ALWAYS ON THE SAFE SIDE WITH HONEYWELL GAS METERS

> **If you conduct financial transactions with your mobile phone or laptop, you can be sure that security-relevant data will not be affected and that the device cannot be hacked. Shouldn't you also place such demands on the measuring equipment used, which is ultimately your company's cash machine?**

As one of the leading technology companies, Honeywell attaches great importance to the topic of cyber security and has therefore had both the development and maintenance process of its products and some of the products themselves certified accordingly.

CYBER SECURITY BY DESIGN

We have introduced a "Security Development Lifecycle Process" for the development and maintenance of our products. This is certified according to the relevant requirements of ISASecure® Security Development Lifecycle Assurance (SDLA) 3.0.0 and IEC/ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements.

In this way, Honeywell ensures that security aspects are integrated into product development from the outset and do not give rise to changes at a later stage – security mechanisms and controls are treated in the development process in the same way as other elements.

In addition, the process also defines the measures to be taken when rectifying product anomalies.

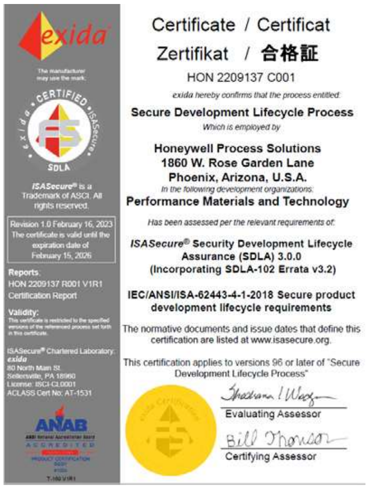
SECURITY DEVELOPMENT LIFECYCLE PROCESS

Work performed according to lifecycle phases

The "Security Development Lifecycle Process" defines in detail which work is to be carried out in which phase of the development process:

- Inception: During project scoping, security requirements are identified and incorporated into the project requirements.
- Elaboration: The main goals in this phase are to minimize critical technical risks and to develop a suitable architecture.
- Construction: Measures may have been identified during design and implementation that will be implemented at this stage.
- Transition: To ensure that the end user can verify the integrity and authenticity of the product, the product packages and components are signed with a certificate.

If a product anomaly is corrected, a check is made at all times to determine whether the correction could affect the safety of the product. If so, the anomaly and its fix are analyzed to determine how to handle any security issues.



exida

The manufacturer may use the mark:

CERTIFIED · ISASecure · exida · SDLA

ISASecure® is a Trademark of ASCI. All rights reserved.

Revision 1.0 February 16, 2023
The certificate is valid until the expiration date of February 15, 2026

Reports:
HON 2209137 R001 V1R1
Certification Report

Validity:
This certificate is restricted to the specified versions of the referenced process set forth in this certificate.

ISASecure® Chartered Laboratory:
exida
80 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

ANAB
ACCREDITED
PRODUCT CERTIFICATION

Certificate / Certificat
Zertifikat / 合格証

HON 2209137 C001

exida hereby confirms that the process entitled:

Secure Development Lifecycle Process

Which is employed by

Honeywell Process Solutions
1860 W. Rose Garden Lane
Phoenix, Arizona, U.S.A.
In the following development organizations:
Performance Materials and Technology

Has been assessed per the relevant requirements of:

***ISASecure®* Security Development Lifecycle Assurance (SDLA) 3.0.0**
(Incorporating SDLA-102 Errata v3.2)

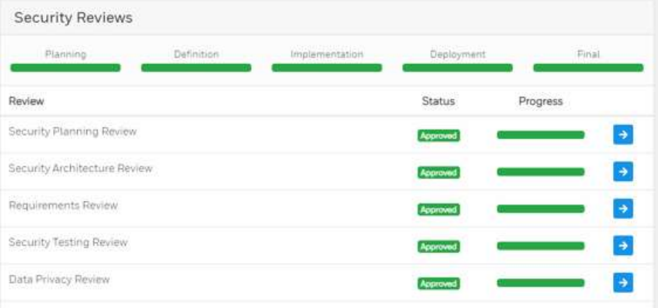
IEC/ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements

The normative documents and issue dates that define this certification are listed at www.isasecure.org.

This certification applies to versions 96 or later of "Secure Development Lifecycle Process"

Evaluating Assessor

Bill Thomson
Certifying Assessor



Security Reviews

Planning	Definition	Implementation	Deployment	Final
▬	▬	▬	▬	▬

Review	Status	Progress	
Security Planning Review	Approved	▬	→
Security Architecture Review	Approved	▬	→
Requirements Review	Approved	▬	→
Security Testing Review	Approved	▬	→
Data Privacy Review	Approved	▬	→

Roles in the development process

To implement the tasks mentioned, further security-specific roles are defined in addition to the usual roles in a development project:

- Security Architect (project role): This person guides the team in defining the architecture requirements from a security perspective and provides design guidance based on cyber security.
- Security Tester (project role): The security tester has a high understanding of potential cyber security attacks and has special training in the use of security tools.
- Master Security Architect (organizational role): This person is responsible for advising and mentoring the Security Architect, for final approval of threat assessments, and for determining solutions to unresolved security issues that the Security Architect encounters.
- Master Security Tester (organizational role): This role is responsible for advising and supporting security testers and the test tools used.

Results in the development process

During the development process, a number of documents are created that are used to review the results, as well as for final approval. These include:

- Requirements repository: collection of security requirements and non-functional requirements based on the Master Security Requirements (MSR). The security requirements relevant to the project are selected and included in the project's requirements repository.
- Software architecture: The document provides information on how the system architecture is built to meet security requirements that need special treatment in the architecture.
- Threat model: Analysis and assessment of the risk level of the application including information on
  - Vulnerabilities: definition of the potential points of attack.
  - Threats: identification of possible scenarios of how the system could be misused.
  - Measures: mechanisms for risk minimization of the possible threats; additional requirements or architectural elements that need to be implemented and tested.

Additional documents such as reports of the static code analysis, a planning for the security tests or even a checklist with which the required security information for the user documentation is checked complete the required deliverables.

Approval by the Chief Technology Officer (CTO)

Appropriate tools are used to monitor compliance with the process and the review of the deliverables. After the individual process steps have been carried out and documented, a final review is carried out and submitted to the CTO for approval.

All products containing software or firmware must be finally approved by the CTO with regard to cyber security requirements before going into mass production.

Safety requirements for outsourced components

Of course, the high safety requirements for the certified development process not only apply to the products developed by Honeywell, but also to the product development processes at suppliers who develop components for Honeywell. The task of the Security Architect is to ensure that the selected suppliers meet the defined security requirements before they are commissioned with the development.

Vulnerability management

Cyber security vulnerabilities are reported through internal and external sources:

- Internal processes: These are security assessments or security tests, threat models, static code analyses and code reviews, or design or architecture reviews.
- External communications such as black hat or white hat hackers, customers, security organizations (e.g., NIST, BSI [German Federal Office for Information Security]), etc.

Reported vulnerabilities are captured via appropriate reports in Honeywell bug management systems and prioritized to determine the version in which the fix will be available.

COMPONENT CERTIFICATION ACCORDING TO IEC 62443

As mentioned at the beginning of the article, a second aspect in addition to the certified development and maintenance process is the certification of the product itself. This is what more and more customers and authorities are demanding, although it is often not specified in detail which certification is desired.

Based on our experience in the field of industrial automation, we as a manufacturer have decided to strive for component certification according to IEC 62443 (secure industrial automation and control systems) for gas meters.

The international series of standards IEC 62443 deals with the cyber security of industrial automation and control systems (IACS) and pursues a holistic approach for operators, integrators, and manufacturers.

Cyber security is becoming an increasingly important consideration when evaluating gas meters. At Honeywell, we have long been aware of our responsibility and have implemented appropriate measures in the development and maintenance of our products. Product certification is due to follow.

Stay on the safe side with Honeywell products!

Bernhard Thomas
bernhard.thomas@honeywell.com