Because they are purchasing items from across a variety of industries — from smart lighting to wireless printers — there is a need for a common procurement language that applies to these varied products. CSA Group's CVP is a major step in this direction, and it has been leveraged by several industry verticals as a standardized security framework.

Using our CVP model, a manufacturer can demonstrate the sophistication or maturity level of processes and products, which then helps provide security evidence for IoT solutions. Investing in this program as a manufacturer makes it easier for network owners to evaluate and choose your products. It contributes to reduced overall risk from cyber threats and helps you increase your attractiveness to the market as a cyber-mature vendor of connected solutions.



CVP – 3 STEPS

This three-step program allows manufacturers to identify security activities employed for their IoT solutions, understand their existing maturity level, and develop specific test programs supporting an effective security culture for their connected solutions. The three steps include:

1. A self-assessment of security activities using a structured template developed by CSA Group.

2. CSA Group conducts an audit of the information presented in the self-assessment template and provides feedback on any gaps, which helps to affirm a current level of cybersecurity maturity within the organization and product.

3. CSA Group can also perform product security testing using either voluntary international standards or a custom test plan appropriate for the IoT solution.

Completing all three steps can provide the richest evidence to determine security maturity at the organization and solution (product) level.

The maturity level of each cybersecurity activity is assessed so that an organization can assert their security maturity in relationship to best practices. The maturity levels of the CVP range from Level 0 to Level 3, where Level 0 means no evidence exists of the basic controls needed to protect the organization or its products, while Level 3 affirms a well-established process for security implementation with continuous support and security enhancements.

csagroup.org/cyber

Contact Us

Put CSA Group's industry-leading knowledge and experience to work for you.

1 800 463 6727
sales@csagroup.org
store.csagroup.org

05/2019