# Achilles System Certification (ASC) from GE Digital

## Frequently Asked Questions

Safeguard your devices and meet industry benchmarks for industrial cyber security.

# What is ASC Program?

GE Digital developed the Achilles System Certification (ASC) program, enabling control system vendors to formally illustrate compliance of their control system products with cyber-security requirements specified by the IEC 62443-3-3 standard (Part 3-3: System security requirements and security levels).

This certification spans the design and engineering technical security requirements for a control system product. The security requirements and its associated security levels can be used by the control system vendor, asset owner, or integrator to assess cybersecurity of their systems.
The control system products can also be certified to four security levels (SL-1 to SL-4) based on the security capabilities implemented for the system.

# Who does the ASC certification program apply to?

The ASC program is applicable to organizations that supply control system products for integration into automation solutions as part of their core business.

Asset owners or the end-users of the control system product can use the ASC to select the product that meets their security requirements. Therefore, control system vendors are able to build security features into their products that can be certified as conformant to the IEC 62443-3-3 requirements selected by the asset owner. This certification relieves the asset owner from having to verify these capabilities themselves for each of their control system product.

# Why is ASC important to your organization?

Depending on the industry and the activities a product supplier performs, product suppliers may choose to have their control systems certified for a variety of reasons. Common reasons include:

- Your customer requires it
- Your company has adopted IEC 62443 as the basis for security so it doesn't have to provide separate, custom security solutions for each customer
- Your company doesn't want to separately validate its control system's security capabilities for each customer; instead it wants to provide the ASC certificate to its customers
- Your company wants to establish credentials as a qualified supplier
- Your company wants to have a reputation of being a leader in the area of security
- Your company wants to keep up with the competition
- Your company wants to proactive in the face of regulation

In addition, the IEC 62443 series provides a common language to facilitate the interaction between end-users (asset owners), device manufacturers and control system vendors, and integration and maintenance providers (service providers).

It becomes easier for asset owners to compare the security capabilities of control systems of different suppliers, since ASC certificates specify the exact IEC 62443-3-3 requirements that the control system product meets. Control systems without ASC certificates are more difficult for asset owners to compare and evaluate.

## How is ASC program different from Achilles Practices Certification (APC) program?

The ASC Program is based on the IEC 62443-3-3 standard and certifies security capabilities that are implemented in the control system product. This certification does not cover the organization's cyber security program requirements (such as risk management, governance, HR security practices, cyber security trainings, etc.) or any practices related to secure development, integration, maintenance or operation services of the product.

Security levels are defined by IEC 62443-3-3 as measure of attacker proficiency. They are assigned to individual IEC 62443-3-3 requirements to indicate that the strength of the required capability corresponds to the strength of the attacker. As a result, protection against more capable attacks are provided by security capabilities with higher security levels. A control system consisting of several components is certified as a system with the ASC certificate showing the lowest SL that the system meets. Hence component themselves are not individually certified.

In contrast, the APC covers the procedural aspects of the control system solution's integration and maintenance activities from organizational governance, through solution design and services development, testing and commissioning, to maintenance and support. The APC is applicable to control system vendors, system integrators, and maintenance service providers.

The APC maturity level at which the solution is certified allows one to evolve security program and control system solution product capabilities. Solution services or systems can be certified at different maturity levels.

## Does the certification apply to a product line or a company?

The certification applies to control system components that are declared in scope, along with the desired level of security for them. Product suppliers, service providers, and asset owners can get their control system product certified through ASC program.

## What are the security levels against which control system product can be certified?

Control system product can be certified against four security levels based on the security assurance against cyber threats. Protection against more capable attacks are provided by security capabilities

with higher security levels. As a result, zones with higher risk should be assigned higher security levels. These levels are listed below:

| Security Level | Description |
|---|---|
| 1 | Help prevent casual or coincidental violations of security |
| 2 | Help protect against intentional violation using simple means with low resources, generic skills, and low motivation |
| 3 | Help protect against intentional violations using sophisticated means with moderate resources, IACS specific skills, and moderate motivation |
| 4 | Help protect against intentional violations using sophisticated means with extended resources, IACS specific skills, and high motivation |

# How can I choose correct security level for my product?

A control system vendor can choose the security levels based on the core security features it has implemented for the control system product, or for which it wishes to be assessed for conformity.

The asset owner or end-user should choose the security level based on the security level it needs for each zone where the control system product will reside. The higher the protection desired for the control system product, the higher the security level that it should possess. Therefore, zones with higher risk should be assigned higher security level.

The target security level of the control system product can be determined based on the results of a cyber risk assessment. As a result, requirements that, when implemented, reduce risk to an acceptable level should be selected.

Where is the certification subject matter described?

The control system vendor and GE Digital must agree on the subject matter for certification, which is described in the ASC 3-3 Program Application including:

The list of requirements to which the applicant claims conformance against, can be selected:

- Individually
- By functional requirement (FR) categories
- By security levels

A description of the existing control system product (control system and components) to be certified.

An indication of whether the applicant supports its compliance as:

- Control system vendor
- Asset owner, enforcing security requirements down through its supply chain

The certificate shows that certification has been achieved; the actual scope and subject matter of the certification is described in its complementary document (ASC Audit Workbook and Audit Report).

# How often do suppliers have to re-certify?

Certification is awarded for a specific version of a product, and that certificate is valid as long as that version is supported by the applicant. Re-certification is necessary for new versions and for improvements in security level (new capabilities or improved capabilities).

# How long does the certification process take?

The timeline for certification is dictated by the organization submitting the evidence, and any impact or dependency the ASC certification activities may have on other certification-related processes at the applicant's organization. However, there are pre-defined allowed lead times for executing certain project activities.

# What does the ASC process entail?

GE Digital provides assistance (listed below) during certification that is dependent on the maturity of the applicant's control system program capabilities.

For applicants who have a cyber security program in place, GE Digital provides assistance in understanding the IEC 62443-3-3 requirements and the process for completing and submitting the IEC 62443-3-3 certification application. This assistance is provided in the form of the Certification Process Training Workshop. The workshop provides:

- Guidance in the selection of the IEC 62443-3-3 requirements to which conformance will be claimed (generally as a result of customer requirements)
- Guidance in aligning existing security capabilities with these requirements to determine where compliance deficiencies exist.

For applicants who are just getting started with their security programs, GE Digital bundles the above with assistance in developing a compliant security program. In this program, GE Digital consultants work with the applicant to determine how to best integrate security into the applicant's control system

# What technical capabilities are covered in ASC program?

Control Security product shall have capabilities in one or more areas listed below:

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability

Submitted statements must be signed by senior management or a legal representation of the company as a legal entity.

## How do you choose the requirements in scope of the certification?

The list of requirements to which the applicant claims conformance against, can be selected:

- Individually
- by functional requirements groupings
- by security levels (SL-1 to Sl-4)

The security level to which conformance is claimed is defined by applicant's product security capabilities.

## What happens if my control system product fails certification?

Certificates are awarded for the requirements that are passed. GE Digital will work with applicants on questionable requirements.

## What do I receive once the certification process has completed?

Upon attaining certification, you will receive a final report, certificate, and public report. The certification is announced online, by email, and by press release. You can refer to the certification in your communications (with restrictions) to demonstrable validation of your organization's practices towards a security best practices benchmark in the process control industry.

# How do my customers benefit from certification of my product?

Product level certifications assure your customers that your product incorporates security mechanisms that can be applied as part of the deployment of industrial control systems. It therefore becomes easy for end-users to compare products from different control security vendors using IEC62443-3-3 as baseline criteria.

# How is my certification made public?

GE Digital maintains an ASC certification page on the GE Digital website. Applicants have the option of being listed on that page. Certification achievements can also be announced by newsletter and press release.

# What does GE Digital do with the data?

All data and evidence received and collected during the certification process and appraisal review is treated as highly confidential. It is stored in a secure server at the GE Digital facility.
Access is granted to only a restricted set of GE Digital Cyber Security Consultants to protect the confidentiality and privacy of applicant data.
The applicant can request a copy of the data. GE Digital compiles aggregate program statistics, stripped of specific customer details, which it may use at its discretion.

# Can an awarded certificate be canceled? Under what circumstances would this happen?

Yes, a certificate can be canceled if it is discovered that the applicant provided inaccurate responses or falsified evidence, misused the logo or any public communication, or similar activities

# What if our organization does not yet comply to certain requirements, but has plans in place to do so?

You may choose to adopt a phased approach, in which you become certified for what you can do today and you add new capabilities in future certifications.

## About GE

GE (NYSE: GE) is the world's Digital Industrial Company, transforming industry with software-defined machines and solutions that are connected, responsive and predictive. GE is organized around a global exchange of knowledge, the "GE Store," through which each business shares and accesses the same technology, markets, structure and intellect. Each invention further fuels innovation and application across
our industrial sectors. With people, services, technology and scale, GE delivers better outcomes for customers by speaking the language of industry.

## Contact Information

Americas: 1-855-YOUR1GE (1-855-968-7143)
gedigital@ge.com

## www.ge.com/digital