

Achilles Practices Certification Datasheet

BUSINESS CHALLENGE

The growing threat to operational technology environments is growing. To remain competitive, organizations must connect their operations to broader enterprise IT networks, but in doing so the risk of cyber attack is increased.

The IEC 62443-2-4 standard was developed to help ensure that industrial control and automation systems meet required levels of cyber security to minimize vulnerability to cyber attacks. Certification to the standard is a valuable demonstration of an organization's commitment to cyber security, offering peace of mind to end-users and satisfying regulatory requirements.

Achilles Practices Certification Service

Ensuring device security across the development lifecycle

To gain operational efficiency from advances in technology, Operational Technology (OT) environments are being connected to the broader enterprise IT infrastructure. That infrastructure, however, is under near constant attack from increasingly organized, sophisticated attackers. Advanced malware is finding its way into OT systems at an increasing rate.

In an effort to reduce the risk to reliability, continuity and operational quality of industrial control and automation systems. A standard was established for the incorporation of security best practices into the system development lifecycle. The standard, IEC 62443-2-4, was adopted globally and created a framework and a common language that helps end users communicate their requirements and expectations for the security of systems developed and serviced by their vendors.

Challenge

IEC 62443-2-4 established that manufacturers must now demonstrate that security measures are incorporated in their development lifecycle across four key areas:

- **Organization** – the development and implementation of security governance, policies and procedures
- **System capability** – building security functions into the manufacturers' systems or services, and that compensating security functions are used to protect system components and subsystems that do not have built-in security capabilities
- **Commissioning and acceptance testing** – demonstrating that the security functions built into the vendor's system are correctly implemented and that the systems are ready to be operated by the principal or selected vendor
- **Maintenance and support** – ensuring that maintenance of security functions built into the manufacturers' systems are correct and timely support is delivered in response to security-related events

BENEFITS

- A simple, scalable, and cost effective solution that demonstrates compliance with the industry standard.
- Validates third party incorporation of security best practices.
- Provides practical metrics and requirements for secure installation and configuration.
- Improves supplier, vendor and end-user communication of requirements.
- Ensures systems and networks meet current and emerging international cyber security standards and government regulations.

Solution

Wurldtech's Achilles Practices Certification ensures device manufacturers include cyber security best practices in the processes and procedures used to develop their products. It was developed to enable product suppliers, system integrators and maintenance service providers to formally illustrate compliance of their solutions with cyber-security capabilities required by the IEC 62443-2-4 standard.

Achilles Practices Certification spans the entire system lifecycle from organizational governance, through solution design and services development, testing and commissioning, to maintenance and support.

The certification is recognized as the industry standard for the development of best practices and provides peace of mind with documented evidence of compliance. Solutions with the certification are found to be robust and designed according to security best practices.

FEATURES

Achilles Practices Certification is delivered across four phases. You may elect to follow all four sequentially, or choose the phase that is suited to your current needs.

Phase 1 - Scoping

You determine the desired outcomes of the certification and define the specific system to be certified. The scope of project is designed specifically to achieve your goals. The desired level of certification is dependent upon the purpose, current security practices and resources.

Phase 2 - Vendor Preparation

In Phase 2 the information you provide is reviewed to ensure it meets the requirements and identifies any ambiguity or other parameters that need to be corrected.

Phase 3 - Appraisal

Wurldtech verifies that the information you provided accurately depicts security best practices. Here we look at specific process areas and the applicable requirements to ensure that all of the relevant criteria are met.

Phase 4 - Reporting

Upon attaining certification, you receive a final, confidential report that details your practices and assesses its conformance to necessary regulations. You also receive a certificate of accomplishment, and a public report that you may use to demonstrate your achievement.



Certification Categories

We offer four certification categories, with four certification levels in each category:

Product Supplier

Certificate for security capabilities of Automation Solution products in support of APC integrators and maintenance provider certificates. IEC 62443-2-4 identifies security capabilities required of the Automation Solution.

Integrator Certificate

Certificate for integrator security programs. Certifies that the applicant has a verified set of security capabilities that can be performed for the implementation/deployment of an Automation Solution.

Maintenance Provider Certificate

Certificate for maintenance provider security programs. Certifies that the applicant has a verified set of security capabilities that can be performed for the maintenance of an Automation Solution.

Solution Certificate

Certificate for the application of security capabilities during integration and/or maintenance of a specific Automation Solution.

Certification levels

IECEE Selectable certification

Awarded for successful completion of requirements that you select for verification.

Bronze certification

Our entry-level certification, awarded for successful completion of all applicable requirements for security policies and practices that have been implemented and verified.

Silver certification:

Awarded for successful completion of all applicable requirements and selected requirement enhancements that have been implemented and verified through direct measurement or analysis.

Gold certification:

Awarded for successful completion of all applicable security policies and practices that exist in your system. Gold level contains additional performance and industry-specific requirements.



Why Wurldtech

Wurldtech, a GE Company, helps you harden your security posture and prepare to succeed in the new digital industrial landscape. We understand operational technology like no other, and we can help you protect it like no other as well.

Contact us to learn more:

Toll free: 1 877 369 6674

Email: sales@wurldtech.com

CONNECT WITH US

Follow us:



Securing Innovation Blog
wurldtech.com

Wurldtech is a trademark of the General Electric Company. All other trademarks are the property of their respective owners. Wurldtech reserves the right to make changes in specifications and features shown herein, or discontinue the product described at any time without notice or obligation.

© 2016 Wurldtech Security Technologies Inc. All rights reserved.

APC-DS-0616